

# СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ БЕЗПЕКИ ТА ОБОРОНИ

ISSN 2311-7249 (Print)

ISSN 2410-7336 (Online)

№ 3(36)  
2019

Науковий журнал

## Засновник і видавець

Національний університет оборони України  
імені Івана Черняхівського  
Журнал заснований у 2008 році

## Адреса редакції

Національний університет оборони України  
імені Івана Черняхівського  
Інститут інформаційних технологій  
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, російською та англійською мовами  
Журнал виходить 3 рази на рік

Наказом Міністерства освіти і науки України  
від 29 грудня 2014 р. №1528 журнал включено до  
Переліку наукових фахових видань України  
в галузях “технічні науки” та “військові науки”

Рекомендовано до друку Вченою радою  
Національного університету оборони України  
імені Івана Черняхівського  
(протокол № 12, 23.12. 2019 р.)

При використанні 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:

### Військова кібернетика та системний аналіз

- Лобанов А.А., Мозговий Р.А. До оцінювання ефективності управління військами (силами) 5  
Нестеров О.М. Удосконалений метод розрахунку пропускну здатності системи зв’язку спеціального призначення на інформаційних напрямках ..... 11  
Коренівська І.С. Підхід щодо оцінювання надійності функціонування підсистеми передачі даних автоматизованої системи управління авіацією та протиповітряною обороною ..... 15  
Мельник Я.В., Бобильов В.С. Методичні рекомендації щодо використання існуючих програмного забезпечення та програмних утиліт для визначення топології гетерогенних мереж для знаходження альтернативних варіантів підключення ..... 19  
Муренко В.О., Безуглий В.М. До питання оцінювання ефективності об’єднаної підготовки сил оборони військової частини надводних сил Військово-Морських Сил та морської охорони Державної прикордонної служби ..... 25  
Міренко В.І., Кітків С.В. Непівмарківська математична модель технічного обслуговування радіоелектронних засобів зенітного ракетного озброєння ..... 29  
Москаленко А.О., Глуховець Ю.В., Варич В.В., Івко С.О. Методика застосування сигналів удосконаленої модуляції циклічним звуком коду з адаптацією по швидкості передавання інформації в перспективних радіоінтерфейсах ..... 35  
Ляшенко І.О., Ключак О.М., Зелінська С.П. Безперервні динамічні моделі надійності програмного забезпечення інформаційно-управляючих систем спеціального призначення 41  
Котлярів В.П., Кузнецов О.А. Щодо питання визначення раціональних способів виконання завдань з урахуванням задач розподілу ..... 45  
Романченко І.С., Потьомкін М.М., Кравець О.П., Саковський Г.А. Комплексний метод ранжування та його використання для багатокритеріального порівняння альтернатив ..... 49

### Протиборство у кібернетичному просторі

- Гришук Р.В., Жовноваток Р.М., Носова Г.Д. Гібридні загрози у кіберпросторі: фактори впливу на природу виникнення ..... 53  
Гульков М.О., Толкачев В.С. Технічний захист інформації, як складова інформаційної безпеки, у контексті євроатлантичної інтеграції України ..... 59

### Військово-космічні та геоінформаційні технології

- Зуйко В.В., Зотов С.В., Кошлань О.А. Методика оцінювання надійності виконання заходів топогеодезичного забезпечення ..... 65

### Інформаційно-аналітична діяльність у сфері безпеки та оборони

- Крайнов О.В., Грозовський Р.І., Кравчук А.А. Методика оцінки якості інформаційно-аналітичного забезпечення роботи автоматизованих інформаційних систем органів управління військового призначення ..... 69  
Лук’янчук В.В., Ніколаєв І.М., Опенько П.В., Дзюбенко Ю.А. Шляхи і принципи розвитку технологічного базису зенітного ракетного озброєння ..... 75  
Марко І.Ю., Чернишова І.М., Муштук А.В., Марко Є.І. Методика визначення обсягу фінансових ресурсів для забезпечення з’єднання (частини) Збройних Сил України необхідною кількістю технічно готового озброєння та військової техніки ..... 83  
Дачковський В.О., Родченко Л.М. Методика оцінювання відновлюваності озброєння та військової техніки ..... 89  
Бабрица А.О. Обґрунтування показника вибору оптимального алгоритму виділення фону у відеопослідовностях з камер відеоспостереження відомчих систем відеоспостереження 97  
Кузнецов І.Б., Дядечко А.О., Марценківський В.Т. Алгоритм контролю параметрів озброєння та військової техніки для інформаційно-виміральної системи військового призначення ..... 103  
Тіхонов Г.М., Баталов В.І., Безуглий В.М. Підготовка апарату керівництва до командно-штабного навчання з використанням засобів імітаційного моделювання ..... 109  
Ганненко Ю.О., Закалад М.А. Аналіз функціонування системи логістики у провідних країнах світу ..... 115

### Інтелектуальні ІТ та робототехніка у сфері безпеки та оборони

- Пермяков О.Ю., Королюк Н.О., Маслійова С.О. Підхід щодо автоматизації процесів оцінки повітряного противника на пунктах управління Повітряних сил ЗСУ ..... 123

### Інтерактивні моделі розвитку науково-освітнього простору

- Чопі Д.А., Дерев’ячук А.І., Козир Н.М. Основні інноваційні напрями застосування сучасних інформаційних технологій у підготовці військових фахівців ..... 127

### Високотехнологічні аспекти воєнного мистецтва

- Бутвін Б.Л., Машикін О.О., Соляницький О.І. Метод розрахунку інтегрального показника якості моделей та поліноміальних комплексів операцій (бойових дій) ..... 135  
Кожурба В.І., Довгополій А.С., Гусяков О.М., Лойко М.П. Дослідження можливості використання невибухового імпульсного сейсмічного джерела для знищення вибухових пристроїв ..... 141

### Стратегічні комунікації та когнітивні системи спеціального призначення

- Пунда Ю.В., Козинець Л.П., Клименко В.С. Методологічні підходи до визначення рівня конфліктності міждержавних відносин ..... 151  
Алещенко В.І. Особливості сучасних психологічних операцій в умовах гібридної війни 157  
Артошин Л.М., Лагодний О.В. Індикатори виявлення негативного психологічного впливу під час моніторингу електронних засобів масової інформації ..... 165  
Войтко О.В., Кацалап В.О., Чернега В.М. Особливості сприйняття та реагування на отриману інформацію ..... 171

---

## **Редакційна колегія**

### ***Головний редактор***

**РАКУШЕВ Михайло Юрійович,**

доктор технічних наук, старший науковий співробітник  
Національний університет оборони України імені Івана Черняховського

### ***Члени редколегії:***

**КОРОЛЮК Наталія Олександрівна,**  
кандидат технічних наук, доцент

**МАЦЬКО Олександр Йосипович,**  
кандидат військових наук, професор

**ДАНИК Юрій Григорович,**  
доктор технічних наук, професор

**КАТЕРИНЧУК Іван Степанович,**  
доктор технічних наук, професор

**КОЦЮРУБА Володимир Іванович,**  
доктор технічних наук, доцент

**КРАВЧЕНКО Юрій Васильович,**  
доктор технічних наук, професор

**ЗИНЧЕНКО Андрій Олександрович,**  
доктор технічних наук, доцент

**КОВБАСЮК Сергій Валентинович,**  
доктор технічних наук, старший науковий  
співробітник

**РУБАН Ігор Вікторович,**  
доктор технічних наук, професор

**ГАЦЕНКО Сергій Станіславович,**  
кандидат технічних наук

**САВЧЕНКО Віталій Анатолійович,**  
доктор технічних наук, професор

**МАЛАНЧУК Марина Федорівна,**  
кандидат економічних наук

**Goran SHIMIC,**  
доктор філософії, професор

**ПЕРМЯКОВ Олександр Юрійович,**  
доктор технічних наук, професор

**ВОЙТКО Олександр Володимирович,**  
кандидат військових наук

**ВАРЛАМОВ Ігор Давидович,**  
кандидат технічних наук, доцент

**ЛОБАНОВ Анатолій Анатолійович,**  
доктор військових наук, професор

**РОМАНЧЕНКО Ігор Сергійович,**  
доктор військових наук, професор

**ТЕЛЕЛИМ Василь Максимович,**  
доктор військових наук, професор

**РЕПЛО Юрій Євгенович,**  
доктор військових наук, професор

**ШЕМАЄВ Володимир Миколайович,**  
доктор військових наук, професор

**СОЛОННИКОВ Владислав Григорович,**  
доктор технічних наук, професор

**ЛАВРІНЧУК Олександр Васильович,**  
кандидат технічних наук, старший науковий  
співробітник

### ***Відповідальний секретар***

**ВОЙТКО Олександр Володимирович,** кандидат військових наук

# MODERN INFORMATION TECHNOLOGIES IN THE SPHERE OF SECURITY AND DEFENCE

ISSN 2311-7249 (Print)

ISSN 2410-7336 (Online)

№ 3(36)  
2019

Scientific journal

## Founder and Publisher

National Defence University of Ukraine  
named after Ivan Cherniakhovsky  
The journal was founded in 2008

## Address:

National Defence University of Ukraine  
named after Ivan Cherniakhovsky,  
Information Technology Institute

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 KB №20490-10290PIP)

The journal is published  
in Russian, Ukrainian and English

The journal is published thrice a year

According to the Document of the Ministry of  
Education and Science of Ukraine  
issued on December 29, 2014 (№ 1528) the journal  
was included into the Ukrainian list of specialized  
scientific publications in engineering sciences and  
military sciences

*Recommended to publication  
by the Scientific Council of the National  
Defence University of Ukraine  
named after Ivan Cherniakhovsky  
(Protocol № 12, 23.12. 2019)*

When using the materials, the reference to the journal  
“Modern Information Technologies  
in the Sphere of Security and Defence” is mandatory

The editorial board can have a different viewpoint  
than that of the authors

The content of the materials is the authors' responsibility

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:

### *Military cybernetics and system analysis*

- Lobanov A., Mozghovyi R.* To evaluate the effectiveness of the army (force) management .....5  
*Nesterov O.* The enhanced method of capacity computation for the special-forces communication system in information directions .....11  
*Korenivska I.* The approach of assessing the reliability of troops (forces) automated control systems data subsystems .....15  
*Melnyk Y., Bobylow V.* Methodological recommendations for the use of existing software and software utilities for determining the topology of heterogeneous networks for finding alternative connection options .....19  
*Murenko V., Bezuhlyi V.* On the issue of evaluating the effectiveness of joint training of the Defense Forces of the military part of the Surface Forces of the Naval Forces and the maritime security of the State Border Guard Service .....25  
*Mirnenko V., Kitk S.* Semi-market mathematical model of radio electronic maintenance of anti-air missile arms .....29  
*Moskalenko A., Ghlukhovec J., Varych V., Ivko S.* Methods of application of signals of advanced modulation by cyclic shift of the code with adaptation on speed of information transmission in perspective radio interfaces .....35  
*Lyashenko I., Kliuchak O., Zelinska S.* Unlimited dynamic models advanced software information-controlling systems for special appointment .....41  
*Kotliarov V., Kuznetsov A.* Concerning the question of definition of rational ways of performing the tasks considering the problems distribution .....45  
*Romanchenko I., Potomkin M., Kravets O., Sakovskiy H.* A complex method of range and its use for multicriteria comparison of alternatives .....49

### *Confrontation in the cybernetic*

- Hryshchuk R., Zhovnovatiuk R., Nosova H.* Hybrid threats in cyber space: factors of influence on nature of emergence .....53  
*Hulkov M., Tolkachov V.* Technical protection of information as a component of information security, in the context Euro-Atlantic integration of Ukraine .....59

### *Military space and geoinformation technologies*

- Zuiko V., Zotov S., Koshlan O.* Method of assessment of reliability of compliance of topogeodesic security measures .....65

### *Information and analytical activities in the field of security and defense*

- Krainov O., Hrozovskiy R., Kravchuk A.* Quality assessment method of information-analytical support of work of automated information systems of military management bodies .....69  
*Lukyanchuk V., Nikolaev L., Open'ko P., Dzubenko Y.* Ways and principles of development of anti-aircraft missile systems technological base .....75  
*Marco I., Chenyshova I., Mushtuk A., Marco Y.* The method of determining the volume of financial resources for the provision of the armed forces of the Ukraine of the necessary .....83  
*Dachkovskiy V., Rodchenko L.* Recovery methodology weapons and military equipment .....89  
*Babaryka A.* The justification of optimal algorithms index choice for the background subtraction in video sequences derived from stationary cameras of video surveillance systems .....97  
*Kuznetsov I., Diadchko A., Martsenkivskii V.* Algorithm for controlling the parameters of arms and armament for the military information-measuring system .....103  
*Tikhonov H., Bataluk V., Bezuhlyi V.* Preparing the management apparatus for command post exercises using simulation tools .....109  
*Hannenk I., Zakalad M.* Analysis of the logistics system in the leading countries of the world .....115

### *Intelligent IT and robotics in the field of security and defense*

- Permakov A., Korolyuk N., Masliova S.* Approach on the automation of aircraft owner's evaluation processes at the points of management of the air force .....123

### *Interactive Models of Scientific Educational Environment Development*

- Chopa D., Derevianchuk A., Kozyr N.* General innovative directions of the use of modern information technologies in the training of military specialists .....127

### *High-tech aspects of martial arts*

- Butvin B., Mashkin O., Solomitskii O.* Application of modified equations of dynamics of average for operational forecasting of the turn and results of battle action .....135  
*Kotsiuruba V., Dovhopolyi A., Husliakov O., Loiko M.* Studies on the possibility of using the non-explosive pulse seismic source to neutralize explosion devices .....141

### *Strategic communications and special purpose cognitive systems*

- Punda Y., Kozynets I., Klimentenko V.* Methodological approaches to determining the conflict level of inter-state relations .....151  
*Aleshchenko V.* Peculiarities of modern psychological operations in the conditions of the hybrid war .....157  
*Artushin L., Lahodnyi O.* Determination indicators of negative psychological influence under monitoring of electronic mass media .....165  
*Voitko O., Katsalap V., Cherneha V.* The peculiarities of perception and response to the information produced .....171

---

## **Editorial Board**

### *Chief Editor*

*Mykhailo RAKUSHEV,*

Doctor of technical sciences, senior research fellow  
National Defence University of Ukraine named after Ivan Cherniakhovsky

### *Editorial Board members:*

*Nataliia KOROLIUK,*

candidate of technical sciences,  
associate professor

*Yurii DANYK,*

doctor of technical sciences, professor

*Volodymyr KOTSIURUBA,*

doctor of technical sciences, associate professor

*Andrii ZINCHENKO,*

doctor of technical sciences, professor

*Ihor RUBAN,*

doctor of technical sciences, professor

*Vitalii SAVCHENKO,*

doctor of technical sciences, professor

*Goran SHIMIC,*

doctor of philosophy, professor

*Oleksandr VOITKO,*

candidate of military sciences

*Anatolii LOBANOV,*

doctor of military sciences, professor

*Vasyl TELELYM,*

doctor of military sciences, professor

*Volodymyr SHEMAIEV,*

doctor of military sciences, professor

*Oleksandr LAVRINCHUK,*

candidate of technical sciences,  
senior research fellow

*Oleksandr MATSKO,*

candidate of military sciences, professor

*Ivan KATERYNCHUK,*

doctor of technical sciences, professor

*Yurii KRAVCHENKO,*

doctor of technical sciences, professor

*Serhii KOVBASJUK,*

doctor of technical sciences,  
senior research fellow

*Serhii HATSENKO,*

candidate of technical sciences

*Maryna MALANCHUK,*

candidate of economic sciences

*Oleksandr PERMIAKOV,*

doctor of technical sciences, professor

*Ihor VARLAMOV,*

candidate of technical sciences,  
associate professor

*Ihor ROMANCHENKO,*

doctor of military sciences, professor

*Yurii REPILO,*

doctor of military sciences, professor

*Vladyslav SOLONNIKOV,*

doctor of technical sciences, professor

### *Executive Secretary:*

*Oleksandr VOITKO,* candidate of military sciences

*Анатолій Анатолійович Лобанов (доктор військових наук, професор)*

*Руслан Анатолійович Мозговий (кандидат військових наук)*

*Національний університет оборони України імені Івана Черняхівського, Київ, Україна*

## ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ВІЙСЬКАМИ (СИЛАМИ)

Воєнна наука завжди розглядала наявність стійкого та безперервного управління військами (силами) як одну з вирішальних умов перемоги, підкреслювала його особливу роль у досягненні успіху в операціях. Виходячи з цього, впродовж багатовікової історії воєнного мистецтва особливе значення надавалося розвитку органів, засобів та методів керівництва Збройними Силами і управлінню військами. Так само і в сучасних умовах, як в теорії, так і в практичній підготовці військ (сил), питання управління займали і будуть займати одне з найважливіших місць. Військові фахівці провідних країн вважають, що чітко організоване управління військами (силами) може надати істотну перевагу в ході їх застосування.

В статті розглядаються методи оцінювання ефективності управління військами в залежності від випадкових факторів і способів математичного опису процесу управління. Запропоновані методи оцінювання надають можливість отримати більш об'єктивну та адекватну оцінку ефективності управління військами (силами) при врахуванні різних часткових показників.

**Ключові слова:** модель, метод, система управління, ефективність.

### Вступ

**Постановка проблеми.** Дослідженнями в області воєнного мистецтва встановлено, що при рівності бойових потенціалів угруповань військ перевага однієї із сторін може бути досягнута за рахунок більш досконалого управління, яке може підвищити бойовий її потенціал на 25 %, і навіть більше [1]. У збройних силах провідних держав світу робиться усе можливе для досягнення необхідного рівня якості управління [2]. Прикладом цьому є впровадження інформаційних технологій в управління багатонаціональними силами в операції "Свобода Іраку", що дозволило (за даними іноземних засобів інформації) підвищити їх ефективність більше ніж у 2 рази. Отже, питання оцінювання ефективності управління військами завжди були одними з найважливіших і актуальність їх з часом тільки підвищується.

**Аналіз останніх досліджень і публікацій.** Під час оцінювання ефективності управління військами широко застосовується моделювання операції (бойових дій), яке полягає у встановленні якісних та кількісних зв'язків між умовами ведення бойових дій, параметрами рішення командувача (командира) та плану операції (бою) і властивостями управління військами [1].

При побудові моделі управління військами (силами) процеси, які складають сутність операції (бойових дій), певним чином спрощуються і схематизуються. Із множини факторів, що впливають на них, обирається порівняно невелика кількість найважливіших і отримана схема описується за допомогою того чи іншого методичного апарату залежно від методів оцінювання ефективності.

Загальних способів побудови моделей не існує. У кожному конкретному випадку модель будується із цільової спрямованості операції (бойових дій) і завдання дослідження.

Таким чином завдання удосконалення існуючого науково-методичного апарату оцінювання ефективності управління військами залишається актуальним завданням, необхідність вирішення якого диктується нагальними потребами теорії і практики управління військами.

**Метою статті** є аналіз методів оцінювання ефективності функціонування системи управління військами.

### Виклад основного матеріалу дослідження

Оцінювання ефективності управління військами може здійснюватися різними методами.

Найбільшого застосування набули методи – ретроспективного аналізу, фізичного

моделювання, математичного моделювання і експертних оцінок. Розглянемо докладніше їх сутність [4].

*Метод ретроспективного аналізу* базується на вивченні досвіду управління військами у ході операцій (бойових дій) минулих війн і військових конфліктів. Критерієм ефективності управління військами тут виступає порівняння фактичного результату операцій (бойових дій), з тим, що був визначений (потрібний). Недолік даного методу полягає у наявності лише одного результату операції (бойових дій), що знижує об'єктивність результатів аналізу.

*Метод фізичного моделювання операцій (бойових дій)* пов'язаний з проведенням тактичних, командно-штабних навчань, воєнних ігор у ході яких по фактичних результатах дій сторін можна зробити висновки про доцільність тієї чи іншої організації управління військами. Цей метод потребує значних ресурсних затрат, тому що для отримання достатньо стійких результатів необхідно проводити велику кількість навчань.

Уникнути недоліків попередніх методів дозволяє *метод математичного моделювання операцій (бойових дій)*. Він заснований на побудові математичних залежностей, які дозволяють імітувати хід і результат операції (бойових дій) сторін, тобто математичних моделей.

Під математичною моделлю операції (бойових дій) розуміють систему математичних залежностей і логічних правил, яка дозволяє з необхідною повнотою і у відповідному взаємозв'язку імітувати найсуттєвіші реальні сторони операції (бойових дій) і з заданою точністю визначити значення показників ефективності.

До найважливіших ознак класифікації математичних моделей відносяться ступень урахування в моделі випадкових факторів і спосіб математичного опису процесу.

За наявністю або відсутністю урахування випадкових факторів моделі можна поділити на детерміновані і стохастичні. У детермінованих моделях відображаються процеси, в яких відсутні випадкові події. Стохастичні моделі передбачають обчислення показників при імовірнісному характері процесів, які імітуються.

За способом математичного опису процесів, які проходять у складній системі, моделі можна поділити на аналітичні та імітаційні.

Для аналітичного моделювання характерно те, що зв'язок між умовами операцій (бойових дій) і їх результатом встановлюється за допомогою алгебраїчних, диференціальних, інтегральних рівнянь, логічних умов та інших функціональних співвідношень. Їх перевагою є те, що в цих

моделях знаходяться явні залежності між показниками і параметрами. Однак на практиці залежності, що необхідні, можна отримати тільки для дуже простих умов. Часто, бажаючи мати рішення в явному вигляді, йдуть на значне спрощення аналітичної моделі, що погіршує точність результату.

Нижче наведені декілька прикладів підходів до аналітичного моделювання визначення ефективності функціонування системи управління військами.

*Підхід 1.* Оскільки управління військами передбачає за планом вирішення певного комплексу оперативних завдань в операції (бойових діях) то його ефективність, безумовно, залежатиме від результатів вирішення цих оперативних завдань. Отже, ефективність функціонування системи управління з аспекту способу ведення операції (бойових дій), який визначає певну послідовність вирішення оперативних завдань, можна розглядати як ступінь реалізації усього об'єму оперативних завдань, що визначені у плані (замислі) операції [5].

$$E_{cy} = \frac{\sum_{i=1}^n Z_{SRi}}{\sum_{i=1}^n Z_{SBi}} \quad (1)$$

де:  $E_{cy}$  – ефективність системи управління військами;

$Z_{SRi}$  – оперативне завдання, яке реалізовано в ході операції;

$i \in \{1, \dots, n\}$  – множина оперативних завдань;

$Z_{SBi}$  – оперативні завдання, які заплановані до виконання в ході операції.

*Підхід 2.* Під ефективністю функціонування системи управління можна розуміти ступінь реалізації потенційних оперативних (бойових) спроможностей угруповання військ, військових частин і підрозділів, на які здійснює прямий вплив система управління. Оперативні, бойові та спеціальні спроможності угруповання військ – здатність угруповань військ (сил) виконувати певні завдання (забезпечувати реалізацію визначених військових цілей) за певних умов обстановки, ресурсного забезпечення та відповідно до встановлених стандартів. Оперативні, бойові спроможності включають ударні, вогневі та маневрені можливості, рознесені за масштабом (відповідно для оперативних, оперативно-тактичних і тактичних угруповань військ, військових частин і підрозділів). За такого підходу ефективність функціонування системи управління військами можна розглядати як ступінь

реалізації оперативних (бойових) спроможностей угруповання в операції (бойових діях) та визначається виразом (2):

$$E_{cy} = \frac{\sum_{i=1}^n B_{Pi}}{\sum_{i=1}^n B_{Pi}}, \quad (2)$$

де:  $E_{cy}$  – ефективність системи управління військами;

$B_{Pi}$  – оперативні (бойові) спроможності, які були реалізовані в ході операції (бойових діях),  $i \in \{1, \dots, n\}$ ;

$B_{Pi}$  – потенційні оперативні (бойові) спроможності.

*Підхід 3.* На систему управління військами покладається виконання низки завдань, основними з яких є:

підтримання готовності штабів до управління військами;

підтримання високого рівня бойової готовності військ;

безперервне добування, збір, вивчення, відображення і аналіз даних обстановки і прогнозування її розвитку; вироблення (уточнення) замислу операції (бойових дій);

формулювання (уточнення) рішення; доведення завдань до підлеглих частин (підрозділів);

планування (уточнення плану) операції (бойових дій);

організація (відновлення) управління військами;

організація (відновлення) і підтримка взаємодії; організація забезпечення військ;

організація і здійснення контролю та надання допомоги підлеглим штабам і військам.

Відповідно, в такому аспекті ефективність функціонування системи управління військами угруповання доцільно розглядати як ступінь своєчасного виконання покладених завдань управління в ході операції (бойових дій), вираз (3):

$$E_{cy} = \frac{\sum_{i=1}^n Z_{Pi}}{\sum_{i=1}^n Z_{Bi}}, \quad (3)$$

де:  $E_{cy}$  – ефективність функціонування системи управління військами;

$Z_{Pi}$  – завдання (з управління) системи управління військами, яке було реалізоване в ході ведення операції (бойових дій), де  $i \in \{1, \dots, n\}$  – множина завдань (з управління) покладених на

систему управління;

$Z_{Bi}$  – завдання (з управління) системи управління, яке було сплановано до виконання, де  $i = \overline{1, n}$ .

*Підхід 4.* Відповідно теорії управління військами до функціонування системи управління військами висувається ряд вимог:

високий рівень готовності до функціонування; забезпечення можливості як централізованого, так і децентралізованого управління військами (силами);

оперативність;

стійкість;

безперервність;

скритність;

якість.

Отже, щоб функціонування системи управління військами було ефективним повинні виконуватися усі вимоги, причому з розвитком теорії військового мистецтва ці вимоги можуть зазнавати змін. Чим менше виконуються (або взагалі будь-яка не виконується) зазначені вимоги, тим менше буде ефективність функціонування системи управління військами. Отже, ступінь відповідності цим вимогам також можна розглядати як ефективність функціонування системи управління.

Таким чином, система управління буде ефективна, коли всі її показники (які характеризують відповідність вимогам, що висуваються до неї) будуть відповідати потрібним (мінімально допустимим) значенням, або бути близькими до них.

В такому випадку ефективність функціонування системи управління буде – ступінь реалізації вимог, що висуваються до неї та визначатися виразом (4):

$$E_{cy} = \frac{\sum_{i=1}^n R_{Pi}}{\sum_{i=1}^n R_i}, \quad (4)$$

де:  $E_{cy}$  – ефективність системи управління військами;

$R_{Pi}$  – вимога до функціонування системи управління, яка була виконана в ході ведення операції (бойових дій),  $i \in \{1, \dots, n\}$  – множина вимог до СУ;

$R_i$  – вимоги, які висуваються до системи управління.

Однак цей підхід має низку суттєвих недоліків.

По-перше, в різних умовах обстановки і на різних етапах підготовки і ведення операції (бойових дій) значення різних вимог, які висуваються до управління військами, не є

однаковими. Крім цього деякі вимоги є взаємозалежними, наприклад, “скритність” і “стійкість”, “стійкість” і “безперервність”, “оперативність”. Оскільки ці особливості дуже складно формалізувати і урахувати, то під час згортання часткових показників в інтегральний можуть виникнути значні помилки.

По-друге, отриманий інтегральний показник ( $K_y$ ) вже достатньо складно інтерпретувати, тобто чітко визначити його фізичний смисл.

І, нарешті, по-третє, при такому підході до оцінювання ефективності управління військами критерій, що застосовується, не має прямого зв'язку з кінцевою метою операції (бойових дій). І це головний недолік, бо створення системи управління військами, навіть самої досконалої – не самоціль, а лише засіб, призначений для забезпечення ефективного виконання завдань операції (бойових дій).

*Підхід 5.* Аналіз циклу управління, який створюється системою управління, показує, що в цьому процесі чітко проявляються чотири головних етапи:

збір інформації (даних) та оцінювання обстановки;

вироблення замислу і формулювання рішення; доведення завдань до підлеглих військових частин і підрозділів;

контроль виконання поставлених завдань.

Якщо розглядати, що кожен етап-цикл реалізує своєрідна підсистема, то рішення завдання по визначенню ефективності функціонування системи управління можна звести, у кінцевому результаті, до оцінювання ефективності реалізації кожного зі згаданих етапів циклу управління, тобто ефективності функціонування підсистем – збору інформації (даних) та оцінювання обстановки; вироблення замислу і формулювання рішення; доведення завдань до підлеглих військових частин і підрозділів; контролю виконання поставлених завдань.

У такому випадку ефективність функціонування системи управління буде визначатися виразом (5).

$$\begin{cases} E_{cy} = f(E_{СИ}; E_{ВР}; E_{ДЗ}; E_{К}) \\ E_{cy} \geq E_{cy}^{потр} \end{cases} \quad (5)$$

де:  $E_{cy}$  – ефективність функціонування системи управління військами;

$E_{СИ}$  – ефективність функціонування підсистеми збору інформації;

$E_{ВР}$  – ефективність функціонування підсистеми вироблення рішення;

$E_{ДЗ}$  – ефективність функціонування підсистеми доведення завдань до підлеглих;

$E_{К}$  – ефективність функціонування підсистеми контролю;

$E_{cy}^{потр}$  – потрібний рівень ефективності функціонування системи управління військами.

У подальшому як критерій ефективності використовується або критерій максимального результату (коли вирішується завдання максимізації рівня ефективності управління)  $K_y = K_{y_{max}}$ , або критерій придатності (коли вирішується завдання досягнення потрібного рівня ефективності управління)  $K_y \geq K_{потр}$ , де  $K_{потр}$  – потрібний рівень ефективності управління військами.

*Підхід 6.* Виходячи з визначення, що система управління військами – це сукупність функціонально і ієрархічно пов'язаних між собою підсистем органів управління, пунктів управління та системи зв'язку і АСУ, стає можливим запропонувати ще один підхід до оцінювання її ефективності.

Оцінювання ефективності системи управління в цілому можна визначити як ефективність функціонування її складових підсистем. При цьому слід мати на увазі, що загальна ефективність системи управління не є простою сумою ефективності її елементів, вона буде мати вигляд (6):

$$\begin{cases} E_{cy} = f(E_{COY}; E_{СПУ}; E_{СЗ}) \\ E_{cy} \geq E_{cy}^{потр} \end{cases} \quad (6)$$

де  $E_{cy}$  – ефективність функціонування системи управління військами;

$E_{COY}$  – ефективність функціонування підсистеми органів управління;

$E_{СПУ}$  – ефективність функціонування підсистеми пунктів управління;

$E_{СЗ}$  – ефективність функціонування підсистеми зв'язку та АСУ;

$E_{cy}^{потр}$  – потрібний рівень ефективності функціонування системи управління військами.

Усі наведені вище підходи досить прості, складність полягає у визначенні (знаходженні) значень часткових показників (складових) ефективності функціонування системи управління військами. Твердження “чим краще функціонує система управління військами, тим вище ефективність ведення операції (бойових дій)” в принципі може бути правильним. Але, в ньому міститься велика невизначеність, так як успіх операції (бойових дій) військ буде залежати



великою мірою від протидії (впливу) противника, стану, оперативних (бойових) можливостей підлеглих військ, а також їх бойової готовності.

Саме тому, завдання щодо визначення кількісного внеску системи управління військами в досягнення кінцевої мети операції є складною і важливою одночасно. Ефективність функціонування будь-якої системи може (повинна) мати кількісну міру і виражатися числом. При цьому, для прийняття рішень командувачу дуже важливо мати методіку оцінювання ефективності системи управління, яка має чітко характеризувати стан системи управління.

У тих випадках, коли побудову аналітичної моделі операції (бойових дій) важко здійснити, застосовується інший, імітаційний метод моделювання, відомий під назвою методу статистичних випробувань чи методу Монте-Карло. Його ідея полягає у наступному. Замість опису випадкових подій, які у сукупності характеризують операцію (бойові дії) математичними залежностями проводиться розіграш-моделювання випадкових подій за допомогою деякої процедури, яка дає випадковий результат (наприклад, датчика випадкових чисел). При цьому параметри, що цікавлять, задаються певним діапазоном значень. У результаті розіграшу отримується одна реалізація результату операції (бойових дій). Здійснивши такий розіграш

велику кількість разів, отримуємо статистичний матеріал – множину результатів реалізації операції (бойових дій), який для визначення показників ефективності обробляється звичайними методами математичної статистики.

### Висновки й перспективи подальших досліджень

З викладеного зрозуміло, що цілям дослідження процесів, які проходять під час підготовки і у ході ведення операції (бойових дій), найбільш підходять імітаційні моделі.

У випадках, коли відсутня ретроспектива і для оцінювання ефективності управління військами немає можливості застосувати методи моделювання, використовується метод експертних оцінок. Сутність його полягає у тому, що необхідне рішення приймається на основі оцінки досвідчених в цій області людей – експертів. При цьому оцінки експертів певним чином формалізуються і обробляються спеціальними методами.

Отже, завдання удосконалення існуючого науково-методичного апарату оцінювання ефективності управління військами залишається актуальним завданням, необхідність вирішення якого диктується нагальними потребами теорії і практики управління військами.

### Література

1. Алтухов П.К. Основы теории управления войсками. Москва: Воениздат, 1984. 221 с. 2. A.Lobanov, A.Loishyn; I. Tkach, I. Liashenko, A. Zinchenko. Research of main international approaches for risk management process's standardization in the context of internal control standardization in the Armed Forces of Ukraine and providing national security. *Revista ESPACIOS*. Vol. 40 (Number 20) Year 2019. Page 14. 3. Скрите управління військами: навч. посіб. / О.Я. Зубов; В.С.Безбах та ін. Київ: НУОУ, 2017. 72 с. 4. Лобанов А.А., Зубов О.Я. Науково-методичні засади оцінювання та аналізу управлінських рішень прийнятих під час заходів оперативної підготовки. *Труди*

*університету: збірник наукових праць Національного університету оборони України імені Івана Черняховського*. 2018. № 5 (150). С. 97–106. 5. Лобанов А.А., Ролін І. Ф., Марущенко В. В. Управління як функція ведення воєнних дій силами оборони України. *Наука і оборона*. 2019. № 1. С. 9–15. 6. Оцінювання та порівняння рішень сторін у двосторонніх командно-штабних навчаннях (воєнних іграх): навч. посіб. / О.Я. Зубов; В.С. Безбах, Р.Ф. Факадей, А.А. Лобанов. Київ: НУОУ, , 2018. 83 с. 7. Гайдес М.А. Общая теория систем. Системы и системный анализ. Винница: Глобус-Пресс. 2004. 430 с.

## К ОЦЕНКЕ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ВОЙСКАМИ (СИЛАМИ)

*Анатолій Анатольевич Лобанов (доктор военных наук, профессор)*

*Руслан Анатольевич Мозговой (кандидат военных наук)*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*Военная наука всегда рассматривала наличие устойчивого и непрерывного управления войсками (силами) как одну из решающих условий победы, подчеркивала его особую роль в достижении успеха в операциях. Исходя из этого, на протяжении многовековой истории военного искусства особое значение придавалось развитию органов, средств и методов руководства Вооруженными Силами и управлению войсками. Так же и в современных условиях, как в теории, так и в практической подготовке войск (сил), вопросы управления занимали и будут занимать одно из важнейших мест. Военные специалисты*

ведущих стран считают, что четко организованное управление войсками (силами) может оказать существенную преимущество в ходе их применения.

В статье рассматриваются методы оценки эффективности управления войсками в зависимости от случайных факторов и способ математического описания процесса управления. Предложенные методы оценки дают возможность получить более объективную и адекватную оценку эффективности управления войсками (силами) при учете различных частных показателей.

**Ключевые слова:** модель, метод, система управления, эффективность.

## TO EVALUATE THE EFFECTIVENESS OF THE ARMY (FORCE) MANAGEMENT

*Anatolii Lobanov (Doctor of Military Sciences, Professor)*

*Ruslan Mozghovyi (Candidate of Military Sciences)*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

Military science has always considered the existence of a steady and continuous command of troops (forces) as one of the decisive conditions for victory, emphasizing its special role in achieving success in operations. On this basis, throughout the centuries-old history of martial arts, special emphasis has been placed on the development of the organs, means, and methods of commanding and controlling the Armed Forces. Similarly, in modern conditions, both in theory and in the practical training of troops (forces), management issues have occupied and will occupy one of the most important places. Leading military experts believe that a well-organized command of forces (forces) can provide a significant advantage in the course of their deployment.

The article discusses methods of assessing the effectiveness of military control depending on random factors and a method for mathematically describing the control process. The proposed assessment methods make it possible to obtain a more objective and adequate assessment of the effectiveness of military (force) management, taking into account various partial indicators.

**Key words:** model, method, control system, efficiency.

### References

1. Altukhov P.K. Основы теории управления войсками. Москва: Воениздат, 1984. 221 с.
2. A.Lobanov, A.Loishyn; I. Tkach, I. Liashenko, A. Zinchenko. Research of main international approaches for risk management process's standardization in the context of internal control standardization in the Armed Forces of Ukraine and providing national security. *Revista ESPACIOS*. Vol. 40 (Number 20) Year 2019. Page 14.
3. Skryte upravlinnja vijskamy: navch. posib. / O.Ja Zubov; V.S.Bezbakh ta in. Kyjiv: NUOU, 2017. 72 s.
4. Lobanov A.A., Zubov O.Ja. Naukovo-metodychni zasady ocinjuvannja ta analizu upravlinsjkykh rishenj pryjnjatjykh pid chas zakhodiv operatyvnoji pidghotovky. Trudy universytetu: zbirnyk naukovykh pracj Nacionaljnogho universytetu oborony Ukrainy imeni Ivana Chernjakhovskogho. 2018. # 5 (150). S. 97–106.
5. Lobanov A.A., Rolin I. F., Marushhenko V. V. Upravlinnja jak funkcija vedennja vojennykh dij sylamy oborony Ukrainy. *Nauka i oborona*. 2019. № 1. S. 9–15.
6. Ocinjuvannja ta porivnjannja rishenj storin u dvostoronnikh komandno-shtabnykh navchannjakh (vojennykh ighrakh): navch. posib. / O.Ja Zubov; V.S. Bezbakh, R.F. Fakadej, A.A. Lobanov. Kyjiv: NUOU, , 2018. 83 s.
7. Haides M.A. Obshchaia teoriya system. Systemy y systemnyy analiz. Vynnytsa: Hlobus-Press. 2004. 430 s.

## УДОСКОНАЛЕНИЙ МЕТОД РОЗРАХУНКУ ПРОПУСКНОЇ СПРОМОЖНОСТІ СИСТЕМИ ЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НА ІНФОРМАЦІЙНИХ НАПРЯМКАХ

Одним з найбільш актуальних наукових завдань у галузі військового управління під час ведення операції для системи зв'язку спеціального призначення є передавання інформації в режимі реального часу з дотриманням низки вимог щодо якості обслуговування. Це пов'язано із тим, що множина потоків даних передається по мережі, ресурси якої необхідно розподілити між цими потоками за певною пропорцією.

Оскільки дані, які підлягають передаванню, різні за своєю природою та важливістю, то необхідно мати механізми, які дають змогу розв'язувати задачу розподілу ресурсів оперативно, у відповідності до властивостей тих потоків, які передаються у конкретний момент часу через конкретні вузли спеціального призначення. Такі механізми для органів планування системи зв'язку спеціального призначення повинні базуватись на удосконалених методах розподілу ресурсів, що мають високу масштабованість, швидкодію, гнучкість, низьку операційну складність та ресурсоемність.

**Ключові слова:** система зв'язку спеціального призначення; система управління; інформаційний напрямок; інформаційна система; канал зв'язку; пропускна спроможність; автоматизована система управління.

### Вступ

**Постановка проблеми.** Роботи, які присвячені методам оцінки пропускної спроможності, здебільшого, носять теоретичний характер та спрямовані на створення нових алгоритмів управління потоками інформації, що робить їх важко реалізованими в реальній системі зв'язку спеціального призначення. Іншим недоліком існуючих методів є використання комплексного підходу до оцінювання пропускної спроможності інформаційних напрямків без урахування особливостей кожного типу трафіку, що генерується різними мережевими додатками.

Зменшення затримок в обслуговуванні інформаційних потоків частково досягається шляхом вдосконалення технічної складової наприклад використанням обладнання з більшим об'ємом буферної пам'яті, але цей підхід є неприйнятним при передаванні інформації в режимі реального часу.

**Аналіз останніх досліджень і публікацій.** При створенні систем зв'язку спеціального призначення нового покоління виникає проблема розрахунку пропускної спроможності. Існуючий науково-методичний апарат визначення пропускної спроможності системи спеціального призначення за наведеним показником застарів [1], розроблений ще за часів СРСР, орієнтований на застосування аналогових засобів зв'язку. На практиці при визначенні пропускної спроможності використовують математичне моделювання, або, без належного обґрунтування, традиційні формули теорії розподілення інформації [2-5]. Аналітичне вирішення для технологій нового покоління, запропонованих в [6], надзвичайно громіздкі і практично не застосовуються. Загальноприйнятого аналітичного або інженерного способу вирішення проблеми для систем спеціального призначення на сьогодні немає. Такий стан речей в подальшому може привести до зниження ефективності оперативного планування

системи спеціального призначення в процесі управління військами (силами)

**Мета статті.** Удосконалити метод розрахунку пропускної спроможності системи спеціального призначення на інформаційних напрямках для оперативності процесу планування системи зв'язку спеціального призначення.

### Виклад основного матеріалу дослідження

Показником ефективності, який найбільш повно характеризує систему зв'язку спеціального призначення з точки зору виконання покладених на неї завдань, є виконане навантаження, яке оцінюється як за напрямками зв'язку, так і у всій мережі в цілому. У той же час різко збільшилася кількість інформації необхідної для здійснення управління військами. Для доставки інформації широко використовуються сучасні телекомунікаційні сервіси (IP-телефонія, передача даних, IP-відеозв'язок, тощо), що призводить до підвищення вимог до обсягу і якості транспортної мережі передачі даних та часто призводить до невиправдано високих витрат на використання устаткування із завищеними вимогами до його технічних характеристик, утримання не потрібного обладнання та особового складу, надлишкову оренду цифрового ресурсу з телекомунікаційної мережі загального користування. При розгортанні вузів спеціального призначення (ВСП) в інтересах органів управління необхідно враховувати різноманітні джерела трафіку, що циркулює у мережі C4ISR (Command, Control, Communication and Computers System upgrade): інформаційний обмін між базами даних, файловий документообіг, IP-телефонію і IP-відеозв'язок, інформації від сенсорної мережі тощо. Кожен вид трафіку пред'являє свої вимоги до якості транспортної мережі та показника пропускної спроможності. У той же час для розрахунку пропускної спроможності мережі широко використовується примітивний метод, заснований на

простому арифметичному підсумовуванні потоків даних від різних джерел з урахуванням емпіричного «коефіцієнта вибухового трафіку» [7]. При цьому відбувається підсумовування пропускної спроможності ліній зв'язку знизу до гори відповідно до структури типу «дерево» без кореневої гілки [1,3], що відповідає структурі системи управління.

Запропонована у [7] методика призначена для роботи органів управління зв'язком для вибору найбільш оптимального (раціонального) варіанту розгортання системи зв'язку спеціального призначення, що планується. При цьому вважається, що система зв'язку спеціального призначення будується з використанням цифрових каналів та мереж та має деревоподібну структуру.

Вихідними даними для розрахунку пропускної спроможності в такому випадку повинні бути: пропускні спроможності всіх каналів зв'язку первинної мережі (ліній зв'язку та прив'язки) на інформаційних напрямках; мінімально необхідні пропускні спроможності для роботи кінцевих засобів (телефон, передача даних, відеоконференцзв'язок) зв'язку та їх кількість на пункті управління.

Кількісним показником оцінки пропускної спроможності системи зв'язку є швидкість передачі даних в каналах (лініях) зв'язку, що забезпечує визначений перелік інформаційних послуг (сервісів) із заданою якістю зв'язку. У свою чергу, якість зв'язку досягається забезпеченням мінімально необхідної пропускної спроможності, що забезпечить функціонування певної послуги (сервісу).

В основі методу закладена оцінка пропускної спроможності цифрових каналів та мереж. При цьому використовується метод декомпозиції: вся система зв'язку спеціального призначення у розбивається на інформаційні напрямки від старшого ВСП (в інтересах якого здійснюється оцінка системи) до підлеглих ВСП. Розрахункам підлягають всі інформаційні напрямки, а висновок щодо їх функціонування робиться окремо.

Пропускна спроможність цифрових мереж (каналів) на інформаційних напрямках повинна забезпечувати інформаційний обмін всіх користувачів телекомунікаційних сервісів, які використовують даний канал (під сервісами розуміється телефонія, передача даних від АРМ, відеоконференцзв'язок). Вимоги щодо забезпечення необхідної (заданої) якості зв'язку виконуються у випадку підтримання мінімальної швидкості передачі інформації для даного сервісу.

Наведемо запропонований метод аналітичними виразами, що не зроблено у [7]. Врахуємо наявність на пунктах управління декількох мереж передачі даних. Це мережі – мережа відкритої інформації, мережа обміну службовою інформацією та захищена система обміну інформацією. Значення пропускної спроможності для певного сервісу визначається як добуток середнього значення швидкості передачі даних кожного із сервісів та кількості терміналів (робочих місць) кожного сервісу. Сумарна пропускна спроможність  $C_{необх}$  буде мати вигляд:

$$C_{необх} = \sum_{i=1}^I k_i C_i + \sum_{j=1}^J k_j C_j + \sum_{y=1}^Y k_y C_y + \sum_{r=1}^R k_r C_r \quad (1)$$

де:  $C_i$  – середнє значення швидкості передачі даних  $i$ -го сервісу VoIP телефонії;

$C_j$  – середнє значення швидкості передачі даних

$j$ -го сервісу відеоконференц зв'язку;

$C_y$  – середнє значення швидкості передачі даних

$y$ - електронної пошти;

$C_r$  – середнє значення швидкості передачі даних

$r$ -з камер відео спостереження;

$k_i$  – кількості терміналів (робочих місць) сервісів VoIP телефонії;

$k_j$  – кількості терміналів (робочих місць) сервісів відеоконференц зв'язку;

$k_y$  – кількості терміналів (робочих місць) сервісів електронної пошти;

$k_r$  – кількості терміналів (робочих місць) сервісів відео спостереження.

Наведений вираз буде справедливим при використанні стандартизованих швидкостей передачі даних для кожного із сервісів, що забезпечується на пункті управління. Проте, застосування стандартизованих швидкостей описує ідеальний випадок та буде рідко зустрічатися на практиці. Тому доцільно перейти до підсумовування різних швидкостей передачі даних для кожного із сервісів:

$$C_{необх} = \sum_{i=1}^I \sum_{k_i=1}^{K_i} C_i + \sum_{j=1}^J \sum_{k_j=1}^{K_j} C_j + \sum_{y=1}^Y \sum_{k_y=1}^{K_y} C_y + \sum_{r=1}^R \sum_{k_r=1}^{K_r} C_r, \quad (2)$$

де:  $k_i = 1 \dots K_i$  – кількості терміналів

(робочих місць) сервісів VoIP телефонії;

$k_j = 1 \dots K_j$  – кількості терміналів

(робочих місць) сервісів відеоконференцзв'язку;

$i = 1 \dots I$  – кількість сервісів VoIP телефонії;

$j = 1 \dots J$  – кількість сервісів відеоконференц зв'язку;

$y = 1 \dots Y$  – кількість сервісів електронної пошти;

$r = 1 \dots R$  – кількість сервісів відео спостереження;

$C_i$  – значення швидкості передачі даних  $i$ -го сервісу VoIP телефонії;

$C_j$  – значення швидкості передачі даних  $j$ -го сервісу відеоконференц зв'язку;

$C_y$  – значення швидкості передачі даних  $y$ -го сервісу електронної пошти;

$C_r$  – значення швидкості передачі даних  $r$ -го сервісу відео спостереження.

Запропонований підхід, також не є досконалим, та потребує подальшого удосконалення за рахунок введення у вирази (1), (2) пропускних спроможностей необхідних для сталого функціонування інформаційних систем, автоматизованих систем управління та сенсорних мереж. З урахуванням запропонованого вираз (1) можливо переписати до вигляду:

$$C_{необх} = \sum_{i=1}^I k_i C_i + \sum_{j=1}^J k_j C_j + \sum_{y=1}^Y k_y C_y + \sum_{r=1}^R k_r C_r + \sum_{f=1}^F k_f C_f + \sum_{g=1}^G k_g C_g + \sum_{h=1}^H k_h C_h. \quad (3)$$

де  $C_i$  – середнє значення швидкості передачі даних сервісу VoIP телефонії;

$C_j$  – середнє значення швидкості передачі даних відеоконференц зв'язку;

$C_y$  – середнє значення швидкості передачі даних електронної пошти;

$C_r$  – середнє значення швидкості передачі даних з камер відео спостереження;

$C_f$  – середнє значення швидкості передачі даних в інформаційній системі;

$C_g$  – середнє значення швидкості передачі даних в автоматизованій системі управління;

$C_h$  – середнє значення швидкості передачі даних у сенсорній мережі.

Наведений вираз не у повній мірі відображає реальний стан справ. На практиці не можлива ситуація коли значення пропускної спроможності для інформаційних систем, автоматизованих систем управління та сенсорних мереж будуть однаковими. Тому доцільно перейти до виразу (2) та записати його у вигляді виразу:

$$C_{\text{необх}} = \sum_{i=1}^I \sum_{k_i=1}^{K_i} C_i + \sum_{j=1}^J \sum_{k_j=1}^{K_j} C_j + \sum_{y=1}^Y \sum_{k_y=1}^{K_y} C_y + \sum_{r=1}^R \sum_{k_r=1}^{K_r} C_r + \sum_{f=1}^F \sum_{k_f=1}^{K_f} k_f C_f + \sum_{g=1}^G \sum_{k_g=1}^{K_g} k_g C_g + \sum_{h=1}^H \sum_{k_h=1}^{K_h} k_h C_h. \quad (4)$$

де:  $C_i$  – значення швидкості передачі даних  $i$ -го сервісу VoIP телефонії;

$C_j$  – значення швидкості передачі даних  $j$ -го сервісу відеоконференц зв'язку;

$C_y$  – значення швидкості передачі даних  $y$ -го сервісу електронної пошти;

$C_r$  – значення швидкості передачі даних  $r$ -го сервісу відео спостереження.

$C_f$  – значення швидкості передачі даних в  $f$ -ній інформаційній системі;

$C_g$  – значення швидкості передачі даних в  $g$ -ій автоматизованій системі управління;

$C_h$  – значення швидкості передачі даних у  $h$ -ій сенсорній мережі.

Запропонований підхід не надає уявлення про загальну пропускну спроможність мережі і розрахований на отримання сумарної швидкості передачі всіх абонентських пристроїв на пункті управління. При цьому сенсорні мережі розглядаються як кінцеві пристрої віртуально розміщені на пункті управління. Вирази (1 – 4) можливо застосувати лише для визначення пропускної спроможності ВСП найнижчої ланки управління, який не має подальших з'єднань вниз. Фізично – це пропускну спроможність маршрутизатора ВСП пункту управління.

Відповідно до методу [7], пропускну спроможність лінії зв'язку, що поєднує ВСП нижчої ланки управління з вищим вузлом повинна відповідати виразу:

$$C_{\text{ЛЗ}} \geq 1,2 C_{\text{необх}}. \quad (5)$$

Виразом (5) передбачається 20-ти відсоткове резервування пропускної спроможності лінії зв'язку порівняно з розрахунковою пропускнуною спроможністю ВСП.

Пропускна спроможність наступного у системі ієрархії ВСП буде складатися як сума пропускної спроможності абонентських пристроїв ВСП та ліній прямого зв'язку, які до нього підключені від нижчої ланки управління. У випадку, що описується, буде мати місце паралельне з'єднання ВСП. Відповідно [7], сумарна пропускна спроможність буде мати вираз:

$$C_{\sum \text{ЛЗ}} = \sum_{s=1}^S C_{\text{ЛЗ} s}. \quad (6)$$

де  $s=1, \dots, S$  – лінії зв'язку від нижчих пунктів управління.

Таким чином, пропускна спроможність ВСП ротного опорного пункту буде виглядати як сума пропускної спроможності абонентських пристроїв ВСП та трьох ліній зв'язку з підлеглими взводними опорними пунктами:

$$C = \sum_{i=1}^I \sum_{k_i=1}^{K_i} C_i + \sum_{j=1}^J \sum_{k_j=1}^{K_j} C_j + \sum_{y=1}^Y \sum_{k_y=1}^{K_y} C_y + \sum_{r=1}^R \sum_{k_r=1}^{K_r} C_r + \sum_{f=1}^F \sum_{k_f=1}^{K_f} k_f C_f + \sum_{g=1}^G \sum_{k_g=1}^{K_g} k_g C_g + \sum_{h=1}^H \sum_{k_h=1}^{K_h} k_h C_h + \sum_{s=1}^S C_{\text{ЛЗ} s}. \quad (7)$$

Для спрощення аналітичних виразів та формалізації методу визначення пропускної спроможності введемо алгоритм розрахунку пропускної спроможності. На першому етапі проводиться розрахунок пропускної спроможності ВСП пунктів управління за встановленими абонентськими пристроями на робочих місцях посадових осіб та наданими сервісами. На наступних етапах необхідно підсумовувати пропускну спроможність ВСП пунктів управління з урахуванням кількості підключених ліній прямого зв'язку від нижчих пунктів управління.

### Висновки й перспективи подальших досліджень

Наведений удосконалений метод розрахунку пропускної спроможності дозволяє здійснювати оцінку системи зв'язку спеціального призначення під час оперативного планування.

Відрізняється від відомих урахуванням використання цифрових мереж (каналів) та простотою використання, що дозволяє використовувати її для оперативного планування системи зв'язку спеціального призначення.

Удосконалений метод розрахунку пропускної спроможності системи зв'язку спеціального призначення показав, що напрямком подальшого дослідження є удосконалення науково-методичного апарату з питань оцінки ефективності функціонування системи зв'язку спеціального призначення за пропускнуною спроможністю.

Подальші дослідження будуть направлені на розробку методів (методик) удосконалення процесу оперативного планування систем зв'язку спеціального призначення.

### Література

1. **Методики** по расчету и оценке полевых систем связи // Курс лекций. – Л.: ВАС, 1985. 2. **Корнишев Ю.Н.** Теория розподілення інформації / Ю.Н. Корнишев, Г.Л.Фань – СПб.: ХВ-Петербург, 2005. – 288 с. 3. **Боговик А. В.** Эффективность систем военной связи и методы ее оценки / А. В. Боговик, В. В. Игнатов – СПб.: ВАС, 2006. – 183 с. 4. **Величко В.В.** Телекоммуникационные системы и сети / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев. – Т. 3. Мультисервисные сети. – М.: Горячая линия – Телеком, 2005. – 592 с. 5. **Шнепс М.А.** Системы

распределения информации. Методы расчета: Справочное пособие. М.:Связь, 1979. – 312 с. 6. **Ершов В.А.** Метод расчета пропускной способности звена Ш-ЦСИС с технологией АТМ при мультисервисном обслуживании / В.А. Ершов, Э.Б. Ершова, В.В. Ковалев // Электросвязь. – 2000. – № 3. – С. 20-23. 7. **Остапчук В.М.** Методика оцінки пропускної спроможності як характеристики системи військового зв'язку/ В.М. Остапчук, С.І. Фараон, Л.О. Бондаренко Сучасні інформаційні технології у сфері безпеки та оборони. – 2018. – №1(31). – С. 81 – 84.

## УСОВЕРШЕНСТВОВАННЫЙ МЕТОД РАСЧЕТА ПРОПУСКНОЙ СПОСОБНОСТИ СИСТЕМЫ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ НА ИНФОРМАЦИОННЫХ НАПРАВЛЕНИЯХ

*Александр Николаевич Нестеров*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*Одним из наиболее актуальных научных задач в области военного управления при ведении операции для системы связи специального назначения является передача информации в режиме реального времени с соблюдением ряда требований к качеству обслуживания. Это связано с тем, что множество потоков данных передается по сети, ресурсы которой необходимо распределить между этими потоками по определенной пропорции.*

*Поскольку данные, которые подлежат передаче, различные по своей природе и важности, то необходимо иметь механизмы, которые позволяют решать задачу распределения ресурсов оперативно, в соответствии с свойств тех потоков, которые передаются в конкретный момент времени через конкретные узлы специального назначения. Такие механизмы для органов планирования системы связи специального назначения должны базироваться на усовершенствованных методах распределения ресурсов, имеющих высокую масштабируемость, быстродействие, гибкость, низкую операционную сложность и ресурсоемкость.*

**Ключевые слова:** *система связи специального назначения; система управления; информационное направление; информационная система; канал связи; пропускная способность; автоматизированная система управления.*

## THE ENHANCED METHOD OF CAPACITY COMPUTATION FOR THE SPECIAL-FORCES COMMUNICATION SYSTEM IN INFORMATION DIRECTIONS

*Oleksandr Nesterov*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*One of the most actual scientific challenges in the area of military command while conducting an operation for the special-purpose communication system is the real-time data transmission in accordance with requirements for the service quality standards. This is because a great number of data flows are transmitted through the network, whose resource has to be apportioned between those flows.*

*As the data to be transmitted differ in their nature and significance the mechanisms are necessary which should solve the problem of allocating the resource promptly and in accordance with characteristics of the data flows being transmitted at a specific point of time through the specific special-purpose nodes. Such mechanisms for the authorities planning the special-purpose communications systems have to be based on the enhances methods of resource allocation having high-degree scalability, operating speed, flexibility, low operating complexity and resource intensity.*

**Keywords:** *special-purpose communication system, control (command) system. Information direction, information system, channel communication, capacity, automated control system.*

### References

1. **Methods** for calculating and evaluating field communication systems // Course of lectures. - L.: YOU, 1985. 2. **Kornishev Yu.N.** Theory of Information and Information / Yu.N. Kornishev, G.L. Fan - St. Petersburg: HV-Petersburg, 2005. -- 288 p. 3. **Bogovik A. V.** The effectiveness of military communications systems and methods for its evaluation / A. V. Bogovik, V. V. Ignatov - St. Petersburg: VAS, 2006. - 183 p. 4. **Velichko V.V.** Telecommunication systems and networks / V.V. Velichko, E.A. Subbotin, V.P. Shuvalov, A.F. Yaroslavtsev. - T. 3. Multiservice networks. - M.: Hot line - Telecom, 2005. - 592 p. 5. **Shneps**

**M.A.** Information distribution systems. Calculation methods: Reference manual. M.: Communication, 1979.- 312 p. 6. **Ershov V.A.** The method for calculating the bandwidth of the Sh-ISDN link with ATM technology for multiservice service / V.A. Ershov, E.B. Ershova, V.V. Kovalev // Telecommunication. - 2000. - No. 3. - S. 20-23. 7. **Ostapchuk V.M.** Methodology for assessing throughput capacities as a characteristic of a system of voice feedback / V.M. Ostapchuk, S.I. Pharaoh, L.O. Bondarenko Advanced Information Technology in the field of security and defense. - 2018. - No. 1 (31). S. 81-84.

## ПІДХІД ЩОДО ОЦІНЮВАННЯ НАДІЙНОСТІ ФУНКЦІОНУВАННЯ ПІДСИСТЕМИ ПЕРЕДАЧІ ДАНИХ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ АВІАЦІЄЮ ТА ПРОТИПОВІТРЯНОЇ ОБОРОНОЮ

*В статті запропоновано підхід щодо оцінювання надійності функціонування підсистеми передачі даних автоматизованої системи управління авіацією та протиповітряною обороною, який ґрунтується на використанні методу мінімальних шляхів і мінімальних перетинів.*

*Крім того, розглянуті математичні методики оцінювання надійності інформаційних систем, що можуть бути використані при оцінюванні надійності підсистеми передачі даних автоматизованої системи управління авіацією та протиповітряною обороною. Наведено підхід оцінювання надійності варіанту структури автоматизованої системи управління авіацією та протиповітряною обороною.*

**Ключові слова:** надійність; підсистема передачі даних; метод мінімальних шляхів і перетинів.

### Вступ

Автоматизована система управління авіацією та протиповітряною обороною (далі – АСУ авіацією та ППО), як складова частина Єдиної автоматизованої системи управління Збройними Силами України, функціонує на базі підсистеми передачі даних (далі – ПСПД), до складу якої входять канали та засоби зв'язку. Дана підсистема є складним програмно-апаратним об'єктом із розгалуженою інфраструктурою і великим числом вузлів і абонентів. В даний час роль підсистеми передачі даних АСУ авіації та ППО виконує стаціонарна телекомунікаційна мережа Повітряних Сил Збройних Сил України, яка постійно модернізується і розширюється. Від того, наскільки надійно працює зазначена підсистема, залежить надійність функціонування АСУ авіації та ППО в цілому.

**Постановка проблеми.** Досвід дослідної експлуатації, а також проведення навчання свідчать, що на даний час відмічається ненадійна робота ПСПД АСУ авіацією та ППО. При розрахунку надійності такої територіально-розподіленої АСУ, як АСУ авіації та ППО, необхідно враховувати надійності каналів зв'язку, технічних та програмних засобів, що відносяться до ПСПД. Так, в [1] розглянуто підхід щодо оцінювання надійності функціонування технічних та програмних засобів АСУ авіації та ППО. Актуальним стає питання оцінювання надійності функціонування ПСПД зазначеної АСУ, що, в свою чергу, потребує розроблення відповідного науково-методичного апарату.

**Аналіз останніх досліджень і публікацій.** На сторінках наукових видань неодноразово висвітлювались різні моделі та методики щодо оцінювання надійності функціонування автоматизованих систем управління. Так, в [2, 3] запропоновано методологію оцінювання АСУ з урахуванням показників надійності комплексів технічних засобів (ТЗ), програмного забезпечення (ПЗ), а також відмови, які виникають з вини оперативного персоналу (ОП), але дані підходи не

враховують відмови ПСПД. В [4] представлена методика оцінювання надійності трактів передачі даних з врахуванням реальних умов функціонування апаратури, проте поза увагою авторів залишилася розподіленість АСУ.

Проведений аналіз існуючого науково-методичного апарату показав, що існуючі методики або не охоплюють всіх складових сучасних ПСПД або не враховують особливості її побудови та функціонування, які в теперішній умовах суттєво впливають на надійність функціонування ПСПД АСУ авіацією та ППО.

**Метою статті** є розробка часткової методики оцінювання надійності функціонування ПСПД, що може бути застосована при оцінюванні надійності функціонування сучасної АСУ авіації та ППО в цілому

### Виклад основного матеріалу дослідження

Під надійністю ПСПД в дослідженні розуміється властивість підсистеми зберігати у часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції у визначених режимах та умовах застосування, технічного обслуговування, зберігання та транспортування [5].

Відомо що, ПСПД АСУ авіації та ППО є багатофункціональною, оскільки здійснює обмін інформацією між багатьма територіально роз'єднаними КЗА. Вона має складну мережеву структуру. Зв'язок між окремими КЗА може здійснюватися за декількома можливими інформаційним напрямками, включаючи транзит по цілому ряду вузлів ПСПД.

Можливий варіант побудови ПСПД АСУ авіацією та ППО з інформаційними напрямками при трирівневій системі управління показано на рис 1. Для оцінювання ПСПД слід розглядати як граф, в якому вершинами є КЗА, а ребрами є

інформаційні напрямки між даними КЗА.

АСУ авіацією та протиповітряною обороною є надзвичайно складною територіально-розподіленою багатофункціональною системою, яка включає в себе багатоцільові комплекси засобів автоматизації (КЗА): “Ореанда-Центр”, “Ореанда-ЗРБ”, “Ореанда-Авіа”, “Ореанда-РТВ”, “Ореанда-РТВ-1”, Ореанда-Р і РЕБ” різних модифікацій, що пов’язані між собою ПСПД.

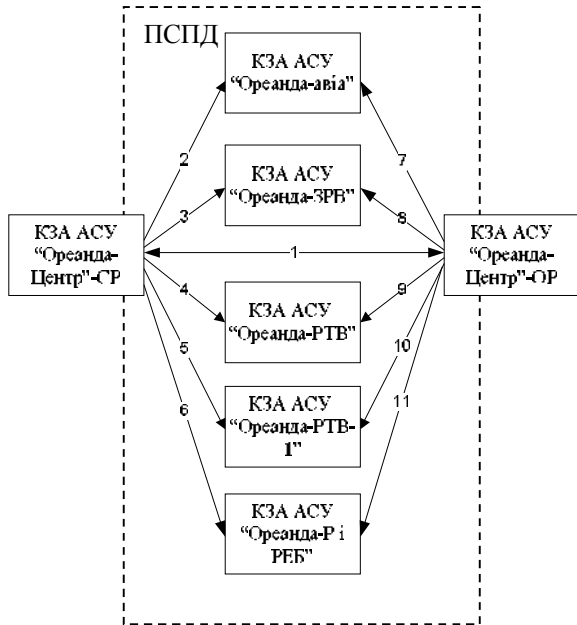


Рис. 1 Структурна схема можливого варіанта функціонування ПСПД АСУ авіацією та ППО при тривірневій системі управління.

Для оцінювання надійності ПСПД АСУ авіації та ППО в дослідженні використовується ймовірність відмови  $Q_{\text{відм}}$ . Оскільки відмова і безвідмовна робота є подіями неспільними і протилежними, то між їх ймовірностями справедливе таке співвідношення:

$$Q_{\text{відм}} = 1 - P_{\text{прац}}, \quad (1)$$

де:  $P_{\text{прац}}$  – ймовірність безвідмовної роботи ПСПД.

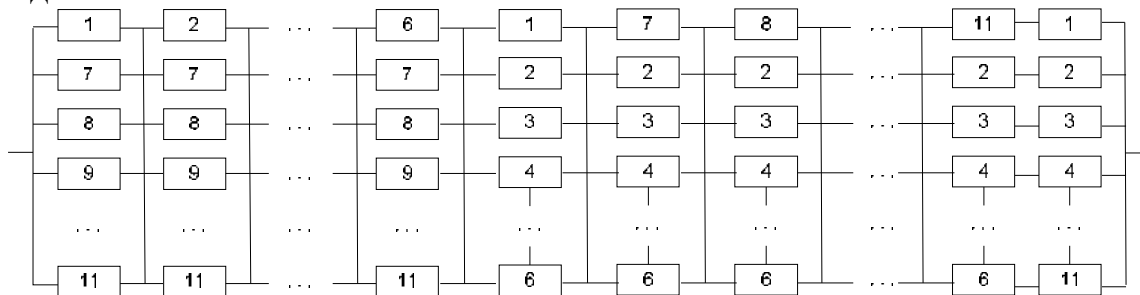


Рис. 3. Паралельно-послідовна, що побудована методом мінімальних перетинів

У схемах на рис. 2 та 3 однойменні елементи вважаються незалежними, хоча, фактично, це одні і ті ж елементи. Оцінка надійності, що отримана методом мінімальних шляхів, є оцінкою зверху, а отримана методом мінімальних перетинів – знизу. Для високонадійних інформаційних систем оцінка за мінімальними перетинами йде “в запас” і має

Для розрахунку надійності функціонування ПСПД АСУ авіації та ППО в будь-який момент часу застосовують теорію систем масового обслуговування, марковских процесів, теорію графів тощо. У зв’язку з цим моделлю надійності функціонування ПСПД настільки складна, що оцінити надійність можна тільки методом повного перебору можливих станів інформаційних напрямків. Такий підхід навіть для порівняно невеликих ПСПД є громіздким.

Тому під час оцінювання надійності ПСПД АСУ авіації та ППО пропонується використовувати метод мінімальних шляхів і мінімальних перетинів (метод Езар - Прошана) [6].

Суть методу полягає в тому, що система з довільною структурою приводиться до послідовно-паралельної схеми мінімальних шляхів або до паралельно-послідовної схеми мінімальних перетинів, для розрахунку за якими існують математичні залежності.

Мінімальний шлях – це безліч елементів, працездатний стан яких забезпечує роботу системи, причому ніяка підмножина цієї множини такою властивістю не володіє. Мінімальний перетин – це безліч елементів, відмова яких призводить до відмови системи, і ніяка підмножина цієї множини такою властивістю не володіє.

Послідовно-паралельна схема, що побудована методом мінімальних шляхів, і паралельно-послідовна, що побудована методом мінімальних перетинів наведені на рис. 2 та 3 відповідно до рис. 1.

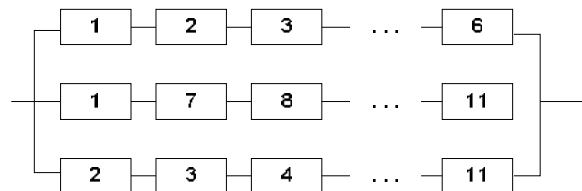


Рис. 2. Послідовно-паралельна схема, що побудована методом мінімальних шляхів

досить високу точність. Оцінка ж за мінімальними шляхами може давати сильно завищені значення ймовірності безвідмовної роботи.

Передбачається, що елементи мінімальних шляхів і мінімальних перетинів можуть перебувати в одному з двох станів – працездатності або відмови з відомими



ймовірностями. Об'єднання ідей методів мінімальних перетинів і розкладання залежностей в ряд дає можливість отримати метод декомпозиції за мінімальними перетинами, що дозволяє оцінювати надійність високонадійних відмовостійких систем з досить складною структурою [3].

Відмови мінімальних перетинів складних систем зазвичай мають ясний фізичний зміст, тому представлення ймовірності відмов системи у вигляді суми ймовірностей відмов окремих мінімальних перетинів відкриває широкі можливості для поглибленого аналізу та синтезу. Легко знаходити слабкі з точки зору надійності ланки систем, досліджувати вплив різних чинників і передбачуваних заходів, будувати оптимальні структури з урахуванням наслідків відмов різних пристроїв і витрат на забезпечення їх надійності.

Застосування методу мінімальних шляхів і мінімальних перетинів здійснюється для обраного показника надійності ПСПД, тобто ймовірності відмови ПСПД.

$$\left(1 - \prod_{i=1}^6 p_i\right) \left(1 - \prod_{j=7}^{11} p_j\right) \left(1 - \prod_{k=2}^{11} p_k\right) > Q_{\text{відм}} > 1 - \left(1 - q_1 \prod_{i=7}^{11} q_i\right) \left(1 - q_2 \prod_{i=7}^{11} q_i\right) \left(1 - q_3 \prod_{i=7}^{11} q_i\right) \left(1 - q_4 \prod_{i=7}^{11} q_i\right) \left(1 - q_5 \prod_{i=7}^{11} q_i\right) * \\ \left(1 - q_6 \prod_{i=7}^{11} q_i\right) \left(1 - \prod_{m=7}^6 q_m\right) \left(1 - q_7 \prod_{n=2}^6 q_n\right) \left(1 - q_8 \prod_{n=2}^6 q_n\right) \left(1 - q_9 \prod_{n=2}^6 q_n\right) \left(1 - q_{10} \prod_{n=2}^6 q_n\right) \left(1 - q_{11} \prod_{n=2}^6 q_n\right) \left(1 - \prod_{s=1}^{11} q_s\right) \quad (3)$$

де:  $p_{i,j,k} = (1 - q_{i,j,k})$  – ймовірність безвідмовної роботи  $i, j, k$ -го інформаційних напрямків;

$q_{l,m,n,s} = (1 - q_{l,m,n,s})$  – ймовірність відмови  $l, m, n, s$ -го інформаційного напрямку.

Формулу (2) можна використовувати для оцінювання надійності ПСПД як в стаціонарному режимі, інтерпретуючи ймовірності як коефіцієнти готовності елементів ПСПД (ймовірність того, що елементи підсистеми виявляються в працездатному стані в довільний момент часу), так і в нестационарному режимі, розглядаючи ймовірності безвідмовної роботи елементів ПСПД за заданий час роботи  $t$  (ймовірність того, що елементи підсистеми будуть працездатні протягом заданого часу роботи при заданих умовах експлуатації).

Для високонадійних мереж при  $Q_{\text{відм}} \approx 0$  верхня межа для ймовірності відмови може розраховуватися за простою формулою, отриманою методом декомпозиції за мінімальними шляхами:

### Література

1. Медведєв В., Кас'яненко М., Коренівська І., Підхід щодо оцінювання надійності функціонування автоматизованої системи управління „Ореанда-ПС”, Теоретичні основи створення і використання інформаційних технологій, *CIT*, 2018, 6 с.  
2. Тескин О.И. Оценка надежности систем на этапе эксплуатационной отработки. М., 1981.  
3. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. М., 1965.

В такому випадку верхнє і нижнє значення ймовірності відмови ПСПД  $Q_{\text{відм}}$  можна отримати за допомогою виразу:

$$\prod_{j=1}^s \left[ 1 - \prod_{i \in I_j} (1 - q_i) \right] > Q_{\text{відм}} > 1 - \prod_{k=1}^r \left( 1 - \prod_{i \in I_k} q_i \right) \quad (2)$$

де:  $q_i$  – ймовірність відмови  $i$ -го інформаційного напрямку;

$r$  – кількість мінімальних шляхів;

$I_k$  – множина індексів елементів, що входять в  $k$ -й мінімальний шлях;

$s$  – кількість мінімальних перетинів;

$I_j$  – безліч індексів елементів, що входять в  $j$ -й мінімальний перетин.

Для варіанту функціонування ПСПД АСУ авіації та ППО, що представлено на рис. 1, верхні і нижні значення ймовірності відмови ПСПД за виразом:

$$Q_{\text{відм}} \approx \prod_{j=1}^s \left[ 1 - \prod_{i \in I_j} p_i \right] \quad (4)$$

При розрахунку надійності ПСПД АСУ авіації та ППО, що представлена на рис.1, при припущенні, що ймовірності безвідмовної роботи всіх інформаційних напрямків зазначеної системи  $p_i = 0,9$  ймовірність відмови  $Q_{\text{відм}} \approx 0,125$ .

### Висновки й перспективи подальших досліджень

Запропонований підхід на відміну від існуючих враховує територіальну розподіленість і ієрархічність системи, що дозволить більш повно оцінити надійність функціонування ПСПД АСУ авіацією та ППО.

Даний підхід можна покласти в основу розробки методики оцінювання стійкості функціонування АСУ авіації та ППО в цілому.

524 с. 4. Рожков Л.И. Средства передачи данных в АСУ. Киев, 1977. 184 с. 5. ДСТУ 3524-97. Надійність техніки. Проектна оцінка надійності складних систем з урахуванням технічного і програмного забезпечення та оперативного персоналу. Основні положення. – К.: Держстандарт України, 1994.– 36 с. 6. Барлоу Р., Прошан Ф. Математическая теория надежности : / пер. с англ. М., 1969. 448 с.

**ПОДХОД К ОЦЕНИВАНИЮ НАДЕЖНОСТИ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ АВИАЦИИ И ПРОТИВОВОЗДУШНОЙ ОБОРОНЫ**

*Илона Сергеевна Корневская*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*В статье предложен подход к оценке надежности функционирования подсистемы передачи данных автоматизированной системы управления авиацией и противовоздушной обороной, основанный на использовании метода минимальных путей и минимальных сечений.*

*Кроме того, рассмотрены математические методики оценки надежности информационных систем, которые могут быть использованы при оценке надежности подсистемы передачи данных автоматизированной системы управления авиацией и противовоздушной обороной. Приведены подход оценки надежности варианта структуры автоматизированной системы управления авиацией и противовоздушной обороной.*

**Ключевые слова:** *надежность; подсистема передачи данных метод минимальных путей и сечений.*

**THE APPROACH OF ASSESSING THE RELIABILITY OF TROOPS (FORCES) AUTOMATED CONTROL SYSTEMS DATA SUBSYSTEMS**

*Iлона Korenivska*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*The article deals with the approach of assessing the reliability of troops (forces) automated control systems data subsystems. It relies on using of minimum paths and minimum intersections method.*

*Moreover, techniques of information systems reliability estimation are considered. The techniques can be used to evaluate the reliability of the automated aviation and air defense control system data transmission subsystem. The proposed approach of reliability estimation of the aviation and air defense automated management system is considered*

**Key words:** *reliability; data subsystem; method of minimum paths and minimum intersections method.*

**References**

- Osborne K.** (2018), Air Force Creates Armed Forces Management System in War [The National Interest]: <https://nationalinterest.org/blog/the-buzz/the-air-force-creation-system-manage-the-militarys-forces-24701>.
- Nisienko B.** Main directions of automation of control processes in the Air Force of the Armed Forces of Ukraine. - M.: Collection of Scientific Papers of Kharkiv National University of the Air Force, 2017. - 19 sec.
- DSTU 3524-97.** Reliability of technology. Design assessment of the reliability of complex systems, taking into account hardware and software and operating personnel. Substantive provisions. - K.: State Standard of Ukraine, 1994. - 36 p.
- DSTU 2862-94.** Reliability of technology. Methods of calculating reliability indicators. General requirements. - K.: State Standard of Ukraine, 1994. - 36 p.
- Gryshko V., Mozharovsky P.** Assessing the reliability of a complex of technical means of complex information and control systems. - M.: Mathematical Machines and Systems, 2009. № 3- 194 p.
- Akimova G., Solovyov A.** Methodology for assessing the reliability of hierarchical information systems, M. Proceedings of ISA RAS, 2006 - 18 p.

Ярослав Вячеславович Мельник  
Віктор Євгенович Бобильов (кандидат військових наук, с.н.с.)

Національний університет оборони України імені Івана Черняхівського, Київ, Україна

## МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ ІСНУЮЧИХ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ПРОГРАМНИХ УТИЛІТ ДЛЯ ВИЗНАЧЕННЯ ТОПОЛОГІЇ ГЕТЕРОГЕННИХ МЕРЕЖ ДЛЯ ЗНАХОДЖЕННЯ АЛЬТЕРНАТИВНИХ ВАРІАНТІВ ПІДКЛЮЧЕННЯ

Сучасне інформаційне середовище постійно наражається на вплив зовнішніх або внутрішніх завад. У сучасний період постійного розвитку і удосконалення засобів радіоелектронної боротьби та методів впливу на телекомунікаційні системи їх захист стає дуже важливою та актуальною проблемою.

Існують програмне забезпечення та програмні утиліти, що представляють собою сукупність підходів, які надають можливість будувати телекомунікаційні мережі стійкими до впливу тих чи інших завад. Але більшість з них стосується технічних аспектів побудови мережі. Що стосується топології таких мереж, то при їх обґрунтуванні можна спиратися лише на їх невелику кількість.

Справа у тому, що гетерогенні мережі мають у своїй структурі велику кількість вузлів, що безпосередньо піддані впливу навмисних та ненавмисних завад. Тому, часом, виникає необхідність здійснювати заміну вузлів, через які проходить інформація, на інші, у зв'язку із впливом на них завад.

Заміна вузлів, або переключення проходження інформації через інші вузли, на які не впливають завади, породжує зміну топології гетерогенної мережі, що забезпечує альтернативні варіанти їх підключення.

На даний час не існує єдиних методичних підходів до реалізації дій щодо зміни топології мереж. Їх наявність надасть можливість обґрунтовано змінювати топологію гетерогенних мереж (ГМ) для забезпечення альтернативних варіантів їх підключення.

Тому, нижче наведена стаття присвячена наданню методичних рекомендацій щодо використання існуючих програмного забезпечення та програмних утиліт для визначення топології гетерогенних мереж при пошуку альтернативних варіантів підключення.

**Ключові слова:** гетерогенна мережа; програмне забезпечення; програмні утиліти; топологія мереж; маршрутизація; структура гетерогенних мереж.

### Вступ

**Постановка проблеми.** У науково-технічних виданнях, що присвячені питанням побудови та використання сучасних телекомунікаційних мереж, описано декілька підходів до їх побудови та утримання у працездатному стані під час впливу на них навмисних та ненавмисних завад.

Структуру телекомунікаційної мережі загального користування (ТМЗК), у тому випадку, коли її неможливо одержати у якості вихідних даних від оператора зв'язку, виявляють шляхом аналізу ТМЗК спеціалізованим програмним (ПЗ). Наприклад, існуючі утиліти PathPing у сімействі операційних систем (ОС) MS Windows XP/2003/7/8/10 дозволяють визначити множину маршрутів у ТМЗК до необмеженої множини її кінцевих і транзитних елементів. Аналогічними утилітами є TracerPath та Tracerout у ОС Unix.

**Метою статті** є надання методичних рекомендацій щодо використання існуючих програмного забезпечення та програмних утиліт для визначення топології гетерогенних мереж при пошуку альтернативних варіантів підключення.

### Виклад основного матеріалу дослідження

Алгоритм розкриття структури мережі систем загального користування носить ітеративний характер та складається із двох етапів: пошуку вузлів мережі та перевірки можливості встановити маршрут через наступний знайдений вузол.

Перед початком роботи алгоритму необхідно визначити вихідні дані. Для їх одержання, у першу чергу, знаходять перший маршрут шляхом трасування маршруту між вузлами зв'язку. При цьому для кожної пари вузлів  $A$  і  $B$  здійснюється як трасування  $A \rightarrow B$  так і  $B \rightarrow A$ , що часто дозволяє знаходити різні маршрути. Приклад реверсивного трасування наведений у таблиці 1.

Таблиця 1  
Приклад реверсивного трасування

	Маршрут $A \rightarrow B$	Маршрут $B \rightarrow A$
1.	217.76.205.218	188.213.165.186
2.	172.16.200.254	188.213.165.3
3.	172.16.200.1	62.149.185.51
4.	217.76.205.217	149.6.18.49
5.	149.6.190.78	130.117.48.113
6.	149.6.190.77	154.54.59.2
7.	130.117.48.93	154.54.60.113
8.	154.54.59.86	130.117.0.62
9.	154.54.58.5	154.54.59.181
10.	130.117.0.17	154.54.59.186
11.	154.54.38.102	154.54.36.234
12.	154.54.59.1	149.6.190.78
13.	130.117.48.114	217.76.205.217
14.	149.6.18.50	217.76.205.218
15.	62.149.185.60	
16.	188.213.165.186	

Одержання множини маршрутів з декількох точок до деякої кількості вузлів ТМЗК вже дозволяє отримати інформацію про її розгалуженість. Для більш детального вивчення структури ТМЗК можна виділити адресу будь-якого транзитного вузла, визначити по ньому адресу підмережі провайдера, до якої він належить, а потім здійснити пошук маршрутів до всіх вузлів, що входять у знайдені підмережі.

Алгоритм розкриття маршруту для одного варіанту підключення складається з наступних кроків (рис. 1):

1. Задається множина множин  $B = \{b^i\}$ ,  $\{b^j\} = \{e_b\}$ ,  $b \cap_j = \emptyset$  граничних вузлів (рис. 1, а).

2. Попарно визначаються усі маршрути  $r = \{e_r^j\}$ , з кожного вузла кожної множини границь до кожного вузла інших множин  $b$  (рис. 1, б).

3. Для усіх визначених в  $\{r\}$  вузлів  $\{e_r^j\}$  здійснюється виділення підсистеми провайдера, до якої належить вузол. Одержують множину  $e = \{e_r^j\}$ , яка містить у собі усі вузли підмереж провайдерів, через які проходять базові маршрути.

4. Кожний елемент  $\{e_r^j\}$  перевіряють на активність. Усі неактивні вузли видаляються з множини (рис. 1, в).

5. Здійснюють пошук маршруту з кожного вузла  $\{e_b\}$  в кожний вузол  $\{e_r^j\}$ . Отриману множину маршруту додають до  $\{r\}$ .

6. Отримують множину альтернативних маршрутів шляхом об'єднання всіх знайдених маршрутів у єдиний граф (рис. 1, г).

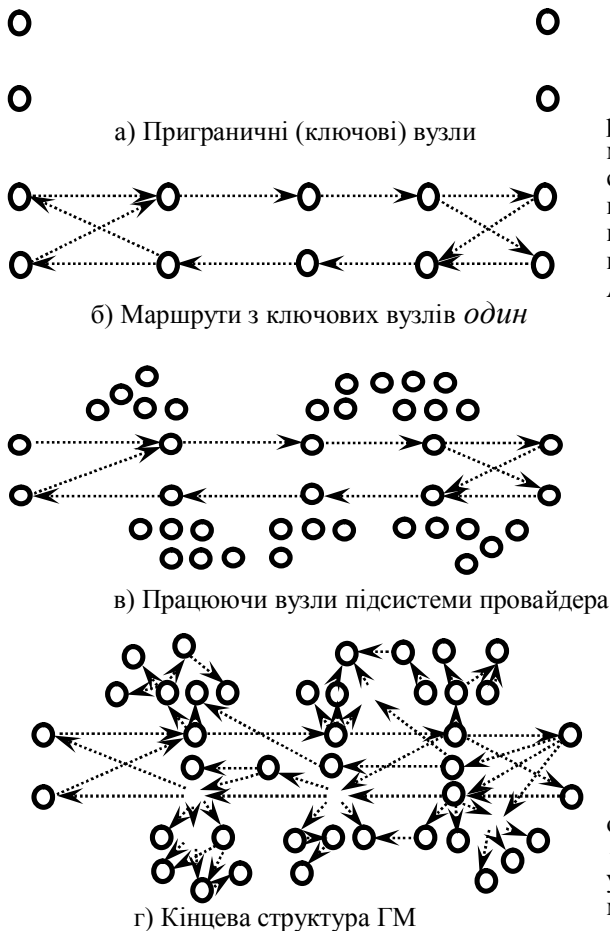


Рис. 1. Візуалізація алгоритмів розкриття ГМ

Даний алгоритм виконується для всіх варіантів підключення граничних вузлів до мережі Інтернет. Перевірка на активність знайдених вузлів здійснюється шляхом пересилання певних пакетів на різні (або усі) порти вузла.

Для автоматизації цих дій може бути використане спеціальне програмне забезпечення nmap, яке поширюється за вільною ліцензією.

Для апробації процедури було зроблено розкриття альтернативних варіантів підключення вузла  $A$  розміщеного у Києві до вузла  $B$ , розміщеного в Італії (місто Ареццо) (рис. 2).

У якості варіантів підключення вузла  $A$  розглядалося ADSL-підключення до локальної мережі. На рис. 3 і 4 показана візуалізація структури розкритої ГМ різних варіантів підключення, а також (рис. 5 і 6) графічний спосіб візуалізації розкритої структури ГМ з'єднання вузлів підключення через локальну мережу та ADSL.



Рис. 2. Географічне розташування вузла  $B$ .

У якості варіантів підключення вузла  $A$  розглядалося ADSL-підключення до локальної мережі. На рис. 3 і 4 показана візуалізація структури розкритої ГМ різних варіантів підключення, а також (рис. 5 і 6) графічний спосіб візуалізації розкритої структури ГМ з'єднання вузлів підключення через локальну мережу та ADSL.

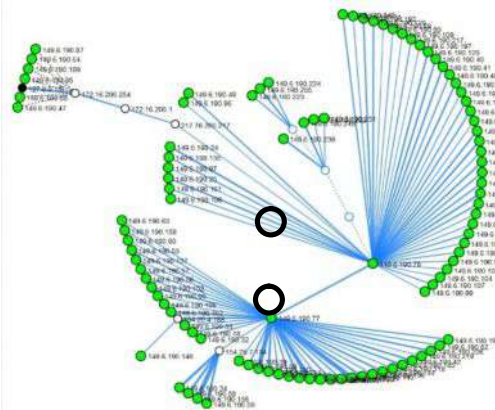


Рис. 3. Візуалізація розкритої структури ГМ з'єднання вузлів через локальну мережу

Покажемо виконання процедури на прикладі одного вузла з базових маршрутів  $B = \{217.76.205.218, 188.213.165.186\}$ . За допомогою утиліти TracertPath знайдемо перший базовий маршрут:

```
$ tracert 188.213.165.186
1: 172.16.200.254
2: 172.16.200.1
```

3: 217.76.205.217  
 4: 149.6.190.78  
 5: gi0-4-0-2.rcr21.kbp01.atlas.cogentco.com [149.6.190.77]  
 6: be2679.ccr21.bts01.atlas.cogentco.com [130.117.48.93]  
 7: be2988.ccr51.vie01.atlas.cogentco.com [154.54.59.86]  
 8: be2974.ccr21.muc03.atlas.cogentco.com [154.54.58.5]  
 9: be3072.ccr51.zrh02.atlas.cogentco.com [130.117.0.17]  
 10: be2043.rcr21.mil01.atlas.cogentco.com [154.54.38.102]  
 11: be3526.rcr51.vce01.atlas.cogentco.com [154.54.59.1]  
 12: be3137.rcr11.qzo03.atlas.cogentco.com [130.117.48.114]  
 13: 149.6.18.50  
 14: it1-is4-b.aruba.it [62.149.185.60]  
 15: host186-165-213-188.serverdedicati.aruba.it [188.213.165.186]

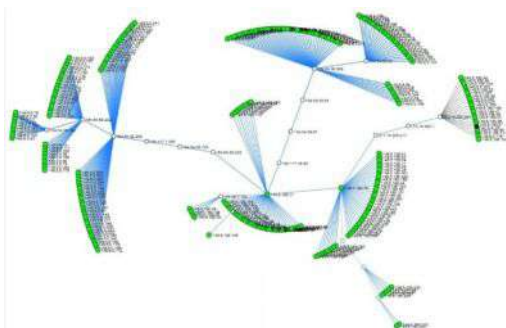


Рис. 4. Візуалізація розкритої структури ГМ з'єднання вузлів через локальну мережу

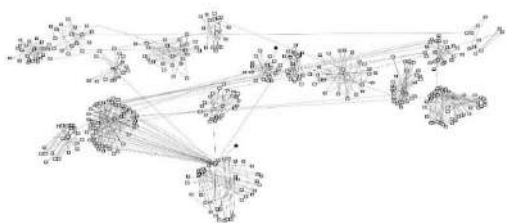


Рис. 5. Графічний спосіб візуалізації розкритої структури ГМ з'єднання вузлів через локальну мережу

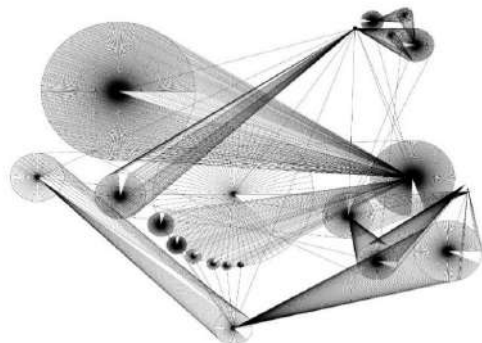


Рис. 6. Візуалізація розкритої структури ГМ з'єднання вузлів через ADSL – підключення

Визначимо підмережу провайдера першого зовнішнього вузла (149.6.190.78) за допомогою утиліти whois:

\$ whois 149.6.190.78

```
inetnum: 149.6.0.0 - 149.6.255.255
Діапазон вузлів 149.6.0.0 .... 149.6.255.255
додається в et. Перевіримо кожний вузол
діапазону за допомогою утиліти nmap. Утиліта
відправить певним чином сформовані запити на
зазначені порти і для кожного працюючого вузла
поверне наступну інформацію:
sudo nmap -sn -PE -PS22, 25, 80 -PA21, 23, 80,
3389 \
-PU -P0 --traceroute 149.6.0-255.0-255
149.6.190.78
Starting Nmap 7.70 ( https://nmap.org ) at 2018-
05-15 10:55
Host 149.6.0.10 is up (0.047s latency).
TRACEROUTE (using port 22/tcp)
HOP RTT ADDRESS
- Hops 1-10 are the same as for 149.6.0.10
11 43.00 ms 149.6.0.0
```

```
Starting Nmap 7.70 at 2018-05-15 12:44 MSD
Host 93.157.123.0 is up (0.0021s latency).
MAC Address: FF:FF:FF:FF:FF:FF (Unknown)
Host novosm-user-gw.gtk.su (93.157.123.1) is up
MAC Address: 00:19:5B:F4:3B:81 (D-Link)
Здійснюється пошук маршруту для кожного
виявленого вузла за допомогою утиліти tracerpath
та всі маршрути запам'ятовуються, а далі
поєднуються. Результат повного розкриття мережі
наведено на рис. 2.
```

У випадку, коли немає можливості здійснювати пошук маршрутів з вузлів однієї з границь, можуть застосовуватися вузли-агенти. Нехай потрібно знайти всі доступні маршрути від вузла 172.16.200.254 (A), до 194.0.131.18 (B, один із серверів компанії МетаУА). Отримаємо за допомогою утиліти tracerpath маршрут A → B. Зімітуємо відсутність доступу до одного з вузлів, та задіємо вузол-агент.

```
1: 172.16.200.254
1: 172.16.205.1
2: 217.76.205.217
3: ctnet-10G-gw.ix.net.ua [185.1.50.23]
4: topnet2-10G-gw.ix.net.ua [185.1.50.234]
5: meta.ae10-822.lsr02-kiev.topnet.ua [77.88.206.13]
6: meta.ae10-822.lsr02-kiev.topnet.ua [77.88.206.14]
7: meta.ua [194.0.131.18]
Побудуємо маршрут з вузла-агента
31.172.139.22 до вузла, який аналізується
194.0.131.18:
```

```
1: v1089.nva1.kv.wnet.ua [31.172.139.22]
1: v3342.nval.kv.wnet.ua [217.20.162.34]
2: v3346.sh2.kh.wnet.ua [217.20.161.241]
3: v3346.sh2.kh.wnet.ua [217.20.161.241]
4: v3351.khar.kh.wnet.ua [217.20.161.85]
5: ea1.hostmsk.wnet.ua [217.20.161.85]
6: meta.br0-kiev-vlan823.top.net.ua [77.88.200.53]
7: meta-gw.top.net.ua [77.88.200.54]
8: meta.ae10-822.lsr02-kiev.topnet.ua [77.88.206.13]
9: meta.ae10-822.lsr02-kiev.topnet.ua [77.88.206.14]
10: meta.ua [194.0.131.18]
```

Після цього здійснимо пошук з вихідного вузла 172.16.200.254 до вузлів з маршруту 31.172.139.22 → 194.0.131.18 і вилучимо частини маршрутів, які повторюються. У результаті було знайдено три маршрути, як наведено на рис. 7.

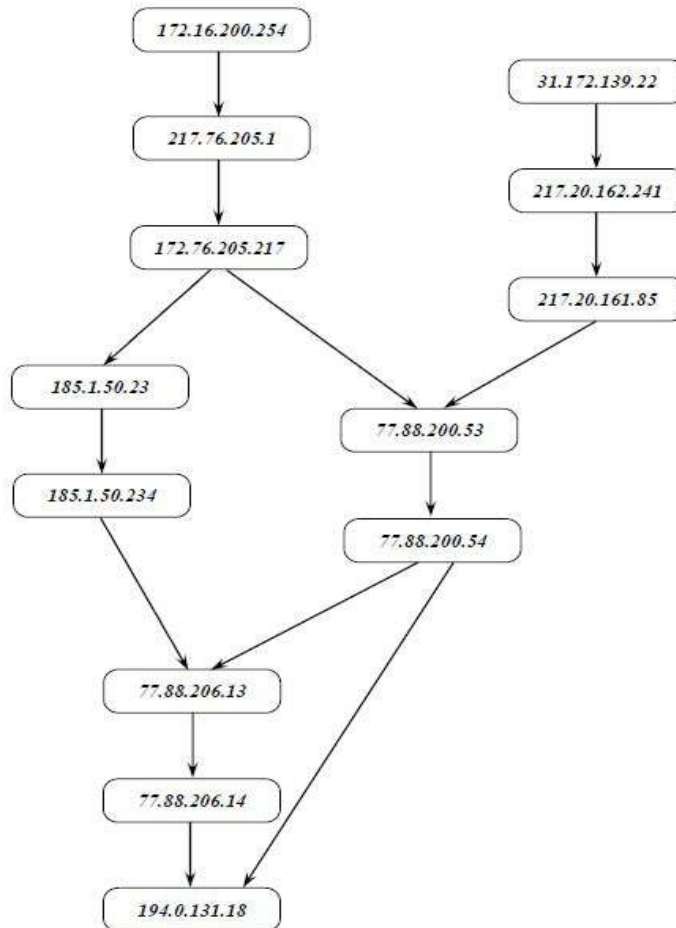


Рис. 7. Візуалізація роботи алгоритму пошуку альтернативних маршрутів за допомогою вузлів-агентів. Знайдено 3 маршрути від 172.16.200.254 до 194.0.131.18 за допомогою агента 31.172.139.22

При наявності експерта в області комп'ютерної безпеки можливо здійснити розкриття програмного та апаратного забезпечення, яке використовується на вузлі, та дати експертну оцінку надійності вузла. Під комплексним показником надійності до ННП  $e_t - \Gamma_0$  вузла розуміється нормоване чисельне значення згортки параметрів надійності, яке характеризує стійкість вузла зв'язку до впливів навмисних та ненавмисних завад. Порядок обчислення  $P_{K_i}$  відомий та описаний. Значення  $P_{K_i}$  обчислюють шляхом підсумовування, або перемножування, або як середнє арифметичне значення його параметрів надійності. При розрахунку надійності конкретного вузла може бути використана географічна інформація. Існують спеціальні бази даних (наприклад, geoip), які з високою точністю повертають інформацію про регіон вузла за його IP-адресою.

Ця ж сама інформація доступна через сервіс whois. Як правило, IP-адреси виділяються провайдером підмережами, тому може бути відсутня необхідність перевірки кожного вузла, якщо вони належать одному власникові. Запит інформації з першого транзитного вузла 217.16.205.1 з першого знайденого маршруту 172.16.200.254 --> 31.172.139.22 показав, що перші 2 транзитних вузла належать одному провайдеру (наведено неповний висновок):

inetmim: 217.76.192.0 - 217.76.205.255  
 netname: UA-CITYNET-20001129  
 descr: T.E.S.T. Ltd Ukraine  
 country: UA  
 organisation: ORG-CJ1-RIPE  
 org-name: "T.E.S.T." Ltd  
 fax-no: +380445911125  
 phone: +7 812 3323433  
 address: 6, Tulchinskaya str., 04080, Kiev, Ukraine

У таблиці 2 представлена інформація з кожного вузла, що входить у маршрут. Як видно з таблиці, дані, отримані з сервісу whois, дозволяють довідатися про місце розташування (топологию) вузла по його IP-адресі.

Звичайно, такі дані можуть вимагати уточнення, тому що можуть повідомляти про місце розташування не самого вузла, а установи, на яку зареєстрована IP-адреса. З вищенаведеної відповіді "whois" ми бачимо, що трафік з мережі провайдера "Ukrainian Internet Exchange" попадає прямо у Київ на майданчик UA-IX через вузол 185.1.50.234. Малоймовірно, що середній провайдер має міжміські канали. З опису вузла виходить, що він належить точці обміну трафіком UA-IX (<https://www.ripe.net/manage-ips-and-asns/db/support>) до якої підключений провайдер.

Додаткову інформацію можна одержувати з назви вузла, так 185.1.50.234 має ім'я DE "Ukrainian Internet Exchange" (UA-IX), що підтверджує

припущення про розміщення цього вузла у Києві. Ця інформація також не має абсолютну достовірність.

Таблиця 2

№ вузла маршруту	IP-адреса вузла	Інформація про вузол, отримана із сервісу whois
1-3	217.76.192.0 217.76.205.255	Київ, Україна, компанія T.E.S.T
4	185.1.50.23	Київ, Україна, точка обміну трафіком "Ukrainian Internet Exchange" (UA-IX)
5	185.1.50.234	Київ, Україна, точка обміну трафіком "Ukrainian Internet Exchange" (UA-IX)
6	77.88.206.13	Київ, Україна, Компанія UA-TOPNET
7	77.88.206.14	Київ, Україна, Компанія UA-TOPNET
8	194.0.131.18	Київ, Україна, Компанія МЕТА-UA

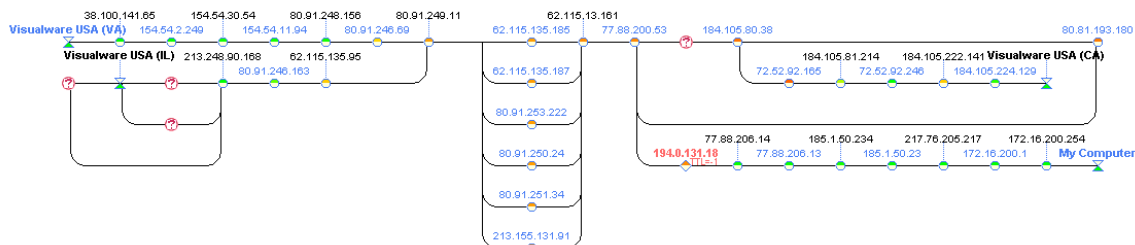
Для розв'язання задачі знаходження альтернативних маршрутів також може бути використане багатоагентне ПЗ, агенти якого можуть перебувати як на вузлах у власності власника ГМ, так і на вузлах, що не належать йому. Як приклад такого ПЗ можна привести пропріетарний продукт Visual Route (<http://www.visualroute.com/>). Це комплекс програм, який містить у собі агента MCS MyRoute та додаток для аналізу даних та моніторингу стану системи VisualRoute. На рис. 8 наведено приклад

маршрутів між двома вузлами мережі Інтернет. Як видно з рис. 8, VisualRoute дозволив знайти 128 однінних маршрутів до вузла мережі, котрий розшукувався (див. на рис. 8 IP 194.0.131.18) з мінімальною кількістю транзитних вузлів - 13. VisualRoute має можливість визначити прив'язку маршруту до карти. Використання в VisualRoute багатоагентної архітектури дозволяє одержати множину маршрутів до заданого вузла з декількох точок мережі. Так на рис. 9 наведено приклад, який зображує множину маршрутів до 80.81.193.180 з декількох територіально розподілених вузлів агентів.



Рис. 8. Візуалізація процесу моніторингу структури ТМЗК

На рис.9 наведено приклад одержання маршрутів до деяких вузлів підмережі, у які входили транзитні вузли на маршруті від вихідного вузла (My Computer) до заданого (80.81.193.180)



### Література

1. Лізунов П.П., Васильєва Г. Л., Мінаєва Ю. І., Філімонова О.Ю. Комп'ютерні мережі і телекомунікації. К.: Київський національний університет будівництва і архітектури, 2017р.  
2. Пермяков О.Ю., Кільменінов О.А., Мельник Я.В. Застосування перколяційних алгоритмів для оцінки

надійності гетерогенних мереж військового призначення. К.: НУОУ, 2019 р. 3. Visual Route and virtual network computing exercises for computer network courses, Number AC 2007-944. American Society for Engineering Education, 2007 p.

## МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ СУЩЕСТВУЮЩИХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ПРОГРАММНЫХ УТИЛИТ ДЛЯ ОПРЕДЕЛЕНИЯ ТОПОЛОГИИ ГЕТЕРОГЕННЫХ СЕТЕЙ ДЛЯ НАХОЖДЕНИЯ АЛЬТЕРНАТИВНЫХ ВАРИАНТОВ ПОДКЛЮЧЕНИЯ

Ярослав Вячеславович Мельник

Виктор Евгеньевич Бобылев (кандидат военных наук, с.н.с.)

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

*Современное информационное пространство постоянно подвергается влиянию внешних или внутренних помех. В современный период постоянного развития и совершенствования средств радиоэлектронной борьбы и методов воздействия на телекоммуникационные системы их защита становится очень важной и актуальной проблемой.*

*Существуют программное обеспечение и программные утилиты, которые обеспечивают совокупность подходов, которые предоставляют возможность строить телекоммуникационные сети устойчивыми к воздействию тех или иных помех. Но большинство из них касается технических аспектов построения сети. Что касается топологии таких сетей, то при их обосновании можно опираться только на их небольшое количество. Дело в том, что гетерогенные сети имеют в своей структуре большое количество узлов, непосредственно подверженных влиянию умышленных и неумышленных помех. Поэтому, возникает необходимость осуществлять замену узлов, через которые проходит информация, на другие, в связи с воздействием на них помех. Замена узлов, или переключение прохождения информации через другие узлы, на которые не влияют помехи, порождает изменение топологии гетерогенной сети, обеспечивающей альтернативные варианты их подключения.*

*В настоящее время не существует единых методических подходов к реализации действий по изменению топологии сетей. Их наличие предоставит возможность обоснованно изменять топологию гетерогенных сетей (ГС) для обеспечения альтернативных вариантов их подключения. Поэтому, ниже приведена статья, посвященная выработке методических рекомендаций по использованию существующих программного обеспечения и программных утилит для определения топологии гетерогенных сетей при поиске альтернативных вариантов их подключения.*

**Ключевые слова:** гетерогенная сеть; программное обеспечение; программные утилиты; топология сетей; маршрутизация; структура гетерогенных сетей.

## METHODOLOGICAL RECOMMENDATIONS FOR THE USE OF EXISTING SOFTWARE AND SOFTWARE UTILITIES FOR DETERMINING THE TOPOLOGY OF HETEROGENEOUS NETWORKS FOR FINDING ALTERNATIVE CONNECTION OPTIONS

Yaroslav Melnyk

Victor Bobylov (Candidate of military sciences, Senior Research Fellow)

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

*The modern information environment is constantly affected by external or internal interference. In the modern period of constant development and improvement of electronic warfare tools and methods of influencing telecommunication systems, their protection becomes a very important and urgent problem.*

*There are software and software utilities that are a set of approaches that make it possible to build telecommunications networks resistant to interference. But most of them relate to the technical aspects of building a network. With regard to the topology of such networks, their justification can only be based on a small number of them. The fact is that heterogeneous networks have in their structure a large number of nodes that are directly exposed to intentional and unintentional interference. Therefore, at times, it may be necessary to replace the nodes through which the information passes through to others due to their interference.*

*Replacing nodes, or switching information through other nodes that are not affected by interference, generates a change in the topology of the heterogeneous network, providing alternative options for connecting them.*

*Currently, there is no single methodological approach to implementing actions to change the topology of networks. Their availability will make it possible to reasonably change the topology of heterogeneous networks (HN) to provide alternative options for their connection. Therefore, the following article is devoted to providing guidance on using existing software and software utilities to determine the topology of heterogeneous networks when looking for alternative connectivity options.*

**Key words:** heterogeneous network; software; software utilities; network topology; routing; structure of heterogeneous networks.

### References

1. Lizunov P.P., Vasilyeva G.L., Minaeva Yu. I., Filimonova A.Yu. Computer networks and telecommunications. K. : Kyiv National University of Civil Engineering and Architecture, 2017. 2. Permyakov O.Y., Kilmeninov O.A., Melnik Y.V. Application of percolation

algorithms for the estimation of the reliability of heterogeneous wax networks. K. : NDUU, 2019. 3. Visual Route and virtual network computing exercises for computer network courses, Number AC 2007-944. American Society for Engineering Education, 2007 p.



*Віктор Опанасович Муренко (кандидат військових наук, професор)  
Віталій Миколайович Безуглий*

*Національний університет оборони України імені Івана Черняхівського, Київ, Україна*

## ДО ПИТАННЯ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ОБ'ЄДНАНОЇ ПІДГОТОВКИ СИЛ ОБОРОНИ ВІЙСЬКОВОЇ ЧАСТИНИ НАДВОДНИХ СИЛ ВІЙСЬКОВО-МОРСЬКИХ СИЛ ТА МОРСЬКОЇ ОХОРОНИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ

*У даній статті на основі системного аналізу практичної діяльності визначено підходи до оцінювання ефективності об'єднаної підготовки військових частинами надводних сил Військово-Морських Сил Збройних Сил України та морської охорони Державної прикордонної служби України, складових сектору безпеки і оборони держави. Обґрунтовано вибір основних показників об'єднаної підготовки сил оборони держави, які в свою чергу забезпечать досягнення необхідного рівня взаємодії військових частин надводних сил Військово-Морських Сил та морської охорони Державної прикордонної служби України, і враховують набуття штабом спроможностей щодо планування спільного виконання завдань та застосування в ході виконання спільних завдань об'єднаними тактичними групами, набуття підрозділами військових частин надводних сил Військово-Морських Сил та морської охорони Державної прикордонної служби України спроможностей спільно діяти в складі об'єднаних корабельних тактичних груп. Визначена система показників максимально розкриває особливості процесу управління та навченості об'єднаною підготовкою сил оборони, які впливатимуть на ступінь досягнення мети об'єднаної підготовки сил оборони держави, а також вказує на їх структуру та ієрархічність.*

***Ключові слова:** об'єднана підготовка сил оборони; надводні сил Військово-Морських Сил; морська охорона Державної прикордонної служби; показники.*

### Вступ

Досвід застосування військових формувань сил безпеки і оборони в зоні проведення антитерористичної операції (АТО) свідчить про наявність низки невирішених (проблемних) питань, що значно знижує ефективність виконання ними поставлених завдань. До таких питань, у першу чергу, доцільно віднести недосконалість підготовки штабів та підрозділів військових частин діяти спільно у складі міжвідомчих тактичних груп та угруповань. В той самий час досвід проведення АТО та операції об'єднаних сил (ООС) вказує на зростання ступеню застосування військових частин надводних сил Військово-Морських Сил Збройних Сил України (ВМС) у складі міжвідомчих угруповань, що в свою чергу вимагає спільного виконання окремих завдань військових частин надводних сил Військово-Морських Сил Збройних Сил України (ВМС) з морською охороною Державної прикордонної служби України (МО ДПС).

Все це вимагає особливої уваги щодо, набуття сумісності визначеним складом сил оборони, підвищенню рівня індивідуальної фахової підготовки особового складу. [6]

**Постановка проблеми.** В останній період проведення АТО та ООС постала гостро проблема підготовки кваліфікованих військових кадрів органів військового управління (ОВУ), які забезпечать якісне планування бойових дій та управління військами (силами) в ході їх ведення. Разом з тим в початковий період проведення бойових дій, а також і у подальшому вказує на низький рівень взаємодії сил оборони при спільному виконанні завдань, внаслідок

попередніх помилок виправлення яких можливо за рахунок об'єднаної підготовки сил оборони (ОПСО) та набуття спроможностей щодо планування бойових дій міжвідомчих угруповань.

На даний час питання організації об'єднаної підготовки Збройних Сил України та інших складових сил оборони знаходиться на початковому етапі визначення її загальних принципів, підходів та визначення загальної структури [4].

Відсутність єдиних поглядів щодо порядку набуття спроможностей спільного виконання завдань у військових частин надводних сил ВМС та МО ДПС, знижує ефективність заходів ОПСО та практично унеможливує досягнення її мети [3].

**Аналіз останніх досліджень і публікацій.** Питанням дослідження ефективності підготовки була присвячена низка попередніх робіт.

Аналіз цих робіт свідчить, що за допомогою різних наукових підходів можливо оцінити результати підготовки військовослужбовця, штабу, підрозділу, отримати комплексну безрозмірну оцінку. Проте, дослідники виходили з тих наукових завдань, які були породжені актуальними проблемами практики свого часу, застосовували такі показники і критерії, які найбільш повно відображали процеси, що розглядалися. Водночас зміни, які відбулися у практиці бойової підготовки військових частин свідчать, що їх не достатньо для визначення ефективності системи об'єднаної підготовки сил оборони [5].

**Метою статті** є запровадження єдиних поглядів на теоретичні положення оцінювання

ефективності ОПСО, визначити основні показники які впливають на ступінь досягнення мети системи ОПСО, а також їх структуру і ієрархічність.

**Виклад основного матеріалу дослідження**

Для оцінювання ефективності ОПСО доцільно визначити критерій, а саме безрозмірну величину  $W_B(t)$ , якій привласнимо характеристики готовності військової частини до взаємодії об'єктів підготовки на час  $t$ . Визначимо її в якості узагальненого показника, за допомогою якого будемо визначати набутий рівень взаємодії військових частин надводних сил ВМС та МО ДПС спільно виконувати завдання у складі об'єднаних корабельних тактичних груп (ОКТГ).

Значення узагальненого показника рівня взаємодії  $W_B(t)$  лежить у межах від 0 до 1:

$$0 < W_B(t) \leq 1 \quad (1)$$

Безпосередній вплив на набуття взаємодії здійснюють інтегральні показники, за допомогою яких пропонується оцінювати її рівень під час виконання заходів ОПСО. Інтегральними показниками визначаємо "рівень взаємодії військової частини ВМС" та "рівень взаємодії військової частини МО ДПС", саме вони і визначатимуть рівень взаємодії спільного виконання завдань.

Тоді функціональна залежність матиме наступний вигляд:

$$W_B(t) = f_B \{ E_{ВВМС}(t); E_{ВМО}(t) \}, \quad (2)$$

де:  $E_{ВВМС}(t); E_{ВМО}(t)$  – інтегральні показники "рівень взаємодії військової частини ВМС", "рівень взаємодії військової частини МО ДПС" на дискретний момент часу  $t$ .

Інтегральні показники залежать від сукупності часткових показників, які розкривають фізичний зміст та визначають відповідний рівень у безрозмірній величині.

Фізичний зміст інтегрального показника "рівень взаємодії військової частини ВМС (МО ДПС)" полягає в тому, що він характеризує спроможність штабу військової частини надводних сил ВМС (МО ДПС) на час  $t$  здійснювати планування застосування та управління діями ОКТГ у ході спільного виконання окремих завдань та готовність ОКТГ виконувати завдання задля, яких вона була створена на час  $t$ .

$$E_{ВВМС(МО)}(t) = f_{ВВМС(МО)} \left\{ \begin{matrix} H_{СПШ}(t); \\ H_{СПОКТГ}(t) \end{matrix} \right\}, \quad (3)$$

Спроможність штабу військової частини ВМС (МО ДПС) залежить від управлінської діяльності суб'єктів ОПСО, його укомплектованості особовим складом, навченості особового складу і рівня забезпечення підготовки. Тоді функціональна залежність матиме вигляд:

$$H_{СПШ}(t) = f_{СПШ} \left\{ \begin{matrix} H_{УСПШ}(t); H_{УШ}(t); \\ H_{НШ}(t); H_{РЗШ}(t) \end{matrix} \right\}, \quad (4)$$

де:  $H_{УСПШ}(t); H_{УШ}(t); H_{НШ}(t); H_{РЗШ}(t)$  – часткові показники "управління ОПСО штабу", "укомплектованість штабу особовим складом", "навченість штабу" та "рівня забезпечення ОПСО"

на дискретний момент часу  $t$ .

Будемо рахувати, що штаб військової частини надводних сил ВМС (МО ДПС) під час процесу навчання укомплектовані особовим складом на 100%, а рівень забезпечення дозволяє виконати всі заходи, які заплановані суб'єктом підготовки на ОПСО, тому частковий показники  $H_{УШ}(t); H_{РЗШ}(t)$ ; приймаємо рівним одиниці, тоді вираз (4) можна записати у такому вигляді:

$$H_{СПШ}(t) = f_{СПШ} \{ H_{УСПШ}(t); H_{НШ}(t) \}, \quad (5)$$

Фізичний зміст часткового показника "готовність ОКТГ"  $K_{СПОКТГ}(t)$  полягає в тому, що він характеризує спроможність ОКТГ виконати завдання за призначенням. Його пропонується розраховувати за функціональною залежністю, яка враховує готовність ОКТГ виконати завдання за призначенням.

Рівень готовності ОКТГ залежить від управління діяльності суб'єкта підготовки ОПСО, її укомплектованості, навченості і рівня забезпечення підготовки. Тоді функціональна залежність матиме наступний вигляд:

$$H_{СПОКТГ}(t) = f_{СПОКТГ} \left\{ \begin{matrix} H_{УСПОКТГ}(t); \\ H_{УОКТГ}(t); \\ H_{НОКТГ}(t); H_{РЗ}(t) \end{matrix} \right\}, \quad (6)$$

де:  $H_{УСПОКТГ}(t); H_{УОКТГ}(t); H_{НОКТГ}(t); H_{РЗ}(t)$  – часткові показники "управління ОПСО ОКТГ", "укомплектованість ОКТГ", "навченість ОКТГ" та "рівня забезпечення ОПСО ОКТГ" на дискретний момент часу  $t$ .

Будемо рахувати, що ОКТГ під час процесу навчання укомплектовані особовим складом на 100%, а рівень забезпечення дозволяє виконати всі заходи які заплановані суб'єктом підготовки на ОПСО тому частковий показники  $H_{УОКТГ}(t); H_{РЗ}(t)$ ; приймаємо рівним одиниці, тоді вираз (6) можна записати у такому вигляді:

$$H_{СПОКТГ}(t) = f_{СПОКТГ} \left\{ \begin{matrix} H_{УСПОКТГ}(t); \\ H_{НОКТГ}(t); \end{matrix} \right\}, \quad (7)$$

Для оцінювання управління ОПСО суб'єктами підготовки, навченості об'єктів ОПСО пропонується використовувати часткові показники.

Частковий показник "управління ОПСО штабу  $H_{УСПШ}(t)$ " залежить від повноти і якості планування ОПСО штабу (ОКТГ), організаційної структури і формування в ній управлінської ієрархії ОПСО штабу (ОКТГ), сукупність спонукальних стимулів суб'єктів підготовки та своєчасному виявленні відхилень у підготовці суб'єктами підготовки ОПСО штабу (ОКТГ). Тоді функціональна залежність матиме вигляд:

$$H_{УСПШ}(t) = f_{УСПШ} \left\{ \begin{matrix} M_{ПСП}(t); M_{ОРГСП}(t); \\ M_{МСП}(t); M_{КСП}(t) \end{matrix} \right\}, \quad (8)$$

$$H_{УСПОКТГ}(t) = f_{УСПОКТГ} \left\{ \begin{matrix} M_{ПСП}(t); \\ M_{ОРГСП}(t); \\ M_{МСП}(t); \\ M_{КСП}(t) \end{matrix} \right\}, \quad (9)$$

де:  $M_{ПСП}(t), M_{ОргСП}(t), M_{МСП}(t), M_{КСП}(t)$  – показники, які характеризують “планування СПСО штабу (ОКПГ)”, “організацію СПСО штабу (ОКПГ)”, “мотивацію ОПСО штабу (ОКПГ)” та “контроль ОПСО штабу (ОКПГ)”.

Частковий показник “навченість штабу НС ВМС (МО ДПС)  $H_{Нш}(t)$  (ОКПГ)  $H_{Нокпг}(t)$ ” залежить від сукупного рівня індивідуальних спроможностей кожного флагманського спеціаліста штабу (командира корабля) та взаємодії флагманських фахівців штабу (злагодження ОКПГ). Тоді функціональна залежність матиме наступний вигляд:

$$H_{Нш}(t) = f_{Нш} \{ C_{ICш}(t); C_{Вф}(t) \}, \quad (10)$$

де:  $C_{ICш}(t); C_{Вф}(t)$  – показники “сукупний рівень індивідуальних спроможностей флагманського

спеціаліста штабу”, взаємодія флагманських фахівців штабу”;

$$H_{Нокпг}(t) = f_{Нокпг} \left\{ \begin{matrix} C_{ICкк}(t); \\ C_{Зокпг}(t) \end{matrix} \right\}, \quad (11)$$

де:  $C_{ICкк}(t); C_{Зокпг}(t)$  – показники “сукупний рівень індивідуальних спроможностей командирів кораблів ОКПГ”, злагодження ОКПГ”.

Система показників, яка використовується для оцінювання ефективності ОПСО наведена на рисунку 1.

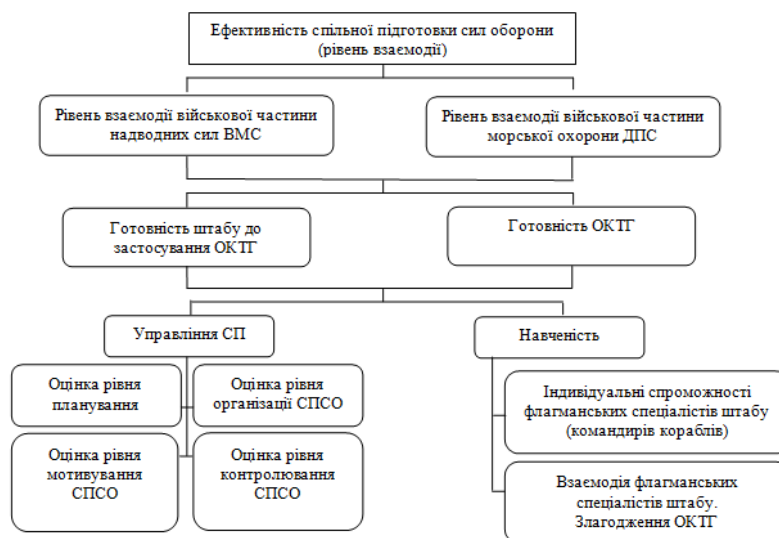


Рис. 1. Система показників оцінювання ефективності об’єднаної підготовки сил оборони військової частини надводних сил ВМС та морської охорони ДПС

Метод згортки показників дозволяє звести багатокритеріальну задачу до однокритеріальної, а вище зазначені показники усіх рівнів будуть мати різну вагомість. Тому під час їх згортки будуть застосовані відповідні “вагові” коефіцієнти, які розрахуємо методом експертного оцінювання.

Зважаючи на те, що інтегральні показники сильно корельовані, для визначення узагальненого показника  $W_B(t)$  пропонується використовувати нормовану мультиплікативну агрегацію [2]:

$$W_B(t) = E_{ВВМС}(t)q_{ВВМС} \cdot E_{ВМО}(t)q_{ВМО} \quad (12)$$

де:  $E_{ВВМС}(t)$  – значення інтегрального показника “рівень взаємодії військової частини ВМС” на час  $t$ ;

$E_{ВМО}(t)$  – значення інтегрального показника “рівень взаємодії військової частини МО ДПС” на час  $t$ ;

$q_{ВВМС}; q_{ВМО}$  – вагові коефіцієнти інтегральних показників.

### Висновки й перспективи подальших досліджень

Таким чином, зрозумілим є те, що об’єднана підготовки сил оборони покликана вирішити основні питання щодо набуття взаємодії військових формувань і правоохоронних органів, підвищити ефективність виконання бойових та спеціальних завдань в ході спільних дій.

Метою ОПСО буде інтеграція спроможностей ЗС та інших складових сил оборони задля виконання певних завдань за певних умов, ресурсного забезпечення та відповідно до встановлених стандартів.

В подальших дослідженнях слід звернути увагу на:

розвиток системи показників об’єднаної підготовки сил оборони;

удосконалення комплексної методики оцінювання ефективності підготовки сил оборони.

Трансформацію існуючих форм (способів) підготовки військ (сил);

пошук нових нестандартних варіантів бойового навчання, які спроможні максимально реалізувати бойовий потенціал військових частин.

**Література**

1. **Брахман Т.Р.** Многокритериальность и выбор альтернатив в технике / Т.Р. Брахман – М. : Радио, 1984. – 364 с. 2. **Вентцель Е.С.** Исследование операций / Е.С. Вентцель. – М. : “Советское радио”, 1972. – 552 с. 3. Єдиний перелік (каталог) спроможностей Міністерства оборони України та Збройних Сил України: за станом на 28 лис. 2017 р. – К. : МОУ, 2017. – 27 с. (Нормативний документ Міністерства оборони України та Генерального штабу Збройних Сил України.) 4. Концепція підготовки Збройних Сил України : за

станом на 22 лют. 2016 р. – К. : Мін-во оборони України та ГШ ЗСУ, 2016. – 14 с. 5. **Хома В.В.** Вимоги до спільної підготовки і застосування збройних сил та державної прикордонної служби України: Збірник тез доповідей Міжнародної науково-практичної конференції “Інтегроване управління кордоном. Теорія і практика”. 2013. – 130 с. 6. Указ Президента України №240/2016 “Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року “Про Стратегічний оборонний бюлетень України”.

**В ВОПРОСУ ОЦЕНКИ ЭФФЕКТИВНОСТИ ОБЪЕДИНЕННОЙ ПОДГОТОВКИ СИЛ  
ОБОРОНЫ ВОИНСКОЙ ЧАСТИ НАДВОДНЫХ СИЛ ВОЕННО-МОРСКИХ СИЛ И МОРСКОЙ  
ОХРАНЫ ГОСУДАРСТВЕННОЙ ПОГРАНИЧНОЙ СЛУЖБЫ**

*Виктор Панасович Муренко (кандидат военных наук, профессор)  
Виталий Николаевич Безуглий*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*В данной статье, на основе системного анализа практической деятельности определены подходы к оценке эффективности совместной подготовки воинских частей надводных сил Вооруженных Сил Украины и морской охраны Государственной пограничной службы Украины, составных частей сектора безопасности и обороны государства. Обоснован выбор наиболее влиятельных показателей совместной подготовки сил обороны государства, что в свою очередь обеспечат достижение необходимого уровня взаимодействия воинских частей надводных сил Военно-Морских Сил и морской охраны Государственной пограничной службы Украины, и учитывают приобретение штабом возможностей по планированию совместного выполнения задач и применения в ходе выполнения общих задач объединенными тактическими группами, приобретение подразделениями воинских частей надводных сил Военно-Морских Сил и морской охраны Государственной пограничной службы возможностей совместно действовать в составе объединенных корабельных тактических групп. Определенная система показателей максимально раскрывает особенности процесса управления и обучения общей подготовкой сил обороны, которые будут влиять на степень достижения цели совместной подготовки сил обороны государства, а также указывает на их структуру и иерархичность.*

*Ключевые слова: объединенная подготовка сил обороны; надводные сил Военно-Морских Сил; морская охрана Государственной пограничной службы; показатели.*

**ON THE ISSUE OF EVALUATING THE EFFECTIVENESS OF JOINT TRAINING OF THE DEFENSE  
FORCES OF THE MILITARY PART OF THE SURFACE FORCES OF THE NAVAL FORCES AND  
THE MARITIME SECURITY OF THE STATE BORDER GUARD SERVICE**

*Viktor Murenko (Candidate of military sciences, Professor)  
Vitalii Bezuhlyi*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*In this article, based on a systematic analysis of practical activities, approaches to assessing the effectiveness of joint training of military units of the Armed Forces of Ukraine and maritime security of the State Border Service of Ukraine, constituent parts of the security and defense sector of the state are determined. The choice of the most influential indicators of joint training of the State Defense Forces is substantiated, which in turn will ensure the achievement of the necessary level of interaction between the military units of the Naval Forces and the Maritime Protection of the State Border Service of Ukraine, and take into account the acquisition by the staff of opportunities for planning joint execution of tasks and application fulfillment of common tasks by joint tactical groups, acquisition by units of military units of surface forces of the Navy of the State Border Guard Service of the State Opportunity to act jointly within the Joint Tactical Groups. The system of indicators as much as possible reveals the peculiarities of the process of management and training of the general training of the defense forces, which will influence the degree of achievement of the goal of joint training of the defense forces of the state, as well as indicate their structure and hierarchy.*

*Key words: joint training of the Defense Forces; surface warfare forces of the Navy; coast guard State Border Service.*

**References**

1. **Brahman T.R.** Multicriteria and the choice of alternatives in engineering. Brahman - M.: Radio, 1984. - 364 p. 2. **Wentzel ES** Operations research / ES Wentzel. - M.: "Soviet Radio", 1972. - 552 p. 3. Single list (catalog) of the capabilities of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine: as of 28 November. 2017 - K.: MOU, 2017. - 27 p. 4. The concept of training of the Armed Forces of Ukraine: as of February 22. 2016 - K.: Ministry of Defense of Ukraine and the General Staff of the

Armed Forces of Ukraine, 2016. - 14 p. 5. **Homa VV** Requirements for Joint Training and Use of the Armed Forces and the State Border Guard Service of Ukraine: Proceedings of the International Scientific Conference on Integrated Border Management. Theory and Practice ". 2013. - 130 p. 6. Presidential Decree No. 240/2016 "On the Decision of the National Security and Defense Council of Ukraine of May 20, 2016" On the Strategic Defense Bulletin of Ukraine ".

Володимир Іванович Мірненко (доктор технічних наук, професор)  
Сергій Володимирович Кітік

Національний університет оборони України імені Івана Черняхівського, Київ, Україна

## НАПІВМАРКІВСЬКА МАТЕМАТИЧНА МОДЕЛЬ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ ЗЕНІТНОГО РАКЕТНОГО ОЗБРОЄННЯ

В роботі представлено математичну модель технічного обслуговування радіоелектронних засобів зенітного ракетного озброєння, які експлуатуються за планово-попереджувальною стратегією експлуатації. Модель побудована з використанням напівмарківського випадкового процесу. За модель відмов використаний дифузійно-немонотонний закон розподілу, що притаманний для виробів радіоелектронної техніки в наслідок електричних явищ, та враховані помилки першого типу.

Встановлена аналітична залежність коефіцієнта технічного використання від параметрів масштабу і форми дифузійно-немонотонного розподілу, періодичності проведення технічного обслуговування, тривалості повного відновлення зразка техніки, ймовірності надходження сигналу про відмову тощо. Приведені графіки залежності коефіцієнта технічного використання від вказаних параметрів моделі. Доведено існування оптимальної періодичності проведення технічних обслуговувань, при якій забезпечується максимальне значення коефіцієнта технічного використання. Основні результати отримані при використанні чисельного методу розрахунків.

**Ключові слова:** технічне обслуговування; напівмарківський випадковий процес; дифузійно-немонотонний розподіл.

### Вступ

**Постановка проблеми.** Організаторів експлуатації радіоелектронної техніки цікавить рівень її технічної ефективності. При цьому постає питання, яким чином можна впливати на процес експлуатації з метою досягнення максимального значення показників ефективності. Загально визнаними показниками ефективності експлуатації виробів радіоелектронної техніки є коефіцієнт готовності і коефіцієнт технічного використання.

Суттєвим для розрахунку показників ефективності є побудова адекватної моделі процесу технічного обслуговування. Методичні похибки, що обумовлені вибором неадекватної теоретичної моделі, можуть бути досить великими.

Важливе місце під час побудови математичних моделей технічного обслуговування виробів радіоелектронної техніки займає вибір закону розподілу часу безвідмовної роботи цих виробів. До ймовірнісних законів розподілу належать експоненціальний, Вейбула, логарифмічно-нормальний розподіли, що рекомендуються державним стандартом України для практичного використання у залежності від типу виробу і характеру вирішуваної задачі. Ймовірнісно-фізичні розподіли мають певну перевагу перед суто ймовірнісними, тому що їх параметри можуть бути визначені як на основі статистичних характеристик відмов, так і на основі аналізу фізичного процесу відмов. У теперішній час найбільш сучасними вважаються дифузійні закони

розподілу, а саме: дифузійно-монотонний і дифузійно-немонотонний розподіли.

Вказані обставини мають суттєве практичне значення, що обумовлює актуальність дослідження.

**Аналіз останніх досліджень і публікацій.** В роботі [1] розглянута можливість побудови адекватної аналітичної моделі процесу технічного обслуговування та ремонту складного об'єкта радіоелектронної техніки у вигляді напівмарківського процесу. Під час дослідження було виявлено значні труднощі, пов'язані з необхідністю визначення аналітичних виразів для інтенсивності переходів між станами процесу. Тому авторами для створення моделі запропоноване використання методу імітаційного статистичного моделювання.

В [2,3] представлені математичні моделі технічних обслуговувань за станом зразків техніки з використання дифузійних розподілів віх відмов. Розраховані аналітичні залежності показників ефективності експлуатації вказаних зразків від характеристик їх надійності і параметрів технічного обслуговування.

Проте дані роботи не можуть бути використані для розрахунку показників ефективності експлуатації виробів радіоелектронної техніки, які експлуатуються за планово-попереджувальною стратегією експлуатації.

**Метою статті** є розробка адекватної математичної моделі технічного обслуговування

радіоелектронних засобів зенітного ракетного озброєння, які експлуатуються за планово-попереджувальною стратегією експлуатації.

**Виклад основного матеріалу дослідження**

Переважає частина радіоелектронних засобів зенітного ракетного озброєння, які експлуатуються за планово-попереджувальною стратегією експлуатації підлягає проведенню профілактичних заходів через визначений час. Такі заходи в багатьох випадках прийнято називати регламентними роботами або роботами технічного обслуговування, які проводяться через невідповідний інтервал часу. В проміжках часу між технічними обслуговуваннями можливі відмови техніки, які будемо називати аварійними. В разі виникнення аварійної відмови проводиться повне відновлення зразка техніки. Крім аварійних відмов, можуть бути так звані помилкові відмови, коли від вбудованої системи контролю надходить сигнал про відмову справної техніки. Такі відмови прийнято називати помилками першого роду, які

складають приблизно 5% від загальних відмов.

Вбудована система контролю постійно контролює окремі найбільш важливі або узагальнені показники працездатності виробу, наприклад напругу джерел живлення, працездатність систем термостатування, потужність передавача, коефіцієнт шуму приймача, коефіцієнти підсилення радіоканалів тощо.

Зовнішня система контролю використовується під час проведення робіт технічного обслуговування для перевірки технічних параметрів та їх настроювання в межі допусків, що визначені в технічній документації. Така система контролює набагато більше параметрів і має значно більшу достовірність контролю, ніж вбудована система контролю.

Для скорочення будемо позначати зовнішню систему контролю ЗСК, а вбудовану систему контролю ВСК.

Схематичне зображення переходів для запропонованої моделі показано на рис.1.

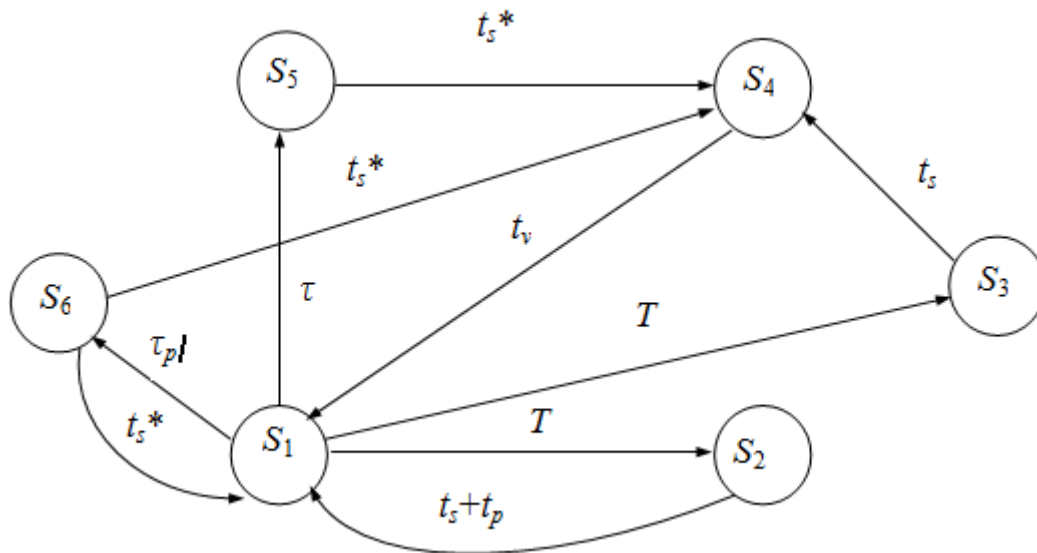


Рис. 1. Схема переходів для запропонованої моделі

Для скорочення зразок радіоелектронної техніки будемо називати об'єктом контролю (ОК). Схема переходів (рис.1) враховує наступні стани ОК і системи контролю (СК):

$S_1$  – ОК працює за призначенням у працездатному стані;

$S_2$  – на ОК проводиться контроль технічного стану наземною системою контролю та виконуються профілактичні роботи, причину в ОК відмови немає;

$S_3$  – на ОК проводиться контроль технічного стану наземною системою контролю, причому в ОК є відмова, яка виникла на переході  $S_1$ –  $S_3$  в момент  $0 < \tau < T$ , не була виявлена вбудованою системою контролю і не вплинула на працездатність ОК;

$S_4$  – виконується повне відновлення ОК;

$S_5$  – в момент часу  $0 < \tau < T$  вбудованою системою контролю зафіксована відмова ОК;

$S_6$  – в момент  $0 < \tau_p < T$  вбудованою системою контролю зафіксований помилковий сигнал про відмову ОК.

На рис.1. використовуються такі позначення:

$T$  – період проведення регламентних робіт;

$t_s$  – тривалість перевірки ОК системою контролю ВСК;

$t_s^*$  – тривалість перевірки ОК системою контролю ЗСК;

$t_p$  – тривалість виконання профілактичних робіт;

$t_v$  – тривалість аварійного відновлення;

$\tau$  – випадковий час надходження від ВСК сигналу про відмову;

$\tau_p$  – випадковий час надходження від ВСК помилкового сигналу про відмову.

На рис.2. показаний ідеальний варіант експлуатації ОК.

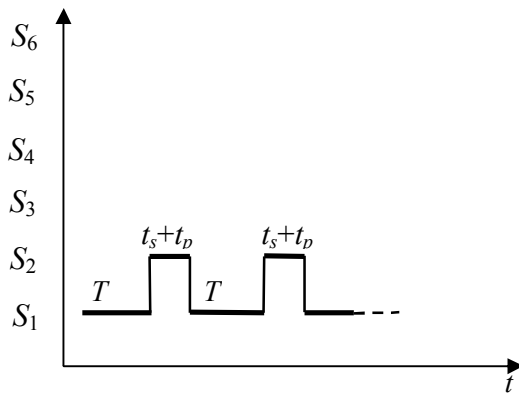


Рис.2. Ідеальний варіант експлуатації ОК

Протягом часу  $T$  ОК працює у справному стані, після чого проводиться контроль технічного стану (час  $t_s$ ) і виконуються профілактичні роботи протягом часу  $t_p$ , після чого ситуація багатократно повторюється.

Можливий варіант реальної експлуатації показаний на рис. 3.

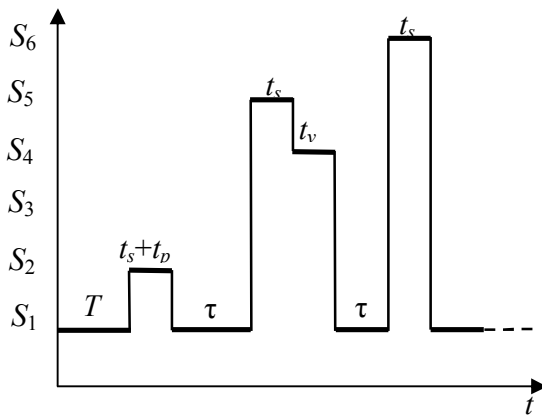


Рис.3. Можливий варіант реальної експлуатації ОК

На рис. 2 і рис. 3 по вертикальній вісі відкладені стани перебування ОК, а по горизонтальній вісі відкладений поточний час.

Процес функціонування ОК будемо описувати напівмарківським випадковим процесом. Особливістю такого процесу є те, що тривалість перебування ОК у попередньому стані при переході до наступного стану може мати довільний закон розподілу. Ця обставина суттєво розширює можливості моделювання процесу експлуатації ОК порівняно з марківським випадковим процесом, для якого така функція розподілу є експоненціальною. Доведено, що максимального коефіцієнту готовності можна досягти при детермінованому періоді проведення регламентних робіт.

Важливе значення під час розробки математичної моделі функціонування ОК має вибір математичної моделі відмов. Для виробів радіоелектронної техніки найбільш придатним вважається дифузійно-немонотонний (DN) закон розподілу часу безвідмовної роботи [4].

Функція розподілу та ймовірність безвідмовної роботи для такого закону розподілу мають вигляд відповідно:

$$F(t) = \Phi\left(\frac{t-\mu}{\nu\sqrt{\mu t}}\right) + \exp\left[2\nu^{-2}\right]\Phi\left(-\frac{t+\mu}{\nu\sqrt{\mu t}}\right) \quad (1)$$

$$P(t) = \Phi\left(\frac{\mu-t}{\nu\sqrt{\mu t}}\right) - \exp\left(2\nu^{-2}\right)\Phi\left(-\frac{\mu+t}{\nu\sqrt{\mu t}}\right), \quad (2)$$

де  $t$  – поточний час;

$\mu$  – параметр масштабу;

$\nu$  – параметр форми;

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x \exp\left(-\frac{t^2}{2}\right) dt \quad \text{– функція Лапласа}$$

Параметр масштабу має розмірність год, а параметр форми – безрозмірний.

Початковими даним, які враховуються у розрахунковій задачі, є:

параметр масштабу  $\mu=200$  год;

параметр форми  $\nu = 0,5$ ;

інтенсивність надходження сигналів помилкових тривог  $\lambda=10^{-3}$  1/год;

період проведення технічних обслуговувань  $T=200$  год;

тривалість контролю зразка техніки наземними засобами контролю  $t_s=2,5$  год;

тривалість контролю зразка техніки вбудованими засобами контролю  $t_s^*=1$  год;

тривалість виконання профілактичних робіт  $t_p=4$  год;

тривалість аварійного відновлення ОК  $t_v=5$  год;

ймовірність надходження сигналу про відмову зразка техніки від вбудованої системи контролю  $\rho=0,7$ ;

достовірність правильного визначення справного стану ОК вбудованими засобами контролю  $d=0,9$ .

Коефіцієнт технічного використання ОК можна визначити з рівняння [5]

$$K_{tv} = \frac{\sum_{i=1}^6 \pi_i(T) \cdot \omega_i(T)}{\sum_{i=1}^6 \pi_i(T) \cdot \eta_i(T)}, \quad (3)$$

де  $\pi_i(T)$  – частота потрапляння ланцюга Маркова до стану  $i$ ;

$\omega_i(T)$  – середній час перебування ОК у працездатному стані;

$\eta_i(T)$  – середній час перебування ОК у будь-якому стані.

У чисельнику (3) записаний середній час перебування ОК у працездатному стані, а у знаменнику – поточний час експлуатації ОК.

Частота потрапляння ланцюга Маркова до стану  $i$   $\pi_i(T)$  може бути визначена з системи рівнянь (4).

$$\left. \begin{aligned} \bar{\pi}_i(T) &= \bar{\pi}_i(T) \cdot P_{ij}(T) \\ \sum_{i=1}^6 \pi_i(T) &= 1 \end{aligned} \right\}, \quad (4)$$

де  $\bar{\pi}_i(T)$  – вектор потрапляння ланцюга Маркова до стану  $i$ ;

$P_{ij}(T)$  – матриця переходів ОК зі стану  $i = \overline{1,6}$  до стану  $j = \overline{1,6}$ .

Матриця перехідних ймовірностей для запропонованої моделі має вигляд

$$P_{ij}(T) = \begin{pmatrix} 0 & P_{12} & P_{13} & 0 & P_{15} & P_{16} \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ d & 0 & 0 & 1-d & 0 & 0 \end{pmatrix} \quad (5)$$

де  $P_{12} = P(T)e^{-\lambda t}$ ;

$$P_{13} = (1-\rho) \int_0^T e^{-\lambda t} dF(t);$$

$$P_{15} = \rho \int_0^T e^{-\lambda t} dF(t);$$

$$P_{16} = \lambda \int_0^T e^{-\lambda t} [1-F(t)] dt.$$

Сума ймовірностей по кожному рядку матриці (5) повинна дорівнювати одиниці. Для всіх рядків, окрім першого, це очевидно.

Враховуючи значення  $F(t)$  і  $P(t)$  для DN-розподілу для початкових даних, отримаємо значення компонентів матриці перехідних ймовірностей

$$P_{ij}(200) = \begin{pmatrix} 0 & 0,4093 & 0,1304 & 0 & 0,3043 & 0,1558 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0,9 & 0 & 0,1 & 0 & 0 & 0 \end{pmatrix}.$$

Сума ймовірностей по першому рядку матриці дорівнює одиниці, що свідчить про вірність виконаних розрахунків.

Після підстановки матриці (5) в рівняння (4) можна отримати значення компонент вектора  $\bar{\pi}_i(T)$  шляхом розв'язання наступних рівнянь

$$a(T) = \frac{1}{1 + P_{12} + 2P_{13} + 2P_{15} + P_{16}(2-d)};$$

$$\pi_1(T) = a(T);$$

$$\pi_2(T) = a(T)P_{12};$$

$$\pi_3(T) = a(T)P_{13};$$

$$\pi_4(T) = a(T) \cdot (P_{13} + P_{15} + P_{16} \cdot [1-d]);$$

$$\pi_5(T) = a(T)P_{15};$$

$$\pi_6(T) = a(T)P_{16}.$$

Можна переконатися, що сума ймовірностей компонент вектора  $\bar{\pi}_i(T)$  дорівнює одиниці, що свідчить про адекватність розрахунку, виконаного за допомогою даного методу.

Далі здійсимо розрахунок середніх тривалостей перебування ОК у різних станах напівмарківського процесу. Наприклад, для стану  $S_7$  отримаємо

$$\eta_1(T) = [1 - F(T)] \cdot e^{-\lambda T} + (1-\rho) \cdot \int_0^T e^{-\lambda t} \times \\ \times dF(t) \cdot T + \rho \int_0^T e^{-\lambda t} \cdot dF(t) \cdot \int_0^T t \cdot dF_5(t) + \\ + \lambda \cdot \int_0^T e^{-\lambda t} [1 - F(t)] dt \cdot \int_0^T t \cdot dF_6(t) \quad (6)$$

Можна показати, що для початкових даних моделі  $\eta_1(T) = 163,82$  год,  $\eta_2(T) = t_p + t_r = 6,5$  год,

$\eta_3 = t_s + t_r = 6,5$  год,  $\eta_4 = 5$  год,  $\eta_5 = t_s^* = 1$  год,  $\eta_6 = 1$  год.

Здійсимо розрахунок середнього часу одного переходу напівмарківського процесу:

$$\eta_s(t) = \pi_1(t) \cdot \eta_1(t) + \pi_2(t) \cdot \eta_2(t) + \pi_3(t) \cdot \eta_3(t) + \\ + \pi_4(t) \cdot \eta_4(t) + \pi_5(t) \cdot \eta_5(t) + \pi_6(t) \cdot \eta_6(t) = 69,18 \text{ год.}$$

Для розрахунку коефіцієнта технічного використання визначимо середній час безвідмовної роботи ОК у стані  $S_7$ :

$$\omega_1(T) = \int_0^T (1 - F(x)) \cdot e^{-\lambda x} \cdot dx = 155,88 \text{ год.}$$

Коефіцієнт технічного використання у точці  $T=200$  год з урахуванням рівняння (4) буде

$$K_{tv} = \frac{\pi_1(200) \cdot \omega_1(200)}{\eta_s(200)} = 0,9196.$$

Для визначення залежності  $K_{tv}$  від параметрів моделі у широких межах їх змін виконано розрахунки чисельним методом. Графічна інтерпретація отриманих результатів наведена на рис. 4-7. Так, на рис. 4 показана залежність  $K_{tv}$  від періодичності  $T$  проведення технічних обслуговувань при зміні параметра форми  $v$  від 1 до 0,25 при  $\mu=600$  год;  $\lambda=10^{-3}$  1/год;  $t_s=2,5$  год;  $t_s^*=1$  год;  $t_p=4$  год;  $t_r=5$  год.



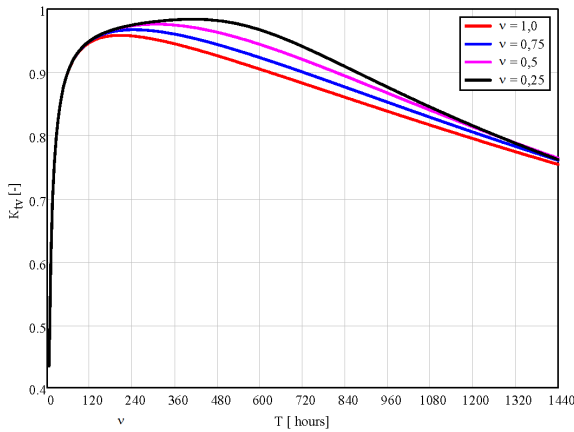


Рис. 4. Залежність  $K_{tv}$  від періодичності  $T$  проведення технічних обслуговувань при зміні параметра форми  $\nu$  від 1 до 0,25 при  $\mu=600$  год;  $\lambda=10^{-3}$  1/год;  $t_s=2,5$  год;  $t_s^*=1$  год;  $t_p=4$  год;  $t_v=5$  год

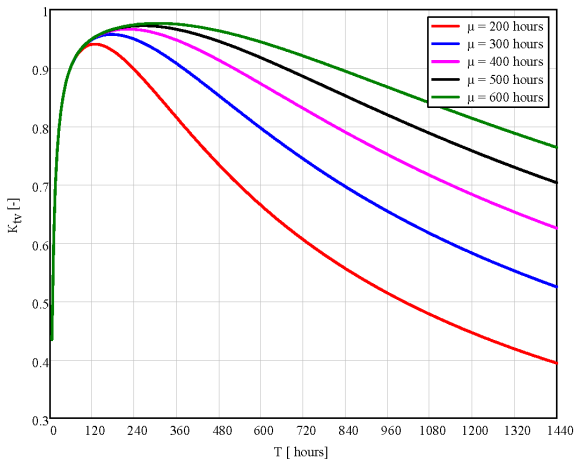


Рис. 5. Залежність  $K_{tv}$  від періодичності  $T$  проведення технічних обслуговувань при значенні параметра форми  $\nu=0,5$  і зміні параметра масштабу  $\mu$  від 200 до 600 год при  $\lambda=10^{-3}$  1/год;  $t_s=2,5$  год;  $t_s^*=1$  год;  $t_p=4$  год;  $t_v=5$  год

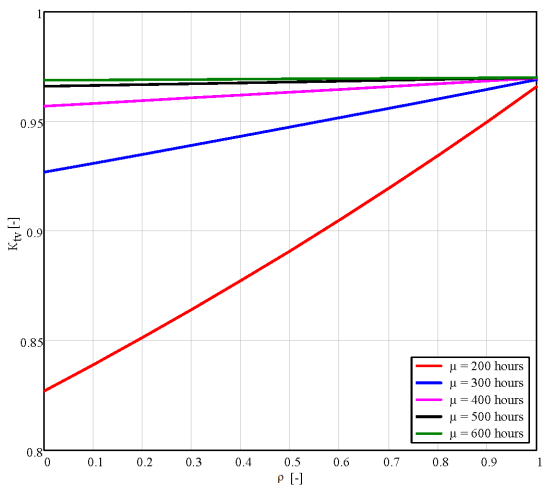


Рис. 6. Залежність  $K_{tv}$  від ймовірності надходження сигналу про відмову від вбудованої системи контролю при різних значеннях параметра масштабу  $\mu$  і постійних значеннях  $\nu=0,5$ ;  $T=200$  год;  $t_s=2,5$  год;  $t_s^*=1$  год;  $t_p=4$  год;  $t_v=5$  год

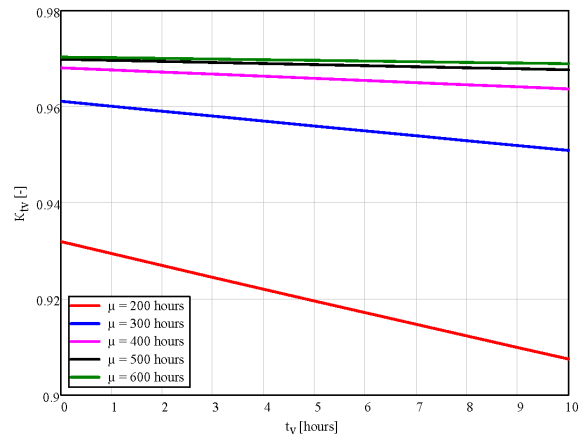


Рис. 7. Залежність  $K_{tv}$  від тривалості аварійного відновлення  $t_v$  зразка техніки при різних значеннях параметра масштабу  $\mu$  і постійних значеннях  $\nu=0,5$ ;  $T=200$  год;  $t_p=4$  год;  $\lambda=10^{-3}$  1/год;  $t_s=2,5$  год;  $t_s^*=1$  год

Аналіз наведених графіків показує (рис. 4) наявність оптимальної періодичності проведення технічних обслуговувань, при якій забезпечується максимальне значення  $K_{tv}$ . При цьому, чим меншим є параметр форми  $\nu$ , тим більшим є  $K_{tv}$ . У даній роботі використані середні значення параметра форми.

При збільшенні параметру масштабу від  $\mu=200$  год до  $\mu=600$  (рис. 5) збільшується  $K_{tv}$ , а також збільшується оптимальне значення періодичності проведення технічних обслуговувань.

При збільшенні ймовірності надходження сигналу про відмову зразка техніки від вбудованої системи контролю  $\rho$  (рис. 6)  $K_{tv}$  збільшується. При цьому для більших значень параметра масштабу забезпечується більше значення  $K_{tv}$ .

Збільшення тривалості відновлення зразка техніки призводить до зменшення  $K_{tv}$  (рис. 7).

### Висновки й перспективи подальших досліджень

В роботі з використанням напівмарківського випадкового процесу побудована математична модель технічного обслуговування радіоелектронних засобів зенітного ракетного озброєння, які експлуатуються за планово-попереджувальною стратегією експлуатації, особливою якої є врахування помилок першого роду з використанням шести станів. Встановлена аналітична залежність коефіцієнта технічного використання від параметрів масштабу і форми, періодичності проведення технічного обслуговування, ймовірності надходження інформації про відмову, тривалості відновлення зразка техніки та інших параметрів моделі.

Визначено існування оптимальної періодичності проведення технічного обслуговування, при якій досягається максимальне значення коефіцієнта технічного використання.

Напрямок подальших досліджень є створення методики оцінювання ефективності технічного обслуговування радіоелектронних засобів з використанням представленої моделі.

### Література

1. С.В. Ленков, В.М. Цицарєв, В.О. Осипа, В.О. Браун Математическая модель процесса технического обслуживания и ремонта сложных объектов радиоэлектронной техники. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. Київ. 2013. № 39. С. 12-19. 2. П.М. Яблонский, С.А. Пустовой, П.В. Опенько Экономико-математическая модель технического обслуживания образцов вооружения и военной техники по состоянию для диффузионно-немонотонного распределения отказов. *Экономика и предпринимательство*. Москва. 2013. № 8. С. 436-443. 3. В.И. Мирненко, П.М. Яблонский, С.А. Пустовой, А.В. Авраменко Математическая модель технического обслуживания изделий авиационной техники с использованием диффузионно-монотонного распределения отказов. *Оралдың Ғылым Жаршысы*. Уралнаучкнига. 2014. №21 (100). С.12-22. 4. ДСТУ 3433-96 Надійність техніки. Моделі відмов Основні положення. *Держстандарт України*. Київ. 1997. 5. ДСТУ 2862-94. Надійність техніки. Методи розрахунку показників надійності. *Держстандарт України*. Київ. 1994.

## ПОЛУМАРКОВСКАЯ МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ ЗЕНИТНОГО РАКЕТНОГО ВООРУЖЕНИЯ

*Владимир Иванович Мирненко (доктор технических наук, профессор)  
Сергей Владимирович Китик*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*В работе представлена математическая модель технического обслуживания радиоэлектронных средств зенитного ракетного вооружения, которые эксплуатируются по плано-предупредительной стратегии эксплуатации. Модель построена с использованием полумарковского случайного процесса. В качестве модели отказов использован диффузионно-немонотонный закон распределения, свойственный для изделий радиоэлектронной техники вследствие электрических явлений, и учтены ошибки первого типа.*

*Установлена аналитическая зависимость коэффициента технического использования от параметров масштаба и формы диффузионно-немонотонного распределения, периодичности технического обслуживания, продолжительности полного восстановления образца техники, вероятности поступления сигнала об отказе. Приведены графики зависимости коэффициента технического использования от указанных параметров модели. Доказано существование оптимальной периодичности проведения технических обслуживаний, при которой обеспечивается максимальное значение коэффициента технического использования. Основные результаты получены при использовании численного метода вычислений.*

*Ключевые слова:* техническое обслуживание; полумарковский случайный процесс; диффузионно-немонотонные распределение.

## SEMI-MARKOV MATHEMATICAL MODEL OF RADIO ELECTRONIC MAINTENANCE OF ANTI-AIR MISSILE ARMS

*Volodymyr Mirnenko (Doctor of Technical Sciences, Professor)  
Serghij Kitik*

*National Defense University of Ukraine named after Ivan Chernyakhovskiy, Kiev, Ukraine*

*The paper presents a mathematical model of maintenance of electronic equipment for anti-aircraft missile weapons, which are operated according to a planned preventive operation strategy. The model is constructed using a semi-Markov random process. As a model of failures, a diffusion-nonmonotonic distribution law is used, which is typical for electronic products due to electrical phenomena, and errors of the first type are taken into account.*

*The analytical dependence of the technical utilization coefficient on the parameters of the scale and shape of the diffusion-nonmonotonic distribution, the frequency of maintenance, the duration of the complete restoration of the equipment sample, the probability of a failure signal is established. The graphs of the dependence of the technical utilization coefficient on the indicated model parameters are given. The existence of an optimal frequency of technical maintenance is proved, at which the maximum value of the coefficient of technical use is ensured. The main results were obtained using the numerical calculation method.*

*Key words:* maintenance; semi-Markov random process; non-monotonic diffusion distribution.

### References

1. S.V. Lénkov, V.M. Tsitsarév, V.O. Osipa, V.O. Braun Matematicheskaya model' protsessa tekhnicheskogo obsluzhivaniya i remonta slozhnykh ob"yektov radioelektronnoy tekhniki. *Zbirnik naukovikh prats' V'ys'kovogo institutu Kiivs'kogo natsional'nogo universitetu imeni Tarasa Shevchenka*. Kíiv. 2013. № 39. S. 12-19. 2. P.M. Yablonskiy, S.A. Pustovoy, P.V. Open'ko Ekonomiko-matematicheskaya model' tekhnicheskogo obsluzhivaniya obraztsov voozuzheniya i voyennoy tekhniki po sostoyaniyu dlya diffuzionno-nemonotonnogo raspredeleniya otkazov. *Ekonomika i predprinimatel'stvo*. Moskva. 2013. № 8. S. 436-443. 3. V.I. Mirnenko, P.M. Yablonskiy, S.A. Pustovoy, A.V. Avramenko Matematicheskaya model' tekhnicheskogo obsluzhivaniya izdeliy aviatsionnoy tekhniki s ispol'zovaniem diffuzionno-monotonnogo raspredeleniya otkazov. *Oraldyñ Gylým Zharslysy*. Uralnauchkniga. 2014. №21 (100). S.12-22. 4. DSTU 3433-96 Nadiynist' tekhniki. Modeli vidmov Osnovni polozhennya. *Derzhstandart Ukraini*. Kíiv. 1997. 5. DSTU 2862-94. Nadiynist' tekhniki. Metodi rozrakhunku pokaznykiv nadiynosti. *Derzhstandart Ukraini*. Kíiv. 1994.

*Артем Олексійович Москаленко* (кандидат технічних наук)<sup>1</sup>

*Юрій Вікторович Глуховець* (кандидат технічних наук, доцент)<sup>1</sup>

*Василь Володимирович Варич* (кандидат технічних наук, доцент)<sup>1</sup>

*Сергій Олександрович Івко* (кандидат технічних наук)<sup>2</sup>

<sup>1</sup>Полтавський інститут бізнесу ПВНЗ «Міжнародний науково-технічний університет імені академіка Юрія Бугая», Полтава, Україна

<sup>2</sup>Військовий коледж сержантського складу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Полтава, Україна

## МЕТОДИКА ЗАСТОСУВАННЯ СИГНАЛІВ УДОСКОНАЛЕНОЇ МОДУЛЯЦІЇ ЦИКЛІЧНИМ ЗСУВОМ КОДУ З АДАПТАЦІЄЮ ПО ШВИДКОСТІ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ В ПЕРСПЕКТИВНИХ РАДІОІНТЕРФЕЙСАХ

В роботі представлено результати аналізу напрямів розвитку систем радіозв'язку спеціального призначення. Запропоновано методику застосування сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передавання інформації в перспективних радіоінтерфейсах. Розглянуто порядок оцінювання середовища розповсюдження радіохвиль та передавання і прийом сигналів управління; моделі формування та кореляційної обробки сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передавання інформації.

Запропонована методика застосування сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації в перспективних радіоінтерфейсах. Використання запропонованої методики застосування сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації в перспективних радіоінтерфейсах дозволить забезпечити високу пропускну здатність та спектральну ефективність, для даних умов розповсюдження радіохвиль.

**Ключові слова:** модуляція циклічним зсувом коду; методи адаптивної модуляції; радіоінтерфейс.

### Вступ

**Постановка проблеми.** В умовах, коли розвиток науки і технологій дозволяє постійно вдосконалювати системи озброєння, бойову та спеціальну техніку, різко змінюються форми і способи ведення бойових дій, зростає кількість і ускладнюється характер зв'язків між підрозділами силових структур, до їх управління пред'являються більш високі вимоги.

Постійно збільшується обсяг завдань управління, кількість необхідної для їх вирішення вихідної інформації, значно скорочується час циклів управління. Тому зростають вимоги до забезпечення командирів і штабів стійким, безперервним, оперативним та прихованим зв'язком, підвищенням його захищеності, мобільності і пропускну здатності.

Крім того, сучасні системи радіозв'язку спеціального призначення функціонують в умовах дефіциту радіоресурсу та активного радіоелектронного подавлення.

Для забезпечення вищезгаданих завдань та викликів, перспективні системи радіозв'язку спеціального призначення повинні створюватися на основі адаптивних радіотехнологій та мати

здатність зміни випромінюваної потужності і несучих частот в залежності від завадової обстановки і умов розповсюдження радіохвиль в даних умовах та використовуваних частотних діапазонах.

Крім того, відповідно до Концепції розвитку телекомунікацій в Україні [1], одним із основних напрямів розвитку телекомунікацій в Україні є: розвиток широкосмугового абонентського доступу з використанням перспективних технологічних рішень.

Тому тема дослідження є досить актуальною у наш час.

**Аналіз останніх досліджень і публікацій.** В роботах [2] розглянуті питання синтезу сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації, запропонований алгоритм їх кореляційної обробки, приведені правила формування сигналів адаптивної модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації та правила функціонування пристрою вирішення цифрового кореляційного приймача сигналів адаптивної CSSK-модуляції.

В [3,4] проведено дослідження перешкодостійкості сигналів модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації та перешкодостійкості сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації в умовах багатопроменевого розповсюдження радіохвиль.

Проте в даних роботах не розглянуті питання практичного застосування сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації в перспективних радіо інтерфейсах.

**Метою статті** є забезпечення високої пропускну здатності та спектральної ефективності, для даних умов розповсюдження радіохвиль, шляхом впровадження методики застосування сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації в перспективних радіоінтерфейсах.

### Виклад основного матеріалу дослідження

Оцінювання середовища розповсюдження радіохвиль відбувається наступним чином. У обчислювальному пристрої прийомо-передавача здійснюється аналіз характеристик каналу

передачі інформації. Далі відбувається автоматична адаптація схеми модуляції з метою отримання максимальної швидкості передавання інформації для даних умов розповсюдження радіохвиль. Приймально-передавальний пристрій здійснює прийом сигналу від абонента, якому в подальшому буде здійснюватись передавання інформації (рис. 1).

При цьому, форма та інші характеристики вхідного сигналу завчасно відомі. Далі відбувається обробка даного вхідного сигналу на узгодженому фільтрі, за результатами обробки формується співвідношення сигнал/шум. В пристрої управління здійснюється оцінювання співвідношення сигнал/шум і, у відповідності до алгоритму роботи пристрою управління, здійснюється вибір схеми модуляції та порядку обробки інформаційного сигналу джерела повідомлення. Крім того, у пристрої управління здійснюється формування сигналів управління для приймача кореспондента (пунктирна стрілка рис.1).

В приймально-передавальному пристрої кореспондента (рис. 2) здійснюється приймання інформаційних модульованих сигналів та сигналів управління (пунктирна стрілка рис. 2).

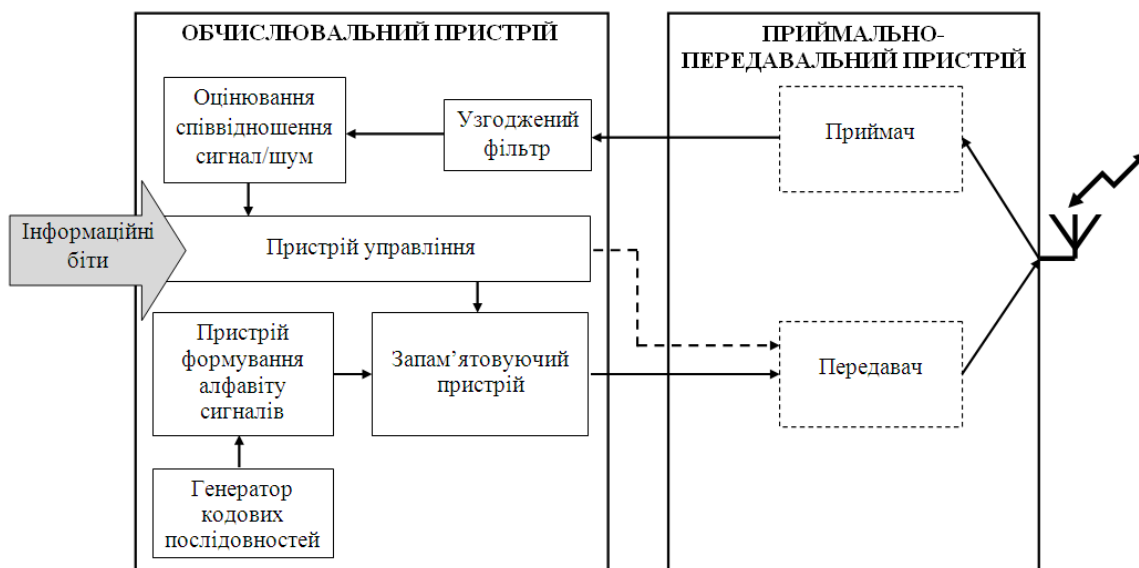


Рис. 1. Порядок передавання сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передавання інформації

У пристрої вирішення, відбувається формування вихідних інформаційних біт на основі вхідного інформаційного сигналу та сигналу управління.

Застосування даного підходу дозволяє мінімізувати ймовірність виникнення помилки на прийомі.

*Модель формування сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передавання інформації*

Порядок передавання сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації зображено на рис. 1.

На початковому етапі формується кодова послідовність у відповідності до заздалегідь обраного типу та характеристик. Процедура формування послідовності здійснюється в генераторі кодових послідовностей (рис. 1).

Згенерована кодова послідовність надходить до пристрою формування алфавіту сигналів. У даному пристрої, у відповідності до правил формування сигналів модуляції циклічним зсувом коду [5], відбувається формування алфавіту сигналів та запис його до запам'ятовуючого пристрою (рис. 1).

В пристрої управління, у відповідності до заздалегідь запрограмованого алгоритму,

здійснюється вибір сигналу із сформованого алфавіту, що підлягає подальшому передаванню. Вхідними даними для цього процесу є оцінене значення співвідношення сигнал\шум та вхідні інформаційні біти джерела повідомлення. Приклад правил формування сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передавання інформації приведено на

рис. 3. У даному прикладі, генератор кодів послідовностей генерує двовимірні послідовності. У пристрої формування алфавіту сигналів здійснюється циклічна перестановка двовимірної послідовності, перетворення в одновимірну послідовність шляхом розгортання двовимірної по рядкам.

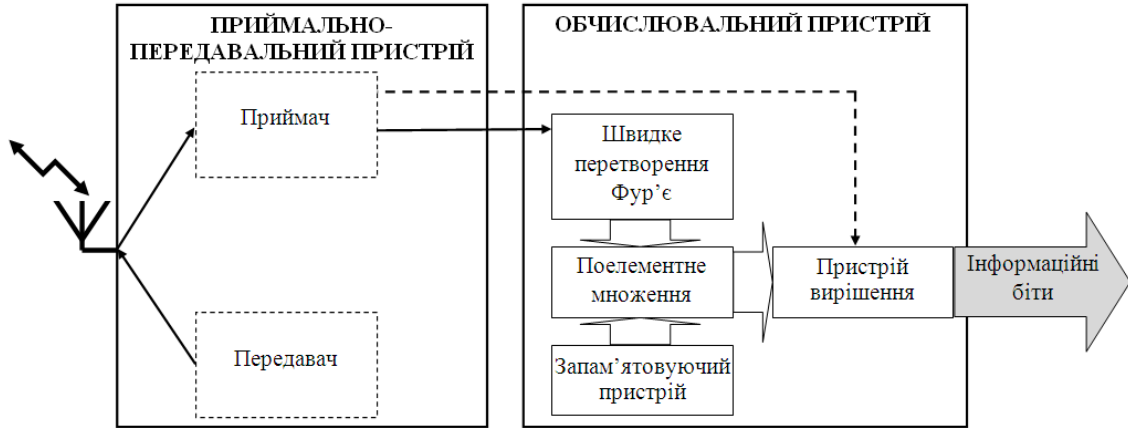


Рис. 2. Порядок прийому сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передавання інформації

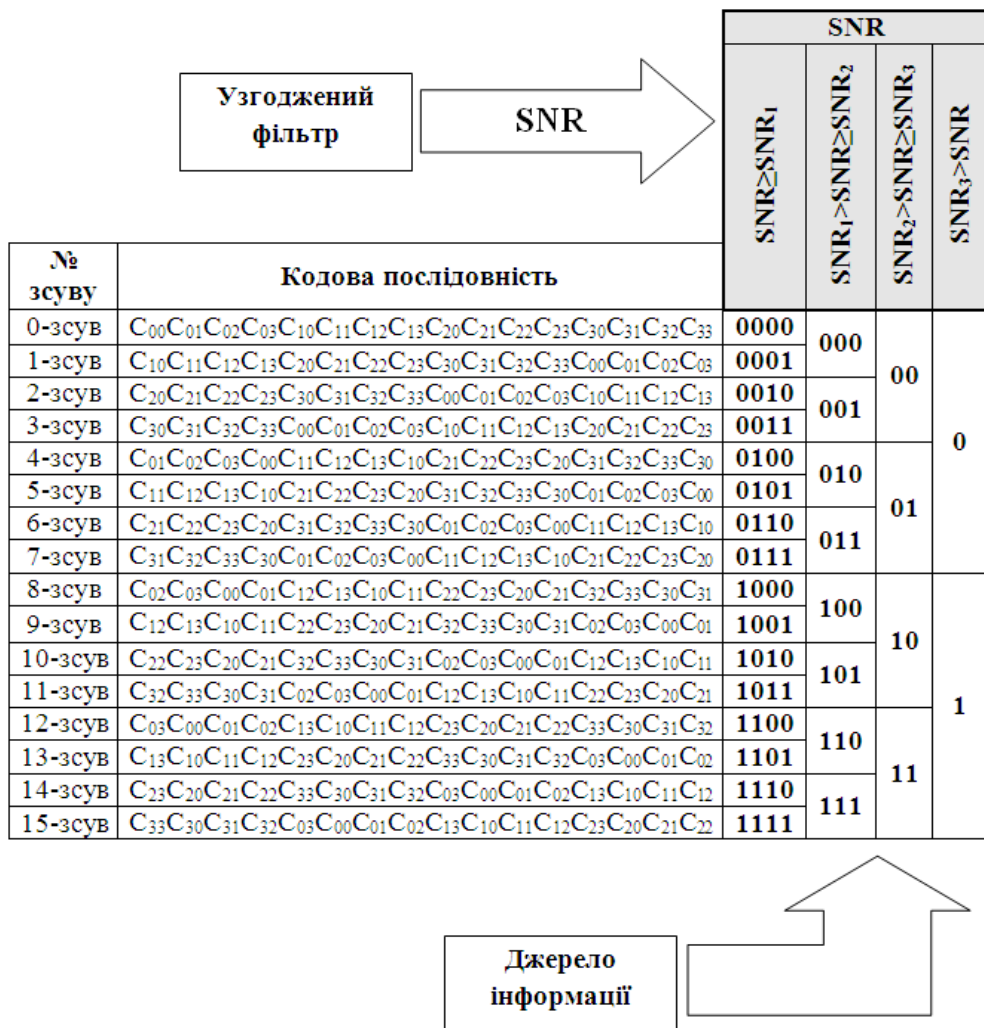


Рис. 3. Приклад правил формування сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передавання інформації

Для даного прикладу у пристрої управління зберігаються заздалегідь уведені значення  $SNR_1$ ,  $SNR_2$  та  $SNR_3$ .  $SNR$  (Signal-to-noise ratio) – співвідношення сигнал/шум визначається як відношення потужності сигналу (значимої інформації) до потужності фонового шуму у даній смузі частот. Якщо значення  $SNR$ , що надійшло від узгодженого фільтру, більше або рівне значенню  $SNR_1$ , що зберігається в пристрої управління, потік інформаційних біт розбивається на четвірки біт. Кожній четвірці відповідає одне значення послідовності алфавіту сигналів (рис. 3). Далі відбувається вибір необхідної послідовності з подальшою її передачею.

Якщо  $SNR$  знаходиться в межах

$SNR_1 > SNR \geq SNR_2$ , то потік інформаційних біт розбивається на трійки біт. Кожній трійці відповідає два значення послідовності алфавіту сигналів (рис. 3). Далі відбувається вибір необхідної послідовності з подальшою її передачею. При подальшому зменшенні значення  $SNR$  формування сигналів відбувається аналогічним чином.

*Модель кореляційної обробки сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передавання інформації*

Приклад кореляційної обробки сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передавання інформації приведено на рис. 4.

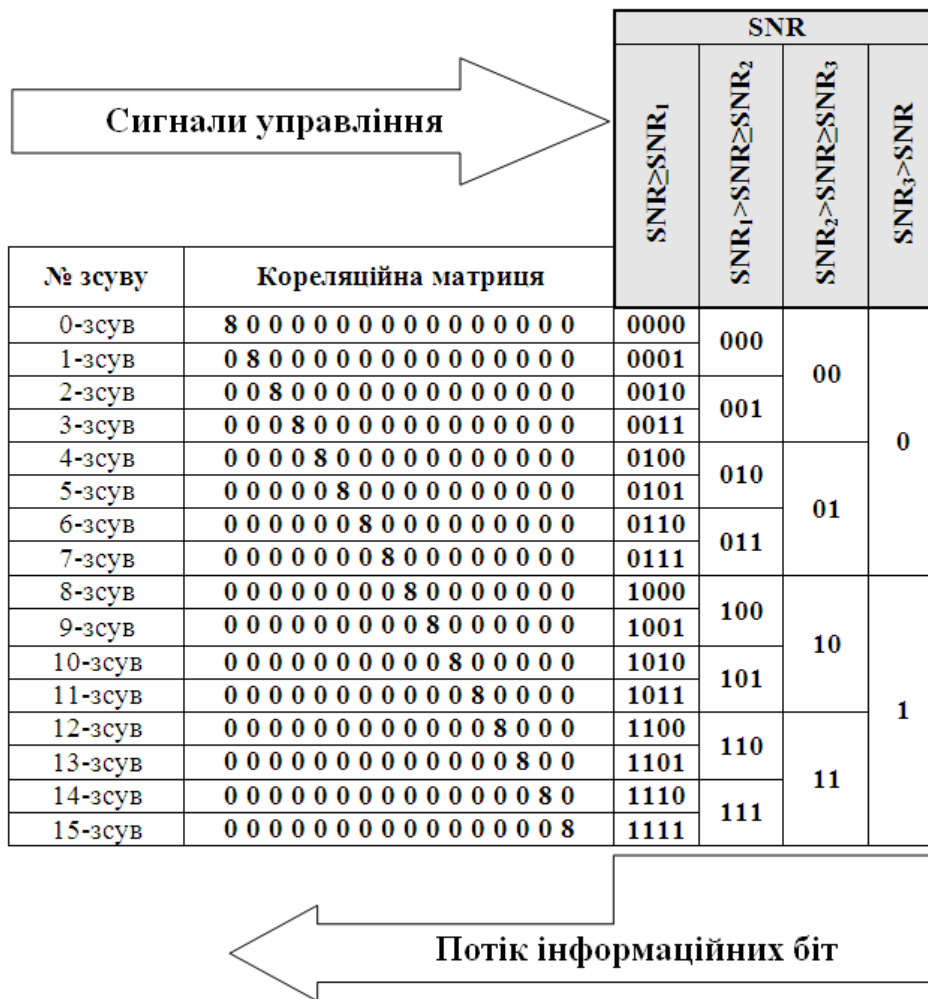


Рис. 4. Приклад кореляційної обробки сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передавання інформації

В тракці прийому сигнали управління надходять з приймача на пристрій вирішення обчислювального пристрою (рис. 3).

Порядок кореляційної обробки запропонованих сигналів є аналогічним обробці сигналів з модуляцією циклічним зсувом коду [5]. Різниця полягає у принципі роботи пристрою вирішення.

В даному випадку прийнятий сигнал управління надходить з приймача на пристрій вирішення. Для даного прикладу сигнал управління буває 4 типів:

- перший тип –  $SNR \geq SNR_1$ ;
- другий тип –  $SNR_1 > SNR \geq SNR_2$ ;
- третій тип –  $SNR_2 > SNR \geq SNR_3$ ;
- четвертий тип –  $SNR_3 > SNR$ .

При надходженні сигналу управління першого типу кожний із шістнадцяти стовпів кореляційної матриці відповідає одній, із шістнадцяти можливих, комбінацій четвірок біт, яка і надходить на інформаційний вихід пристрою (рис. 4).

Якщо з приймача надійшов сигнал управління

другого типу два стани кореляційної матриці відповідають одній, із восьми можливих, комбінацій трійок біт, яка і надходить на інформаційний вихід пристрою. Слід зазначити: стани кореляційної матриці для різних трійок біт не дублюються.

При подальшому зменшенні значення SNR кореляційна обробка сигналів відбувається аналогічним чином.

### **Висновки й перспективи подальших досліджень**

В роботі проведено аналіз напрямів розвитку систем радіозв'язку спеціального призначення. Запропоновано методику застосування сигналів удосконаленої модуляції

циклічним зсувом коду з адаптацією по швидкості передавання інформації в перспективних радіо інтерфейсах.

Використання запропонованої методики застосування сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації в перспективних радіоінтерфейсах дозволить забезпечити високу пропускну здатність та спектральну ефективність, для даних умов розповсюдження радіохвиль.

Напрямок подальших досліджень є дослідження завадостійкості, структурної та енергетичної скритності запропонованих сигналів.

### **Література**

1. Концепція розвитку телекомунікацій в Україні, схвалена Розпорядженням Кабінету Міністрів України від 7 червня 2006 р. № 316-р. 2. **А.О. Москаленко, Г.В. Сокол, Н.В. Рвачова, Т.В. Буряк, Ю.В. Глуховець, В.В. Варич.** Перешкодостійкість сигналів модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації. *Системи управління, навігації та зв'язку.* Київ. 2018. № 3(49). С. 175-180. 3. **А.О. Москаленко, С.В. Волошко, І.І. Слюсарь** Перешкодостійкість сигналів удосконаленої модуляції циклічним зсувом коду з адаптацією по швидкості передачі інформації в умовах багатопробного

розповсюдження радіохвиль. *Сучасні інформаційні технології у сфері безпеки та оборони.* Київ. 2015. № 2 (23). С. 35–39. 4. **А.А. Москаленко, Г.В. Сокол** Метод синтеза сигналов усовершенствованной модуляции циклическим сдвигом кода с адаптацией по скорости передачи информации. *Інформаційно керуючі системи на залізничному транспорті.* Харків. №3 (100). 2013. С. 71-75. 5. **G.M. Dillard et all.,** Cyclic Code Shift Keying: A Low Probability of Intercept Communication Technique // *IEEE Trans. Aerosp. Electron. Systems.,* vol. AES-39, July 2003, pp. 786 -798.

## **МЕТОДИКА ПРИМЕНЕНИЯ СИГНАЛОВ УСОВЕРШЕНСТВОВАННОЙ МОДУЛЯЦИИ ЦИКЛИЧЕСКИМ СДВИГОМ КОДА С АДАПТАЦИЕЙ ПО СКОРОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В ПЕРСПЕКТИВНЫХ РАДИОИНТЕРФЕЙСАХ**

*Артем Алексеевич Москаленко (кандидат технічних наук)<sup>1</sup>*

*Юрий Викторович Глуховец (кандидат технічних наук, доцент)<sup>1</sup>*

*Василий Владимирович Варыч (кандидат технічних наук, доцент)<sup>1</sup>*

*Сергей Александрович Ивко (кандидат технічних наук)<sup>2</sup>*

<sup>1</sup> *Полтавский институт бизнеса ПВУЗ «Международный научно-технический университет имени академика Юрия Бугая», Полтава, Украина*

<sup>2</sup> *Военный колледж сержантского состава Военного института телекоммуникаций и информатизации имени Героев Крут, Полтава, Украина*

*В работе представлены результаты анализа направлений развития систем радиосвязи специального назначения. Предложена методика применения сигналов усовершенствованной модуляции циклическим сдвигом кода с адаптацией по скорости передачи информации в перспективных радиоинтерфейсах. Рассмотрен порядок оценки среды распространения радиоволн и передачи и приеме сигналов управления; модели формирования и корреляционной обработки сигналов усовершенствованной модуляции циклическим сдвигом кода с адаптацией по скорости передачи информации.*

*Предложенная методика применения сигналов усовершенствованной модуляции циклическим сдвигом кода с адаптацией по скорости передачи информации в перспективных радиоинтерфейсах. Использование предлагаемой методики применения сигналов усовершенствованной модуляции циклическим сдвигом кода с адаптацией по скорости передачи информации в перспективных радиоинтерфейсах позволит обеспечить высокую пропускную способность и спектральную эффективность, для данных условий распространения радиоволн.*

**Ключевые слова:** *модуляция циклическим сдвигом кода методы адаптивной модуляции; радиоинтерфейс.*

**METHODS OF APPLICATION OF SIGNALS OF ADVANCED MODULATION BY CYCLIC SHIFT OF THE CODE WITH ADAPTATION ON SPEED OF INFORMATION TRANSMISSION IN PERSPECTIVE RADIO INTERFACES**

*Artem Moskalenko (Candidate of Technical Sciences)<sup>1</sup>*  
*Jurij Ghluhovecj (Candidate of Technical Sciences, Associate Professor)<sup>1</sup>*  
*Vasyly Varych (Candidate of Technical Sciences, Associate Professor)<sup>1</sup>*  
*Serghij Ivko (Candidate of Technical Sciences)<sup>2</sup>*

<sup>1</sup> *Poltava Institute of Business, Poltava Higher Educational Institution «Yuri Bugai International Scientific and Technical University», Poltava, Ukraine*

<sup>2</sup> *Military College of NCOs of the Military Institute of Telecommunications and Informatics named after Kruty Heroes, Poltava, Ukraine*

*This paper presents the results of the analysis of the directions of development of special purpose radio communication systems. The method of application of signals of advanced modulation by cyclic shift of the code with adaptation on speed of information transmission in perspective radio interfaces is offered. The procedure of estimation of radio wave propagation medium and transmission and reception of control signals is considered; models of formation and correlation processing of signals of advanced modulation by cyclic shift of code with adaptation on the speed of information transmission.*

*The technique of application of advanced modulation signals by cyclic code shift with adaptation on the speed of information transmission in perspective radio interfaces is offered. The use of the proposed method of application of signals of advanced modulation by cyclic shift of the code with adaptation on the speed of transmission of information in perspective radio interfaces will allow to provide high bandwidth and spectral efficiency, for these conditions of radio wave propagation.*

**Key words:** *cyclic code shift modulation; methods of adaptive modulation; radio interface.*

### **References**

1. Концепція розвитку телекомунікацій в Україні, схвалена Розпорядженням Кабінету Міністрів України від 7 червня 2006 р. № 316-р.
2. **A.O. Moskalenko, Gh.V. Sokol, N.V. Rvachova, T.V. Burjak, Ju.V. Ghluhovecj, V.V. Varych.** Pereshkodostijkistj syghnaliv moduljaciji cyklichnym zsumom kodu z adaptacijeu po shvydkosti peredachi informaciji. *Systemy upravlinnja, navighaciji ta zv'jazku.* Kyjiv. 2018. № 3(49). S. 175-180.
3. **A.O. Moskalenko, S.V. Voloshko, I.I. Sljusarj** Pereshkodostijkistj syghnaliv udoskonalenoji moduljaciji cyklichnym zsumom kodu z adaptacijeu po shvydkosti peredachi informaciji v umovakh baghatopromenevogho rozpovsjudzhennja radiokhvylyj. *Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony.* Kyjiv. 2015. № 2 (23). S. 35–39.
4. **A.A. Moskalenko, Gh.V. Sokol** Metod synteza syghnalov usovershenstvovanoj moduljaciji cyklicheskyj s dvjohom kodu s adaptaciej po skorosty peredachy ynfornacyy. *Informacijno kerujuchi systemy na zaliznychnomu transporti.* Kharkiv. №3 (100).2013.S.71-75.
5. **G.M. Dillard et all.** Cyclic Code Shift Keying: A Low Probability of Intercept Communication Technique // *IEEE Trans. Aerosp. Electron. Systems.*, vol. AES-39, July 2003, pp. 786 -798.



*Ігор Олександрович Ляшенко (кандидат військових наук)<sup>1</sup>*

*Оксана Миколаївна Ключак<sup>2</sup>*

*Світлана Петрівна Зелінська<sup>2</sup>*

<sup>1</sup>*Київський Національний економічний університет імені Вадима Гетьмана, Київ, Україна*

<sup>2</sup>*Національний університет оборони України імені Івана Черняхівського, Київ, Україна*

## БЕЗПЕРЕРВНІ ДИНАМІЧНІ МОДЕЛІ НАДІЙНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО- УПРАВЛЯЮЧИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

*Розглядається можливість застосування безперервних динамічних моделей для оцінки надійності програмного забезпечення інформаційно-управляючих систем спеціального призначення. За умови досягнення високої надійності, сучасна техніка стає ефективною та конкурентоспроможною. Саме від показника надійності похідними будуть інші, не менш важливі показники – якість, живучість, безпека, готовність – а це основні показники, що визначають ефективність інформаційно-управляючих систем спеціального призначення. Переважна більшість досліджень в цьому напрямку поняття надійності програмного забезпечення виділяє окремо, тому, що при застосуванні понять надійності до програмних засобів варто враховувати особливості і відмінності цих об'єктів від традиційних технічних систем, для яких спочатку розроблялася теорія надійності. Принципова відмінність програм від техніки, та технічних систем зокрема, полягає в тому, що програма не зношується з плином часу, а навпаки, виявляються помилки, які не були знайдені раніше, програмне забезпечення з часом вдосконалюється і покращується.*

**Ключові слова:** безперервні динамічні моделі; оцінка надійності; програмне забезпечення; інформаційно-управляючі системи спеціального призначення.

### Вступ

Розвиток інформаційних технологій та комп'ютерної техніки та всебічне проникнення її в усі сфери життєдіяльності людини передбачає постановку нових задач для розробників програмного забезпечення. Програмні продукти стають дедалі складнішими, багатокomпонентними і вимагають спеціалізованого підходу.

За умови досягнення високої надійності, сучасна техніка стає ефективною та конкурентоспроможною. Саме від показника надійності похідними будуть інші, не менш важливі показники – якість, живучість, безпека, готовність – а це основні показники, що визначають ефективність інформаційно-управляючих систем спеціального призначення.

**Постановка проблеми.** Переважна більшість досліджень в цьому напрямку поняття надійності програмного забезпечення (ПЗ) виділяє окремо [1], тому, що при застосуванні понять надійності до програмних засобів варто враховувати особливості і відмінності цих об'єктів від традиційних технічних систем, для яких спочатку розроблялася теорія надійності. Принципова відмінність програм від техніки, та технічних систем зокрема, полягає в тому, що програма не зношується з плином часу, а навпаки, виявляються помилки, які не були знайдені раніше, програмне забезпечення з часом вдосконалюється і покращується.

**Аналіз останніх досліджень і публікацій.** Для розв'язання завдань оцінки та прогнозування надійності на даний час використовують цілий ряд різноманітних моделей надійності ПЗ [1–8].

### Виклад основного матеріалу дослідження

Модель надійності програмного забезпечення передбачає побудову математичної моделі для оцінки залежності надійності програмного забезпечення від певних параметрів. Такими параметрами є частота помилок, які дозволяють оцінити якість систем реального часу, що функціонують в безперервному режимі, і в той же час отримувати непряму інформацію про надійність ПЗ [3].

На сьогоднішній день виділяють наступні типи моделей надійності [9]:

- аналітичні;
- динамічні;
- статичні;
- емпіричні.

Найбільш широко на сьогоднішній день використовуються динамічні моделі [2, 4, 10] на основі неоднорідного пуассонового процесу, в яких вихідні дані збираються в процесі тестування ПЗ протягом фіксованих або випадкових часових інтервалів. Кожен інтервал являє собою стадію, на якій виконується деяка послідовність тестів та виявляється деяка кількість помилок.

В даній роботі пропонується розглянути особливості безперервних динамічних моделей оцінки надійності програмного забезпечення. Проаналізувати їх переваги та недоліки з метою виявлення доцільності їх застосування для оцінки надійності програмного забезпечення інформаційно-управляючих систем спеціального призначення.

*Модель Jelinski–Moranda.*

Дана модель [11] побудована на припущенні, що час до чергової відмови розподілено експоненціально, а інтенсивність відмов програмного забезпечення пропорційна кількості помилок, що залишилися в програмі.

Відповідно до цих припущень імовірність безвідмовної роботи програмного забезпечення як функція часу  $t_i$  дорівнює [4]

$$P(t_i) = e^{-\lambda_i t_i},$$

де:  $\lambda_i$  – інтенсивність відмов.

$$\lambda_i = C_D(N - (i - 1)),$$

де:  $C_D$  – коефіцієнт пропорційності;

$N$  – апріорна кількість помилок.

Розрахунок часу  $t_i$  починається з моменту останньої відмови програмного забезпечення.

За методом максимуму правдоподібності, позначимо через  $k$  номер відмови, що прогнозується, та отримаємо функцію правдоподібності вигляду

$$F = \prod_{i=1}^{k-1} C_D(N - i + 1) e^{-C_D(N - i + 1)t_i}.$$

Логарифмічна функція правдоподібності має вигляд

$$L = \ln F = \sum_{i=1}^{k-1} [\ln(C_D(N - i + 1)) - C_D(N - i + 1)t_i]$$

Відповідно умови знаходження екстремума

$$\frac{dL}{dC_D} = \sum_{i=1}^{k-1} \left[ \frac{1}{C_D} - (N - i + 1)t_i \right] = 0,$$

$$\frac{dL}{dN} = \sum_{i=1}^{k-1} \left[ \frac{1}{N - i + 1} - C_D t_i \right] = 0.$$

Відповідно можна отримати

$$C_D = \frac{\sum_{i=1}^{k-1} \frac{1}{N - i + 1}}{\sum_{i=1}^{k-1} t_i}.$$

Зробивши відповідну підстановку отримуємо

$$(k - 1) \frac{\sum_{i=1}^{k-1} t_i}{\sum_{i=1}^{k-1} \frac{1}{N - i + 1}} = \sum_{i=1}^{k-1} (N - i + 1)t_i.$$

При відомих значеннях  $k$ ;  $t_1, t_2, \dots, t_k$  можна знайти значення параметрів моделі  $C_D$  та  $N$ , а потім інтенсивність відмов, час між відмовами

$t_{k+1}$ , імовірність безвідмовної роботи через час  $t_{k+1}$  після останньої відмови.

*Модель перехідних ймовірностей Маркова* дозволяє отримати оцінки і прогнози імовірного числа помилок, які будуть виправлені в заданий час, на основі попереднього моделювання інтенсивності помилок, що трапляються  $l$ , а також прийнятої системи виправлення помилок, що працює з інтенсивністю  $m$ . Модель дозволяє отримати прогнози для готовності  $A(t)$  і надійності  $R(t)$  системи програмного забезпечення.

В даній моделі приймаються наступні основні:

будь-яка помилка розглядається як випадкова і без градації наслідків, які вона породжує;

інтенсивність прояву помилок постійна і рівна  $l$ ;

інтенсивність виправлення помилок постійна і рівна  $m$ ;

час переходу системи з одного стану в інший нескінченно малий.

Надійність системи  $R(t)$  визначається імовірністю відсутності відмови в інтервалі  $[0, t]$ :

$$R(t) = P\{t' \geq t\}.$$

Під готовністю системи на час  $t$  розуміється імовірність того, що система знаходиться в робочому стані на час  $t$ :

$$A(t) = P.$$

Будь-який стан системи визначається рядом перехідних ймовірностей  $\{P_{ij}\}$ , де  $P_{ij}$  означає імовірність переходу зі стану  $i$  в стан  $j$  та не залежить від попередніх та наступних станів системи, крім станів  $i$  та  $j$ .

Вираз для готовності системи на час  $t$  ( $t > 0$ ) отримуємо на підставі визначення

$$A(t) = \sum_{k=0}^{\infty} P_{n-k}(t).$$

де:  $n$  – кількість помилок у системі.

Готовність системи на час  $t$  визначається як результат простої суми складання усіх ймовірностей станів зайнятості.

Надійність системи залежить від ступеня її налагодження, тобто чим вище ступінь налагодження системи, тим більше очікувана надійність. Припустимо, що до моменту  $t$  система тільки що увійшла до стану  $(n - k)$ , тобто помилка  $k$  тільки що усунена. Назвемо цей час як  $t$ . Тоді в інтервалі часу  $(0, T_k + 1)$ , де в  $t = T_k + 1$  може виявитися помилка  $(k + 1)$  при прийнятій постійній інтенсивності прояву помилок  $l_k$ .

На підставі формули функції надійності, що породжує імовірність відсутності відмов в інтервалі часу від 0 до  $t$ ,  $R(t) = e^{-\lambda t}$ , отримуємо вираз для надійності:

$$R_k(\tau) = e^{-\lambda_k \tau}; \quad 0 \leq \tau \leq T_{k+1}; \quad k = 0, 1, 2, \dots$$

## Висновки й перспективи подальших досліджень

Розглянуті безперервні динамічні моделі оцінки надійності програмного забезпечення маючи деякі недоліки (поведінка системи прогнозується під час функціонування у

середньому; не передбачається внесення нових помилок при виправленні виявлених) дають можливість прогнозувати характеристики системи шляхом моделювання до початку роботи, або після закінчення роботи системи. А це, на сьогодні дуже актуально.

## Література

1 А.М.Попов Основы теории надежности / Попов А.М., Гуров С.В. / – СПб.: БХВ – Петербург, 2006. – 704 с.  
2. Липаев В.В. Надежность программных средств / Липаев В.В. / – М.: СИНТЕГ, 1998. – 232 с. 3. Тайер Т. Надежность программного обеспечения / Тайер Т., Липов М., Нельсон Э. / Пер. с англ. – М.: МИР, 1981. – 323 с. 4. Монахов Ю.М. Функциональная устойчивость информационных систем. В 3 ч. Ч. 1. Надежность программного обеспечения : учеб. пособие / Ю. М. Монахов / Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2011. – 60 с. – ISBN 978-5-9984-0189-3. 5. Ляшенко І.О. Розрахунок надійності функціонування інформаційно-управляючих систем спеціального призначення / Ляшенко І.О., Кузьмічов Д.А., Кравченко І.Ю. / Збірник наукових праць / інститут проблем моделювання в енергетиці НАНУ. № 64. К.: 2012. – С. 31-35. 6. Ляшенко І.О. Аналіз динамічних дискретних моделей оцінки надійності програмного забезпечення / Ляшенко І.О., Кузьмічов Д.А., Кравченко І.Ю. / Збірник наукових праць / інститут проблем моделювання в енергетиці НАНУ. № 65. К.: 2012. – С. 41-45. 7. Ляшенко І.О. Аналіз

статичних моделей оцінки надійності програмного забезпечення інформаційно-управляючих систем спеціального призначення / Ляшенко І.О., Кузьмічов Д.А. / Моделювання та інформаційні технології, збірник наукових праць / інститут проблем моделювання в енергетиці НАНУ. № 65. К.: 2012. – С. 47-51. 8. Ляшенко І.О. Аналіз безперервних динамічних моделей оцінки надійності програмного забезпечення інформаційно-управляючих систем спеціального призначення / Ляшенко І.О., Кузьмічов Д.А. / Моделювання та інформаційні технології, збірник наукових праць / інститут проблем моделювання в енергетиці НАНУ. № 66. К.: 2012. – С. 58-62. 9. Казарин О.В. Теория и практика защиты программ / Казарин О.В. / – М.: МГУЛ, 2004. – 450 с. 10. K.-Y. Cai, D.-B. Hu, Ch.-G. Bai, H. Hu, T. Jing Does software reliability growth behavior follow a non-homogeneous Poisson process // Information and Software Technology. – Vol. 50. – 2008. – P. 1232–1247. 11. Z. Jelinski and P. Moranda Software reliability research // in Statistical Computer Performance Evaluation. – W. Freiberger, Ed. – New York: Academic. – 1972. – P. 465–484.

## НЕПРЕРЫВНЫЕ ДИНАМИЧЕСКИЕ МОДЕЛИ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

*Игорь Александрович Ляшенко (кандидат военных наук)<sup>1</sup>  
Оксана Николаевна Ключак<sup>2</sup>  
Светлана Петровна Зелинская<sup>2</sup>*

<sup>1</sup>Киевский Национальный экономический университет имени Вадима Гетьмана, Киев, Украина

<sup>2</sup>Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Рассматривается возможность применения непрерывных динамических моделей для оценки надежности программного обеспечения информационно-управляющих систем специального назначения. При условии достижения высокой надежности, современная техника становится эффективной и конкурентоспособной. Именно показатели надежности производными будут другие, не менее важные показатели – качество, живучесть, безопасность, готовность - а это основные показатели, определяющие эффективность информационно-управляющих систем специального назначения. Подавляющее большинство исследований в этом направлении понятие надежности программного обеспечения выделяет, потому, что при применении понятий надежности к программным средствам следует учитывать особенности и различия этих объектов от традиционных технических систем, для которых изначально разрабатывалась теория надежности. Принципиальное отличие программ от техники, и технических систем в частности, заключается в том, что программа не изнашивается со временем, а наоборот, выявляются ошибки, которые не были найдены ранее, программное обеспечение со временем совершенствуется и улучшается.

**Ключевые слова:** непрерывные динамические модели; оценка надежности; программное обеспечение; информационно-управляющие системы специального назначения.

## UNLIMITED DYNAMIC MODELS ADVANCED SOFTWARE INFORMATION-CONTROLLING SYSTEMS FOR SPECIAL APPOINTMENT

*Igor Lyashenko (candidate of military sciences)<sup>1</sup>  
Oksana Kliuchak<sup>2</sup>  
Svitlana Zelinska<sup>2</sup>*

<sup>1</sup>*Kiev National Economic University named after Vadim Getman, Kiev, Ukraine*  
<sup>2</sup>*National Defense University of Ukraine named by Ivan Cherniakhovsky, Kyiv, Ukraine*

*The possibility of using continuous dynamic models to assess the reliability of special-purpose information management systems is considered. With the achievement of high reliability, modern technology becomes efficient and competitive. It is the reliability indicator that the derivatives will be other, equally important indicators - quality, survivability, safety, availability - and these are the main indicators that determine the effectiveness of special-purpose information and control systems. The overwhelming majority of research in this direction highlights the concept of software reliability, because when applying the concepts of reliability to software, one should take into account the features and differences of these objects from traditional technical systems for which the theory of reliability was originally developed. The fundamental difference between programs and technology, and technical systems in particular, is that the program does not wear out over time, but rather, errors that were not found earlier are detected, the software improves and improves over time.*

**Key words:** *continuous dynamic models; reliability assessment; software; information and control systems for special purposes.*

### References

- 1 A.M.Popov** Fundamentals of the theory of reliability / Popov A.M., Gurov S.V. / - St. Petersburg: BHV - Petersburg, 2006. -- 704 p.
- 2. Lipaev V.V.** Reliability of software tools / Lipaev V.V. / - M.: SINTEG, 1998. - 232 p.
- 3. Thayer T.** Reliability of software / Thayer T., Lipov M., Nelson E. / Per. from English - M.: MIR, 1981. - 323 p.
- 4. Monks Yu.M.** Functional stability of information systems. At 3 hours. Part 1. Software reliability: textbook. allowance / Yu. M. Monakhov / Vladim. state un-t - Vladimir: Publishing house Vladim. state University, 2011. - 60 p. - ISBN 978-5-9984-0189-3.
- 5. Lyashenko I.O.** Rozrahunok nadinosti funktsionuvannya informatsiynogovernig systems of special purpose / Lyashenko I.O., Kuzmichov D.A., Kravchenko I.Yu. / Zbirnik naukovih prac / Institute of Model Modeling in Energy of NASU. No. 64. K.: 2012. - S. 31-35.
- 6. Lyashenko I.O.** Analysis of dynamic discrete models for evaluating the reliability of software / Lyashenko I.O., Kuzmichov D.A., Kravchenko I.Yu. / Zbirnik naukovih prac / Institute of Model Modeling in Energy of NASU. No. 65. C.: 2012. - S. 41-45e
- 7. Lyashenko I.O.** Analysis of static models of evaluation of software security and information-control systems of special designation / Lyashenko I.O., Kuzmichov D.A. / Modeling and information technology, science institute / Institute for Modeling Problems in Energy of NASU. No. 65. K.: 2012. - S. 47-51.
- 8. Lyashenko I.O.** Analysis of uninterrupted dynamic estimation models of software security and information-control systems of special designation / Lyashenko I.O., Kuzmichov D.A. / Modeling and information technology, science institute / Institute for Modeling Problems in Energy of NASU. No. 66. K.: 2012. - S. 58-62.
- 9. Kazarin O.V.** Theory and practice of program protection / Kazarin O.V. / - M.: MGUL, 2004. - 450 p.
- 10. K.-Y. Cai, D.-B. Hu, Ch.-G. Bai, H. Hu, T. Jing** Does software reliability growth behavior follow a non-homogeneous Poisson process // Information and Software Technology. - Vol. 50. - 2008. - P. 1232-1247.
- 11. Z. Jelinski and P. Moranda** Software reliability research // in Statistical Computer Performance Evaluation. - W. Freiberger, Ed. - New York: Academic. - 1972. - P. 465-484.

Володимир Петрович Котляров (доктор технічних наук, професор)  
Олександр Анатолійович Кузнєцов

Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

## ЩОДО ПИТАННЯ ВИЗНАЧЕННЯ РАЦІОНАЛЬНИХ СПОСОБІВ ВИКОНАННЯ ЗАВДАНЬ З УРАХУВАННЯМ ЗАДАЧ РОЗПОДІЛУ

У статті розглядається область досліджень, у якій поєднуються в межах єдиного методичного апарату розв'язання одночасно декількох задач, а саме: розподілу за завданнями плану та способами виконання кожного з них.

Структурно виділяються три етапи досліджень. На першому етапі формуються варіанти можливих способів виконання завдань з дискретністю: одна група – одне завдання. Фактично тут формується множина варіантів-претендентів, із яких у подальшому буде вибраний найкращий.

На другому етапі послідовно виконуються розрахунки, починаючи з визначення парето-ефективних варіантів і закінчуючи вибором з варіантів-претендентів найкращого на основі таксономічних підходів.

На третьому етапі розв'язується оптимізаційна задача розподілу. У рамках цього етапу при визначенні більше ніж однієї групи для виконання одного завдання уточнюються способи дій у плані взаємодії.

**Ключові слова:** розподіл за завданнями; спосіб виконання завдання; показники ефективності; методичний апарат; багатовимірна задача.

### Вступ

**Постановка проблеми.** Під час вироблення оптимального плану органом управління, як правило, розглядається декілька варіантів дій, з яких для безпосереднього планування вибирається більш доцільний. При цьому посадові особи мають проаналізувати завдання, оцінити обстановку та розробити пропозиції до плану на підставі проведення багатоваріантних розрахунків, а у деяких випадках і моделювання з використанням різноманітних засобів спеціального математичного і програмного забезпечення.

Це досить багатовимірна задача, що потребує значного обсягу розрахунків, де особливо необхідно окреслити область досліджень, у якій поєднується в межах єдиного методичного апарату розв'язання одночасно декількох задач, а саме: розподілу за завданнями плану та способами виконання кожного з них. Ці актуальні питання й будуть розглянуті у статті.

**Аналіз останніх досліджень і публікацій.** У спеціальній літературі, внаслідок великої розмірності задач, в основному розглядаються підходи, у яких здійснюється декомпозиція процесу на дві окремі області досліджень. У одній з них розглядається задача визначення способу виконання окремого завдання, з огляду на те, що розподіл загальної кількості сил і засобів вже проведено. В іншій області досліджень, навпаки, розв'язується задача розподілу сил і засобів за завданнями, де вже враховується конкретний, завчасно визначений спосіб дій за кожною з них [1].

Однак на практиці досить часто виникає необхідність поєднання двох підходів. Це насамперед стосується варіанту дій, де після розв'язання задачі розподілу знов виникає необхідність коригування способу дій, особливо у випадках, коли на визначене завдання розподіляється декілька груп виконавців (здійснюється нарощування зусиль). Але такий алгоритм, у вигляді аналітичного зворотного зв'язку щодо визначення приросту показників ефективності, в основному залишається за рамками досліджень.

**Мета статті.** Викладення цілісного підходу щодо визначення раціональних способів виконання завдань з урахуванням задач розподілу та можливості визначення приросту показників ефективності під час нарощування зусиль.

### Виклад основного матеріалу дослідження

Загальна структура такого методичного підходу поділяється на три основних етапи.

На першому етапі (рис. 1) формуються варіанти можливих способів виконання завдань з дискретністю: одна група – одне завдання (блок 1.1). Фактично тут формується множина варіантів-претендентів, із яких у подальшому буде вибраний найкращий.

Така деталізація процесу до “елементарної” пари значно звужує область дослідження і, водночас, дозволяє вже на першому етапі підвищити точність обчислень за рахунок більш повного набору факторів. При цьому для об'єктивності розрахунків тут є можливість використання декількох критеріїв (блок 1.2) з

обмеженнями виду 1.3.

Якщо умови блоку 1.3 не виконуються, то здійснюється коригування способів дій, але тільки за тим завданням, де хоча б одна з умов не виконується. В іншому разі на основі розрахункових показників ефективності формуються матриці результатів оцінювання (блок 1.4) окремо для кожного завдання за всіма сформованими з урахуванням умови 1.3 варіантами. Ці матриці є основою для подальших розрахунків.

Слід зазначити, що перехід задачі в ранг багатокритеріальної потребує використання окремого алгоритму розрахунків, який застосовується на другому етапі (рис. 2) запропонованого методичного підходу, де послідовно виконуються розрахунки, починаючи з визначення парето-ефективних варіантів (блок 2.1) і закінчуючи у блоці 2.4 вибором з варіантів-претендентів (блок 1.1) найкращого на основі таксономічних підходів.

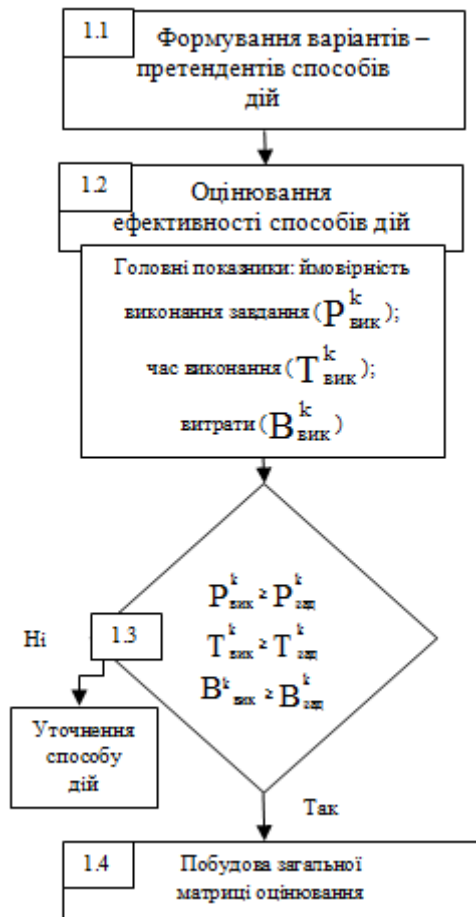


Рис. 1 Розрахунок показників оцінювання ефективності способів дій (перший етап)

У таксономічному підході з метою виключення негативного впливу процедури стандартизації, коли кожний із показників здійснює у середньому однаковий вплив на кінцеві результати ранжування варіантів, у блоці 2.2 введено коригування показників ефективності з урахуванням коефіцієнта ієрархії [2, 3].

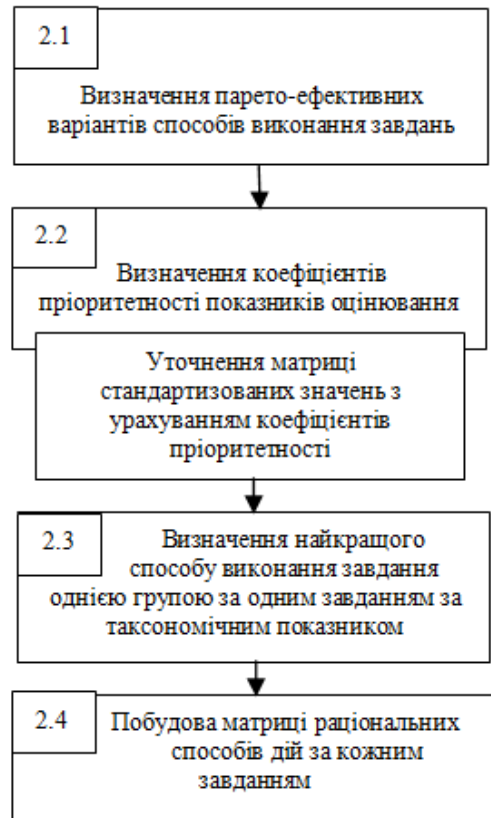


Рис. 2 Порівняння способів дій (другий етап)

Ці коефіцієнти також дозволяють виділити найбільш “впливові” показники ефективності виконання завдань під час можливого коригування складових способів дій, що особливо важливо у подальшому під час уточнення способу дій у процесі взаємодії декількох груп шляхом варіювання найбільш впливових показників.

Таким чином, кінцевим результатом другого етапу є вибір із блоку 2.3 (за пріоритетними рядами таксономічних показників) раціональних способів дій однієї групи за одним завданням, які формують матрицю у блоці 2.4.

Якби умови розподілу сил і засобів полягали у визначенні однієї групи на одне завдання, а загальна кількість груп збігалася з визначеною кількістю завдань, то можна було б вважати, що мета статті досягнута. Але на практиці ці умови не завжди виконуються, що потребує включення до методичного підходу окремого третього етапу (рис. 3), де здійснюється оптимальний розподіл сил і засобів.

Вихідними даними для проведення обчислень на третьому етапі є показники ймовірності виконання завдань з блоку 2.4, а розрахунковий алгоритм визначити не становить складності. У ньому оптимізаційна задача формулюється таким чином. Необхідно знайти розподіл груп для виконання визначених завдань, який забезпечить максимальне значення цільової функції ( $E_{max}$ ), що дорівнює максимальному значенню математичного сподівання кількості виконаних дій.

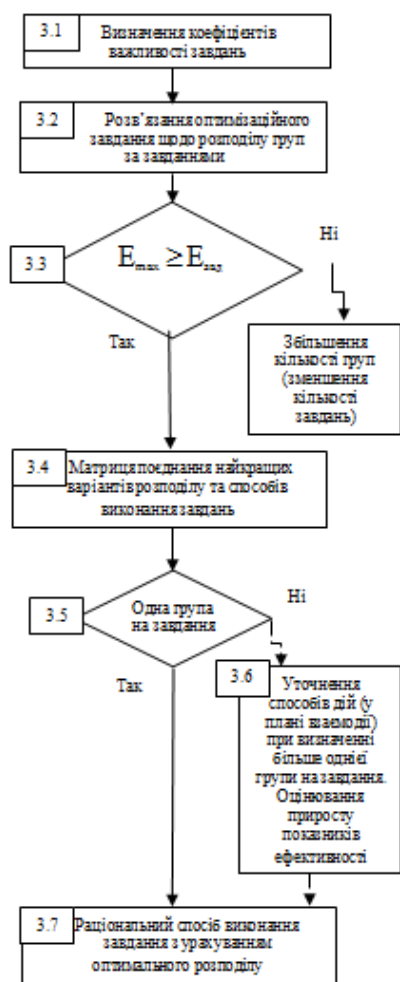


Рис. 3 Розв'язання задачі розподілу (третій етап)

У подальшому у блоці 3.3 показник  $E_{\max}$  порівнюється із заданим значенням  $E_{\text{зад}}$ .

Якщо умова цього блоку не виконується, то здійснюється коригування вихідних даних, а саме збільшення вихідної кількості груп (або зменшення кількості завдань). Якщо умова блоку 3.3 виконується, то визначається раціональний

### Література

1. **Соболев О. М.** Використання комплексу математичних моделей під час проведення досліджень ефективності застосування об'єднань, з'єднань Збройних Сил / О. М. Соболев // Матер. наук.-практ. конф.: Сучасні методи оцінювання ефективності і бойового застосування військ (сил) в операціях (бойових діях) (5 серпня 2004 року). – К.: ЦНДІ ЗС України, 2004.

спосіб виконання завдань з урахуванням оптимального розподілу.

Слід зазначити, що коли на виконання одного завдання за результатами оптимального розподілу визначається більше однієї групи (блок 3.6), то, якщо використовувати розрахунковий алгоритм перших двох етапів методичного підходу, завжди є можливість уточнити способи виконання завдань у плані взаємодії.

Також інтерес представляє й випадок, коли необхідно додатково оцінити приріст показників ефективності (зменшення витрат ресурсів та часу виконання завдання). За таких умов доцільно використовувати метод динаміки середніх, який встановлює аналітичний зв'язок між наведеними параметрами. Позитивний ефект (зменшення витрат ресурсів та часу виконання завдання) досягається за рахунок нарощування зусиль (одне завдання виконується більше ніж однією групою) за незмінності інших умов.

Таким чином, за сукупністю всіх етапів у наведеному методичному підході поєднуються задачі вибору раціональних способів виконання завдань (перший та другий етапи методики) із задачею оптимального розподілу (третій етап).

### Висновки й перспективи подальших досліджень

У статті запропоновано цілісний методичний підхід щодо визначення раціональних способів виконання завдань з урахуванням оптимального розподілу сил і засобів, де на перших двох етапах визначається множина варіантів-претендентів способів виконання завдань, з яких у подальшому на третьому етапі обираються раціональні шляхом розв'язання оптимізаційного завдання розподілу сил і засобів.

Розглянутий підхід передбачає можливість визначення приросту показників ефективності під час нарощування зусиль.

Напрямом подальших досліджень слід вважати програмну реалізацію методики.

## К ВОПРОСУ ОПРЕДЕЛЕНИЯ РАЦИОНАЛЬНЫХ СПОСОБОВ ВЫПОЛНЕНИЯ ЗАДАЧ С УЧЕТОМ ЗАДАЧ РАСПРЕДЕЛЕНИЯ

*Владимир Петрович Котляров (доктор технических наук, профессор)  
Александр Анатолиевич Кузнецов*

*Центральный научно-исследовательский институт Вооруженных Сил Украины, Киев, Украина*

*В статье рассматривается область исследований, в которой объединяются в рамках единого методического аппарата решения одновременно нескольких задач, а именно: распределения по заданиям плана и способам выполнения каждого из них.*

Структурно виділяються три етапи досліджень. На першому етапі формуються варіанти можливих способів виконання задач з дискретністю: одна група – одна задача. Фактично тут формуються множество варіантів-претендентів, з яких в подальшому буде вибран найкращий.

На другому етапі вичислений послідовально виконуються розрахунки, починаючи з визначення парето-ефективних варіантів і закінчуючи вибором з варіантів-претендентів найкращого на основі таксономічних підходів.

На третьому етапі розв'язується оптимізаційна задача розподілу. В межах цього етапу при призначенні більше однієї групи на виконання однієї задачі уточнюються способи дій в плані взаємодії.

**Ключевые слова:** розподілення по задачах; спосіб виконання задачі; показателі ефективності; методический апарат; багатовимірна задача.

## CONCERNING THE QUESTION OF DEFINITION OF RATIONAL WAYS OF PERFORMING THE TASKS CONSIDERING THE PROBLEMS DISTRIBUTION

*Volodymyr Kotliarov (Doctor of Technical Sciences, Professor)*  
*Alexander Kuznetsov*

*Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine*

The article deals with the area of research, which combines several tasks within the framework of a single methodological apparatus of solving multiple tasks at once, namely, the tasks of distribution according to the plan and the ways of performing each of them.

Structurally, there are three stages of research. In the first stage, options are formed for possible ways to perform tasks with discretion: one group - one task. In fact, a number of contenders are being formed here, from which the best will be selected in the future.

In the second stage, calculations are performed sequentially, starting with the identification of pareto-effective variants and ending with the selection of the best-fit options based on taxonomic approaches.

In the third step, the optimization problem of the distribution is solved. As part of this step, when identifying more than one group to accomplish one task, the methods of action in the interaction plan are specified.

**Keywords:** distribution according to the tasks; the way of performing the task; performance metrics methodological apparatus; multidimensional problem.

### References

1. **Sobolev O.M.** Using of math models complex during research of efficiency of Armed Forces formations deployment (2004), [*Vikoristannya kompleksu matematychnykh modeley nid chas provedennya doslidzhen efektyvnosti zastosuvannya obyednan,zyednan Zbroynih syl*], Suchasni metody ocinyuvannya efektyvnosti i boyovogo zastosuvannya viysk (syl) v operaciyah (boyovyh diyah) TsNDI ZS Ukrayiny, Kyiv. 188 p.
2. **Plyuta W.** The Comparative many-dimensional analysis in economic modeling (1989), [*Sravnitelnyi mnogomernyi analiz v ekonomicheskoy modelirovani*], Finansy i Statistika, Moscow, 176 p.
3. **Kosevtsov V.O.** National security of Ukraine: Theory, Reality, Prognosis: monograph. (2000), [*Natsionalna bezpeka Ukrayiny: teoriya, realnist, prognoz: monografija*], TsMBSS, Kyiv, 80 p.



*Ігор Сергійович Романченко* (доктор військових наук, професор)

*Михайло Михайлович Потьомкін* (доктор технічних наук, с.н.с.)

*Олег Петрович Кравець* (кандидат військових наук, с.н.с.)

*Григорій Андрійович Саковський* (кандидат військових наук, с.н.с.)

*Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна*

## КОМПЛЕКСНИЙ МЕТОД РАНЖУВАННЯ ТА ЙОГО ВИКОРИСТАННЯ ДЛЯ БАГАТОКРИТЕРІАЛЬНОГО ПОРІВНЯННЯ АЛЬТЕРНАТИВ

Наведено опис трикритеріального методу ранжування, призначеного для формування пріоритетного ряду альтернатив, та результати його аналізу. При цьому зазначено, що під час розроблення рекомендацій для особи, яка приймає рішення, необхідно не лише визначити найбільш перспективні альтернативи, а й надати обґрунтовані пояснення отриманих результатів, що потребує додаткового аналізу результатів розрахунків. Для зменшення обсягів такого аналізу запропоновано новий метод багатокритеріального порівняння, який передбачає використання декількох комбінацій критеріїв порівняння. При цьому використовуються три однокритеріальні, три двокритеріальні та одне трикритеріальне порівняння. Для цього нового методу наведені формульні залежності, а також надано поетапний опис порядку проведення розрахунків. Можливість практичного застосування запропонованого методу показана на розрахунковому прикладі, для якого у літературних джерелах представлені результати, отримані за відомими багатокритеріальними методами. Порівняння результатів розрахунків за відомими та новим методами свідчить про те, що використання запропонованого методу дає можливість підвищити обґрунтованість розроблених рекомендацій за рахунок підвищення повноти порівняння альтернатив. Це дозволяє зробити висновок, що використання розробленого комплексного методу ранжування може бути достатньо перспективним під час багатокритеріальної оптимізації складних об'єктів.

**Ключові слова:** адитивна згортка; багатокритеріальне ранжування; метод трикритеріального ранжування; метод MOORA; метод VIKOR.

### Вступ

**Постановка проблеми.** Нині під час дослідження проблемних питань як у галузі будівництва збройних сил, так і воєнного мистецтва широко використовуються багатокритеріальні методи, які ґрунтуються на порівнянні альтернатив [1, 2], наприклад, під час формування програм розвитку Збройних Сил, а також визначення раціонального складу угруповань військ (сил). При цьому ці методи повинні забезпечувати обґрунтованість отримуваних результатів.

Тому розроблення методів, які дозволяють підвищити обґрунтованість порівняння альтернатив, є, на наш погляд, актуальним напрямом досліджень.

**Аналіз останніх досліджень і публікацій.** Однією з достатньо поширених задач багатокритеріального порівняння альтернатив є побудова їх пріоритетного ряду, для чого зазвичай розв'язується задача оптимізації у такій постановці.

Нехай є множина альтернативних варіантів деякої системи, кожний з яких характеризується множиною показників. Значення показників задані матрицею  $[E_{ij}]$  ( $i = 1, 2, \dots, n$ ;  $j = 1, 2, \dots, m$ , де  $n$  – кількість альтернатив;  $m$  – кількість показників). Окрім того, є множина коефіцієнтів важливості показників ( $w_j$ ,  $j = 1, 2, \dots, m$ ), а також для кожного показника визначений критерій оптимізації (на максимум або мінімум).

За такими даними необхідно побудувати пріоритетний ряд наявних альтернатив.

У статті [3] наведено метод трикритеріального ранжування, який призначений для розв'язання такої задачі. Послідовність розрахунків за цим методом складається з таких етапів.

На першому етапі здійснюють підготовку вихідних даних, тобто визначають значення показників  $E_{ij}$ , які характеризують кожну альтернативу, а також значення коефіцієнтів важливості  $w_j$ .

На другому етапі здійснюють лінійне нормування вихідних значень показників у інтервал  $[0; 1]$  із забезпеченням перетворення показників, що потребують мінімізації у такі, що потребують максимізації.

На третьому етапі для врахування важливості показників нормалізовані дані масштабують за формулою:

$$g_{ij} = w_j e_{ij}, \quad i = 1, \dots, n; \quad j = 1, \dots, m. \quad (1)$$

На четвертому етапі для кожного показника за масштабованими даними визначають його найкраще  $e_j^+$  значення, яке приймається за найкращий еталон. Значення найгіршого еталону за обраного виду нормування дорівнює нулю.

На п'ятому етапі для кожної  $i$ -ї альтернативи розраховують значення показника  $S_i$ , який

характеризує її наближеність до найкращої точки, за формулою:

$$S_i = \sum_{j=1}^m |(e_j^+ - r_{ij})|, \quad i = 1, \dots, n. \quad (2)$$

На шостому етапі для кожної  $i$ -ї альтернативи розраховують значення показника  $R_i$ , який характеризує її максимальну віддаленість від найкращої точки за показником з найбільшою віддаленістю, за формулою:

$$R_i = \max_j [(e_j^+ - r_{ij})], \quad i = 1, \dots, n. \quad (3)$$

На сьомому етапі для кожної альтернативи визначають значення адитивної згортки

$$A_i = \sum_{j=1}^m r_{ij}, \quad i = 1, \dots, n. \quad (4)$$

На восьмому етапі для кожної альтернативи розраховують узагальнений показник переваги

$$Q_i = (S_i + R_i) / A_i, \quad i = 1, \dots, n. \quad (5)$$

Виходячи з того, що найкраща альтернатива повинна бути максимально наближена до найкращої точки та максимально віддалена від найгіршої, тобто мати найменші значення  $S_i$  і  $R_i$  та найбільше значення  $A_i$ , на заключному (дев'ятому) етапі впорядковують альтернативи за збільшенням  $Q_i$ . При цьому найкращою буде перша альтернатива в отриманому пріоритетному ряду.

Необхідно зазначити, що розглянутий метод забезпечує ранжування альтернатив за узагальненим показником переваги, який, базуючись на часткових показниках, характеризує деякий компроміс щодо віддаленості альтернатив від найкращого та найгіршого еталонів.

Однак, як відомо, остаточне прийняття рішення щодо визначення раціональної альтернативи залишається за особою, яка приймає рішення (ОПР), а результати ранжування є лише деякими рекомендаціями для неї.

При цьому рекомендації, які подаються на розгляд ОПР, повинні достатньо повно характеризувати альтернативи з урахуванням особливостей кожної з них. Тобто подати на розгляд ОПР необхідно не лише отриманий пріоритетний ряд, а й докладний опис суттєвих відмінностей між альтернативами.

Використання розглянутого методу забезпечує лише формальну констатацію факту переваги однієї альтернативи над іншою, а виявлення їх окремих особливостей потребує додаткового аналізу вихідних даних та результатів розрахунків, що може потребувати значного обсягу працевитрат.

Водночас, аналіз розглянутого методу свідчить про те, що виявити відмінності між альтернативами можна шляхом розгляду окремих часткових показників, а також їх комбінацій. Цей підхід фактично передбачає розроблення нового – комплексного – методу, який буде базуватись на розглянутому.

**Метою статті є** розробити новий комплексний метод ранжування та перевірити можливість його практичного використання на тестовому прикладі.

## Виклад основного матеріалу

### дослідження

Як було зазначено вище, особливості окремих альтернатив можуть бути виявлені шляхом їх порівняння з використанням окремих часткових показників або їх комбінацій.

Для забезпечення можливості практичної реалізації таких комбінацій формулу (5) доцільно модифікувати шляхом введення до неї додаткових параметрів, тобто привести її до такого вигляду:

$$Q_i = (S_i^{k_S} + R_i^{k_R}) / A_i^{k_A}, \quad i = 1, \dots, n. \quad (6)$$

При цьому кожен з додаткових параметрів ( $k_S$ ,  $k_R$  та  $k_A$ ) може мати лише одне з двох значень: 0 або 1. Комбінуючи ці значення, можна отримати сімейство методів багатокритеріального порівняльного аналізу, перелік яких наведено в табл. 1.

Таблиця 1

Методи багатокритеріального порівняльного аналізу, які можуть бути отримані за рахунок комбінацій параметрів  $k_S$ ,  $k_R$  та  $k_A$

№	Значення параметрів			Формула для розрахунку узагальненого показника переваги	Метод-аналог
	$k_S$	$k_R$	$k_A$		
1	0	0	0	$Q_i = 2$	не використовується
2	0	0	1	$Q_i = 2 / A_i$	адитивна згортка
3	0	1	0	$Q_i = 1 + R_i$	MOORA (частково) [4]
4	0	1	1	$Q_i = (1 + R_i) / A_i$	–
5	1	0	0	$Q_i = 1 + S_i$	–
6	1	0	1	$Q_i = (1 + S_i) / A_i$	–
7	1	1	0	$Q_i = S_i + R_i$	VIKOR (частково) [5]
8	1	1	1	$Q_i = (S_i + R_i) / A_i$	базовий

Варіант, коли всі параметри дорівнюють 1, відповідає базовому методу трикритеріального ранжування.

Інші комбінації значень параметрів забезпечують отримання трьох однокритеріальних та трьох двокритеріальних методів.

Окрім того, три отримані часткові методи мають відомі аналоги, а три є новими, тобто характеризуються новою комбінацією критеріїв, за якими порівнюються альтернативи.

Таким чином, використання шістьох часткових методів додатково до базового підвищує повноту порівняння альтернатив та, відповідно, можливість виявлення їх особливостей.

При цьому послідовність розрахунків за запропонованим методом передбачає, що перші дев'ять етапів відповідають базовому, а на наступних етапах здійснюється розрахунок узагальненого показника переваги для значень

параметрів з рядків 2–7 табл. 1 та формування відповідних пріоритетних рядів.

За результатами розрахунків буде отримано сім варіантів ранжування, порядок альтернатив у яких залежить від використаного критерію порівняння.

Зрозуміло, що порівняння рангів альтернативи в отриманих рядах дає можливість виявити її переваги (або недоліки) порівняно з іншими за розглядуваними показниками та надати ОПР обґрунтовані рекомендації щодо доцільності її розгляду як раціональної.

Для оцінювання можливості практичного використання розробленого методу розглянемо розрахунковий приклад з [2], який передбачає вибір раціонального складу механізованої бригади. Вихідними даними для нього є 10 альтернативних варіантів складу, кожен з яких характеризується шістьма (однаковими за важливістю) показниками: втратами танків ( $E_1$ ), іншої бронетехніки ( $E_2$ ) та артилерії противника ( $E_3$ ), а також аналогічними показниками ( $E_4$ ,  $E_5$ ,  $E_6$ ) для своїх військ. Зрозуміло, що показники  $E_1$ – $E_3$  потребують максимізації, а решта – мінімізації.

Необхідно зазначити, що, відповідно до [2], варіант № 3 є найкращим за методом таксономії, а варіант № 5 – за адитивною згортою, тобто в разі використання відомих методів було отримано суперечливі результати ранжування альтернатив.

Вихідні дані для розрахунків наведено в табл. 2, а їх результати за запропонованим методом – у табл. 3. При цьому номери варіантів значень параметрів відповідають номерам рядків табл. 1.

Таблиця 2  
Значення показників, за якими оцінюються альтернативи

№, i	Вихідні значення показників					
	$E_{i1}$	$E_{i2}$	$E_{i3}$	$E_{i4}$	$E_{i5}$	$E_{i6}$
1	0,85	0,90	0,72	0,09	0,22	0,10
2	0,74	0,94	0,83	0,06	0,18	0,25
3	0,82	0,84	0,90	0,11	0,12	0,14
4	0,78	0,81	0,69	0,13	0,26	0,16
5	0,93	0,74	0,86	0,04	0,10	0,08
6	0,74	0,87	0,83	0,09	0,14	0,23
7	0,67	0,90	0,79	0,06	0,24	0,12
8	0,85	0,84	1,00	0,13	0,28	0,14
9	0,67	0,81	0,90	0,11	0,29	0,27
10	0,78	0,90	0,97	0,18	0,06	0,18

Аналіз результатів, наведених у табл. 3, свідчить про те, що для 6 з 7 варіантів значень параметрів альтернатива № 5 є найкращою, а альтернатива № 3 перебуває на другому місці.

### Література

1. Романченко І. С., Загорка О. М. Використання таксономічних методів при проведенні досліджень у воєнній справі // Зб. наук. пр. ЦНДІ ЗС України. 2007. № 3 (41). С. 5–16. 2. Загорка О. М., Мосов С. П., Сбитнев А. І., Стужук П. І. Елементи дослідження складних систем військового призначення. Київ: НАОУ, 2005. 100 с. 3. Свіда І. Ю., Потьомкін М. М., Хомчак Р. Б. Метод трикритеріального ранжування та його використання для багатокритеріального порівняння альтернатив //

При цьому особливістю альтернативи № 5 є те, що вона суттєво поступається альтернативі № 3 лише в разі, коли як головний розглядається частковий показник  $R_i$  та відповідний йому критерій.

Тобто вибір найкращого варіанта визначається ставленням ОПР до важливості часткового показника  $R_i$ , необхідність акцентування уваги на якому і виявлена завдяки використанню запропонованого методу.

Таблиця 3

Ранги альтернатив за результатами розрахунків

№, i	Номери варіантів значень параметрів							
	2	3	4	5	6	7	8	
1	4	4	3	4	4	3	3	
2	6	3	6	6	6	6	6	
3	2	1	2	2	2	2	2	
4	9	6	9	9	9	9	9	
5	1	8	1	1	1	1	1	
6	8	2	7	8	8	7	7	
7	7	7	8	7	7	8	8	
8	5	5	5	5	5	5	5	
9	10	9	10	10	10	10	10	
10	3	10	4	3	3	4	4	

### Висновки й перспективи подальших досліджень

Таким чином, у статті наведено комплексний метод ранжування, який забезпечує можливість аналізу особливостей альтернатив шляхом додаткового порівняння їх за окремими частковими показниками та їх доцільними комбінаціями.

Окремі з розглянутих комбінацій параметрів перетворюють цей метод у аналогії існуючих методів багатокритеріальної оптимізації. Окрім того, отримано три методи, які забезпечують порівняння альтернатив за новими сукупностями часткових показників переваги.

Загалом запропонований метод забезпечує підвищення обґрунтованості рекомендацій, які подаються на розгляд ОПР, за рахунок підвищення повноти порівняння розглядуваних альтернатив та забезпечення можливості виявлення їх особливостей.

Необхідно зазначити, що обсяги розрахунків за розробленим методом є прийнятними у разі використання сучасної обчислювальної техніки. Тому подальший розвиток проведених досліджень вбачається в програмній реалізації запропонованого методу та перевірці доцільності його застосування на достатньому обсязі тестових даних.

Сучасні інформаційні технології у сфері безпеки та оборони. Київ, 2017. № 3 (30). С. 88–92. 4. Brauers W. K. M., Zavadskas E. K. The MOORA method and its application to privatization in a transition economy // Control and Cybernetics. 2006. № 35 (2). P. 445–469. 5. El-Santawy M. F. A VIKOR method for solving personnel training selection problem // International Journal Of Computing Science. 2012, February. Vol. 1. № 2. P. 9–12.

## КОМПЛЕКСНЫЙ МЕТОД РАНЖИРОВАНИЯ И ЕГО ИСПОЛЬЗОВАНИЕ ДЛЯ МНОГОКРИТЕРИАЛЬНОГО СРАВНЕНИЯ АЛЬТЕРНАТИВ

*Игорь Сергеевич Романченко* (доктор военных наук, профессор)  
*Михаил Михайлович Потемкин* (доктор технических наук, с.н.с.)  
*Олег Петрович Кравец* (кандидат военных наук, с.н.с.)  
*Григорий Андреевич Саковский* (кандидат военных наук, с.н.с.)

*Центральный научно-исследовательский институт Вооруженных Сил Украины, Киев, Украина*

Приведено описание трехкритериального метода ранжирования, предназначенного для формирования приоритетного ряда альтернатив, и результаты его анализа. При этом указано, что во время разработки рекомендаций для лица, принимающего решение, необходимо не только определить наиболее перспективные альтернативы, но и предоставить обоснованные пояснения полученных результатов, что требует дополнительного анализа результатов расчетов. Для уменьшения объемов такого анализа предложен новый метод многокритериального сравнения, который предусматривает использование нескольких комбинаций критериев сравнения. При этом используются три однокритериальных, три двухкритериальных и одно трехкритериальное сравнения. Для этого нового метода приведены формульные зависимости, а также дано поэтапное описание порядка проведения расчетов. Возможность практического использования предложенного метода показана на расчетном примере, для которого в литературных источниках приводятся результаты, полученные с использованием известных многокритериальных методов. Сравнение результатов расчетов, полученных с использованием известных и нового методов, свидетельствует о том, что использование предложенного метода дает возможность повысить обоснованность разрабатываемых рекомендаций за счет повышения полноты сравнения альтернатив. Это позволяет сделать вывод, что применение разработанного комплексного метода ранжирования может быть достаточно перспективным для многокритериальной оптимизации сложных объектов.

**Ключевые слова:** аддитивная свертка; многокритериальное ранжирование; метод трехкритериального ранжирования; метод MOORA; метод VIKOR.

## A COMPLEX METHOD OF RANGE AND ITS USE FOR MULTICRITERIA COMPARISON OF ALTERNATIVES

*Ighor Romanchenko* (Doctor of Military Sciences, Professor)  
*Mykhajlo Potomkin* (Doctor of Technical Sciences, Senior Research Fellow)  
*Oleg Kravets* (Candidate of Military Sciences, Senior Research Fellow)  
*Hryhorii Sakovskiy* (Candidate of Military Sciences, Senior Research Fellow)

*Central Scientific Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine*

There is description of the three-criteria ranging method intended to form a priority number of alternatives and the results of its analysis. It is noted that during developing recommendations for the decision maker, it is necessary not only to identify the most promising alternatives, but also to provide reasonable explanations of the obtained results, which requires to additional analysis of the results of the calculations. It has been proposed a new multicriteria comparison method to reduce the volume of such analysis, which involves the use of several combinations of comparison criteria. There are used three single-criteria, three two-criteria and one three-criteria comparisons. Formulas dependencies are given for this new method and it is provided a step-by-step description of the calculation procedure. The possibility of practical application of the proposed method is shown in the calculated example, for which the literature sources provide the obtained results for known multi-criteria methods. Comparison of the results of the calculations for known and new methods shows that the use of the proposed method makes it possible to increase the validity of the developed recommendations by increasing the completeness of the comparison of alternatives. It leads to the conclusion that the use of the developed complex method of ranking can be quite promising during multi-criteria optimization of complex objects.

**Keywords:** additive convolution; multi-criteria ranking; three-criteria ranking method; MOORA method; the VIKOR method.

### References

1. Romanchenko I.S., Zagorka O.M. (2007). Using taxonomy methods for military research [Vykorystannja taksonomichnykh metodiv pry provedenni doslidzhenj u vojennij spravi], Col. of scient. pap. CRI of AF of Ukraine, № 3 (41), pp. 5–16.
2. Zagorka O.M., Mosov S.P., Sbitniev A.I., Stuzhuk P. I. (2005). Complex military systems research's componentry [Elementy doslidzhennja skladnykh system vijsjkovogho pryznachennja], NADU, Kyiv, 100 p.
3. Svuda I.U., Potjomkin M. M., Khomchak R. B. (2017). Method of three-criterial ranking and its use for a multi-criterial comparison of alternatives [Metod trykryterialjnogho ranzhuvannja ta jogho vykorystannja dlja baghatokryterialjnogho porivnannja aljternatyv], Modern Information Technologies in the Sphere of Security and Defence, № 3 (30), pp. 88–92.
4. Brauers W. K. M., Zavadskas E. K. The MOORA method and its application to privatization in a transition economy // Control and Cybernetics. 2006. № 35 (2). P. 445–469.
5. El-Santawy M. F. A VIKOR method for solving personnel training selection problem // International Journal Of Computing Science. 2012, February. Vol. 1. № 2. P. 9–12.

*Руслан Валентинович Грищук (доктор технічних наук, професор)*

*Руслан Михайлович Жовноватюк (кандидат технічних наук, с.н.с.)*

*Ганна Дмитрівна Носова*

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

## ГІБРИДНІ ЗАГРОЗИ У КІБЕРПРОСТОРИ: ФАКТОРИ ВПЛИВУ НА ПРИРОДУ ВИНИКНЕННЯ

*Гібридна агресія Російської Федерації проти України поставила перед всією світовою спільнотою нові виклики воєнній безпеці не тільки окремих держав, а й колективній безпеці міждержавних інституцій. Загрози, породжені новими викликами, набули ознак гібридності, а прикмети найбільш небезпечних з них все частіше почали проявлятися у кіберпросторі, який на сьогодні, де-факто, став новим театром воєнних дій. На відміну від “класичних” кіберзагроз, гібридні загрози у кіберпросторі націлені одночасно на усі його рівні – не тільки на логічний та технічний (допоміжні рівні), а й, в першу чергу, на соціальний (основний рівень). Зважаючи на недостатню опрацьованість зазначеної проблеми, її актуальність, новизну та важливість для практики забезпечення кібербезпеки держави у воєнній сфері у статті всебічно досліджено даний новий феномен. Зокрема проаналізовані історичні, правові, політичні, економічні, технологічні, інформаційні та соціальні фактори впливу на природу виникнення гібридних загроз у кіберпросторі, а також приведено результати аналізу передумов їх виникнення. Обґрунтовано та доведено, що досліджувані загрози повинні розглядатися через призму еволюційних процесів трансформації сучасного високотехнологічного суспільства. У результаті проведеного дослідження показано, що негативні прояви ознак гібридних загроз у кіберпросторі мають прямий та опосередкований вплив на усі без винятку сфери функціонування держави – від воєнної до інформаційної. Хаос, невизначеність і нестабільність в суспільстві та державі є наслідками прояву гібридних загроз у кіберпросторі. Це в свою чергу вимагає від системи забезпечення воєнної безпеки держави вироблення адекватних, своєчасних та упереджувальних активних заходів протидії таким загрозам.*

**Ключові слова:** кібернетичний простір; гібридна загроза; неконвенційні бойові дії.

### Вступ

**Постановка проблеми.** Гібридні загрози не є новим безпековим явищем. Наприклад, з часів “Холодної війни” спецслужби протидіючих держав використовували пропаганду та дезінформацію як інструмент асиметричної війни для досягнення власних військово-політичних цілей. Проте саме завдяки стрімкому розвитку технологій та цифровізації всіх сфер функціонування суспільства і держави, особливо воєнної сфери, гібридні загрози набули нового обрису та масштабу [1] й почали проявлятися у нових, до сьогодні нетипових для воєнної безпеки держави, середовищах. Таким середовищем на сьогодні є кіберпростір, який, де-факто, став новим театром воєнних дій [2].

**Аналіз останніх досліджень і публікацій** показав, що гібридні загрози досить ґрунтовно та всебічно вивчалися й досліджувалися провідними науковцями та міжнародними і національними безпековими організаціями, хоча і безвідносно до приналежності до кіберпростору.

Так, за концепцією НАТО від 2010 р., [3] гібридна загроза визначається як протидіювана противником здатність до одночасного застосування традиційних і нетрадиційних засобів адаптивно до поставлених завдань. За результатами спільних досліджень та проведених навчань із залученням сил НАТО, США та провідних вищих військових навчальних закладів США у 2011 р. було підготовлено звіт, де визначено чинники гібридних загроз як

всеохоплюючі за строком, такі, що складаються з великої кількості варіацій шкідливого впливу (акцій) відносно безпеки держави, зокрема тероризм, міграція, піратство, корупція, етнічні конфлікти тощо. У [3] гібридну загрозу визначено як різноманітні та динамічні (мінливі) застосування регулярних і нерегулярних військ та/або кримінальних елементів, об'єднаних разом з метою досягнення взаємодіючого ефекту. Автори в [4] додають до попереднього визначення наступне: застосування, які можуть бути запроваджені у будь-яких типах та різноманітних формах війни одночасно.

Позицію Європейського союзу у питаннях термінології в галузі гібридних загроз було оприлюднено у липні 2017 р. віце-президентом Європейської комісії з питань безпеки. За цим визначенням гібридна загроза – це дипломатичні, військові, економічні та технологічні методи, які держава-агресор спрямовує на те, щоб використати вразливість цілі та створити невизначеність з метою перешкоджання процесу прийняття рішення; охоплює традиційні і нетрадиційні методи атаки, які можуть бути використані як державою, так і недержавними гравцями [5].

Таким чином, у результаті аналізу вказаних вище та інших відкритих джерел встановлено, що на сьогодні є усталена термінологія до тлумачення такої категорії як гібридна загроза. Визначено, що спільною рисою, яка притаманна багатьом визначенням гібридної загрози, є необмеженість її у часі, просторі та формах прояву. При цьому,

якщо часові ознаки та форми прояву гібридної загрози на сьогодні вже достатньо глибоко досліджені, то просторові прояви, зокрема в кіберпросторі, залишилися поза увагою більшості фахівців.

**Метою статті** є всебічне дослідження нового феномену – гібридної загрози в кіберпросторі для встановлення факторів впливу на природу її зародження, що у подальшому стане науковим підґрунтям для вироблення системою забезпечення воєнної безпеки держави адекватних, своєчасних та упереджувальних активних заходів протидії таким загрозам.

### Виклад основного матеріалу дослідження

Передумови виникнення гібридних загроз у кіберпросторі слід розглядати через призму еволюційних процесів трансформації суспільства. Якісний стрибок, спровокований виникненням Інтернету, стрімким розвитком цифрових технологій та відповідного комунікаційного устаткування, перетворив постіндустріальне суспільство на інформаційне, а нові високотехнологічні доробки, у свою чергу, започаткували сучасне високотехнологічне суспільство [6]. У новій, цифровій, ері світ “зменшився” до розмірів кіберпростору, проте став більш вразливим до загроз, зокрема гібридних, всередині цього простору. Тому провідним гравцям, які є регуляторами кіберпростору, все легше стає задовольнити власні геополітичні, фінансові, ресурсні, владні та інші амбіції приховано через кіберпростір.

У загальному фактори виникнення гібридних загроз у кіберпросторі можна виокремити, виходячи з самого поняття кіберпростору та ступеня залучення до нього держави та її громадян [7]. До них відносять і наявність необхідних потужностей для їх реалізації (технологічних, програмних, економічних, інтелектуальних тощо), і екстериторіальність (транскордонність) кіберпростору, доступність Інтернету, відсутність правового регулювання, чітких принципів співіснування та його мирного використання, і геополітичні процеси у світі, і розуміння та сприйняття кіберпростору як середовища для поширення зброї нового типу – кіберзброї [8], яка не заборонена жодними міжнародними конвенціями. Аналіз досвіду підготовки та ведення агресії Російської Федерації (РФ) проти України показав, що в умовах ведення неконвенційних бойових дій [9–14], факторами впливу на природу виникнення цього типу загроз стають історичні, правові, політичні, економічні, інформаційні, технологічні та соціальні процеси у суспільстві.

До історичних факторів впливу на природу виникнення гібридних загроз у кіберпросторі пропонується віднести:

маніпулювання історичними подіями (фактами) в інтересах держави-агресора з метою утвердження “права” на агресивні дії зокрема у кіберпросторі;

історична інтегрованість інформаційного простору між державою-агресором та державою, проти якої здійснюється агресія;

маніпулятивне протиставлення історичних зв'язків у світовому просторі, пошук “прямих

аналогій” у світовій історії для дискредитації противника на світовому рівні;

пошук псевдодоказового історичного підґрунтя як “дозвільної грамоти” на агресивні дії. На прикладі агресії РФ проти України ця теза реалізована у постійному нагадуванні про нібито еквівалентні дії західних країн, зокрема одностороннє проголошення незалежності Косово в 90-х роках та вторгнення до Іраку у 2003 році;

перебільшення військових успіхів через екскурс в історію;

розбурхування масового руху за історичну справедливість (етнічних, національних, мовних, релігійних та інших меншин); [15].

вибіркове і тенденційне ставлення до історичних фактів, яке допомагає маніпуляторам видавати агресора за жертву чи миротворця.

Поява понять “гібридна загроза” та “гібридна війна” поставила перед фахівцями у галузі правових відносин низку питань щодо визначення місця цих понять у міжнародному праві [16] та внутрішньодержавної регуляторної і нормативно-правової діяльності [17]. Нажаль, більшість цих питань і досі залишається не вирішеною [18]. Отже, вплив правових факторів на причини появи гібридних загроз у кіберпросторі важко переоцінити. До таких пропонуємо віднести:

застаріле право збройних конфліктів [19]; відсутність у сучасному міжнародному праві поняття “гібридна війна” як наслідок – безкарність;

зловживання законом як засобом ведення війни шляхом пошуку прогалин у нормативно-правовій базі та відсутності чіткого трактування понять;

спроби нівелювання міжнародних договорів та домовленостей як недійсних та взагалі неіснуючих для сторони-агресора;

відсутність законодавчого уніфікованого визначення поняття “кібернетичні загрози” як на національному, так і на міждержавному рівні;

відсутність налагодженої і законодавчо закріпленої взаємодії між компетентними державними органами, які є суб'єктами кібербезпеки, і здійснення координації з такої діяльності;

відсутність правового механізму регулювання права доступу правоохоронних та інших державних органів щодо можливості перехоплення інформації (прослуховування телефонних переговорів, перлюстрацію електронних повідомлень) без дозволу суду;

слабкі глобальні зв'язки у сфері правового регулювання кібербезпеки, недостатній рівень міжнародного співробітництва;

низький рівень підтримки ініціатив НАТО щодо врегулювання на міжнародному рівні можливості визнання кібератаки “актом війни” [20].

Окрім того, для України актуальною проблемою залишається відсутність належного нормативно-правового забезпечення для процедур захисту діючих та створюваних в системі державного управління та зокрема у системі управління Збройними Силами України баз даних [21].

Зміна геополітичних конфігурацій, перерозподіл сфер впливу, політична та стратегічна невизначеність призводять до

постійного політичного, економічного, інформаційного тиску, що створює зону підвищеного ризику для новітніх гібридних загроз. Відтак *політичними факторами* пропонуємо вважати:

замовчування, небажання помічати диктаторські режими “заради загального миру”; надмірна лібералізація політики країн ЄС;

небажання розпізнати масштаб реальних загроз;

недалекоглядність політичних еліт провідних держав у сподіваннях на демократичну трансформацію еліти країни-агресора з ознаками диктаторського режиму;

окупація частини території сусідньої держави як засіб блокування інтеграції сусідніх держав у західний політичний та безпековий простір;

неефективність державного гарантування безпеки суспільства, низька довіра населення країни до політичних інституцій держави.

Поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур, виробників інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин; розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури, стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації призводять до розширення спектру вразливостей для вдалої реалізації гібридних загроз.

До *економічних факторів* впливу на причини появи гібридних загроз у кіберпросторі відносимо:

низька конкурентоспроможність вітчизняної продукції, як програмної, так і апаратної (або її відсутність) – присутність, зокрема у державному сегменті, переважної більшості продукції іноземного виробництва ставить під загрозу безпеку цього сегмента [22];

збереження присутності бізнесу держави-агресора на територіях і у економічному просторі держави-жертви агресії;

економічна нестабільність всередині країни-жертви: значне економічне розшарування населення, присутність усіх відомих економічних проблем у суспільстві (безробіття, низький рівень життя тощо); низькі темпи економічного зростання;

контроль над важливими економічними активами з боку агресора, що робить можливим фізичне впровадження шкідливого програмного забезпечення на об'єктах критичної інфраструктури для подальших кібератак [23];

зовнішній економічний вплив на діяльність крупних підприємств;

залежність економіки від постачання ресурсів країною-агресором; взаємна залежність від торгових партнерів;

низький загальний рівень урядових витрат у кіберсекторі [24].

Комерційний фундамент сучасних комунікаційних технологій, залежність їх розвитку та ступеню доступності від загального стану економіки – характерні риси кібернетичного простору в цілому та його технологічних складових зокрема. Враховуючи цей взаємозв'язок та на основі аналізу попередньої групи факторів до *технологічних факторів* впливу на причини появи

гібридних загроз у кіберпросторі можна віднести наступні:

зростання обсягів інформації, що зберігається на електронних інформаційних ресурсах;

уніфікація обладнання та комплектуючих; прив'язаність до ресурсної виробничої бази інших країн [25];

вразливість мікропроцесорних платформ, зумовлена зосередженістю їх виробництва в розвинених країнах; відсутність власної мікропроцесорної бази; монополізація технологічно розвиненими країнами виробництва мікропроцесорів як елемент економічного, технологічного та силового (воєнного) тиску на інші країни;

вразливість додатків, що вирішують критичні з точки зору безпеки, задачі, таких як віддалений та термінальний доступ, системи керування (наприклад, підприємством), доступні з інтернету або внутрішньої мережі елементи систем управління (наприклад, виробничим процесом) [26] технічні можливості переховування справжніх виконавців злочинів у кіберпросторі;

використання неліцензійного програмного забезпечення іноземного виробництва (виробництва підприємств країни-агресора);

технологічні труднощі у вирішенні кібервпливу від технологічного збою [27];

низький рівень захищеності систем державних баз даних та дата-центрів для обробки і резервування відомостей електронних інформаційних ресурсів;

відсутність комплексного підходу до захисту (програмна частина + апаратна частина + інформаційна частина);

невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам [28];

технологічна неготовність до попередження та відбиття гібридних загроз;

відсутність прогностичних моделей гібридних загроз;

недостатня кількість і якісний склад засобів забезпечення кібербезпеки зокрема на об'єктах критичної інфраструктури.

Провідні держави здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, розповсюджують інформацію з метою здобуття односторонніх переваг, прагнуть досягнути монополії на інформаційні ресурси. Прикладом цього є події, що розпочались у 2014 році в Україні. Російські засоби масової інформації реалізовували задалегідь підготовлені програми інформаційно-психологічного тиску на населення України на територіях Автономної Республіки Крим та у південно-східних регіонах. Своєрідна інтервенція Росії в інформаційний простір України стала найбільш небезпечною гібридною загрозою сьогодення, а *інформаційні фактори* – впливовим чинником появи гібридних загроз у кіберпросторі. До них відносимо:

контроль держави-агресора над медіаресурсом; применшення у інформаційному просторі значення та можливостей кіберпростору у розповсюдженні гібридних загроз;

розповсюдження хибної інформації щодо стану захищеності об'єктів критичної інфраструктури;

використання медіаресурсу для формування суспільної свідомості позитивного сприйняття гібридних загроз (формування “стокгольмського синдрому”);

створення псевдоісторичної продукції із подальшим її розповсюдженням у кіберпросторі;

низький рівень поінформованості споживача (користувача, суб'єкта кіберпростору) про можливі загрози та заходи захисту від них;

використання інформаційно-пропагандистських інструментів задля розпалювання внутрішніх конфліктів;

використання кіберпростору для інтегрування пропагандистських медіа у медіапростір інших регіонів (приклад: інформаційна агенція Sputnik (РФ) поширює інформацію більш ніж 30-ма мовами у десятках країн ЄС, досягнувши рівня місцевого ньюз-мейкера) [29];

формування у кіберпросторі на міжнародному рівні негативного іміджу держави-жертви агресії, наприклад, через створення хибної уяви про криміногенну обстановку в цій країні;

застосування кібернетичних впливів (атак) на окремі політичні фігури держави з метою керування суспільною думкою щодо держави-жертви шляхом розповсюдження “прямої мови” впливових представників, експертів і т. ін., наприклад, злам персональних сторінок з подальшою підміною контенту тощо;

дискредитаційна кампанія через зарубіжні ЗМІ у бізнес-сфері;

комбіновані дії з метою нарощування протестного потенціалу всередині країни-жертви агресії;

недосконала інформаційна політика уряду; використання технічних можливостей кіберпростору для маніпулювання інформацією з боку противника, зміна її за форматом представлення [30];

активне впровадження цифрових технологій як інструмент створення залежності суспільства від інформації;

низький рівень інформування про успішні атаки противника у кіберпросторі з метою набуття “нетравматичного” досвіду боротьби з ними.

Останні два пункти витікають з цілої низки суспільно-політичних та соціальних явищ у світі, тож окремий розгляд групи *соціальних факторів* впливу на природу виникнення гібридних загроз є цілком доцільним. До цієї групи відносимо:

рівень стійкості суспільства до маніпулювання, навіювання;

рівень обізнаності щодо можливих загроз у кіберпросторі та методів і підходів протидії чи захисту від них;

вплив підконтрольної агресору релігійної складової на адекватне сприйняття будь-яких суспільно-політичних чи інших явищ у країнах-сторонах конфлікту;

рівень культури та знань серед держслужбовців щодо забезпечення безпеки своєї робочої та приватної переписки у кіберпросторі та комунікацій через електронні засоби;

хибне уявлення про склад суспільства як з одного, так і з іншого боку протистояння;

активний розвиток кібертероризму;

незнання населенням основ кібербезпеки і особиста неграмотність в питаннях кіберзагроз серед приватних підприємців та керівників великих підприємств (установ);

можливості кіберпростору щодо реалізації майже усіх видів соціальних небезпек [31];

вплив недержавних організацій (суспільних, громадських) на формування як відношення до самого явища (гібридних загроз у кіберпросторі), так і на сприйняття користувачем цих загроз;

релігійні передумови політичної та військової експансії як засіб для її виправдання [32].

### Висновки й перспективи подальших досліджень

Аналіз вивчення досвіду підготовки та ведення РФ агресії проти України, світових тенденцій цифровізації суспільства, міжнародних практик у галузі забезпечення кібербезпеки підтверджує особливе значення кіберпростору у збройних конфліктах гібридного типу, у якому і самі загрози стають гібридними. Враховуючи те, що діюча на сьогодні система забезпечення інформаційної безпеки воєнної сфери не призначена для виявлення та протидії гібридним загрозам у кіберпросторі, а система забезпечення кібербезпеки воєнної сфери перебуває лише на стадії становлення та набуття необхідних бойових спроможностей питання всебічного вивчення таких загроз стоїть вкрай гостро.

Організація процесу моніторингу, попередження та адекватної протидії гібридним загрозам в кіберпросторі майже не можлива без усвідомлення та розуміння, що собою являють такі загрози, у чому полягає їх сутність та зміст, що є джерелом, з якою метою вони реалізуються, які завдання на них покладаються тощо.

У зв'язку з цим, всебічне вивчення усіх складових гібридних загроз у кіберпросторі та їх класифікація є перспективним напрямком подальших наукових досліджень, результати яких сприятимуть створенню системи оперативного виявлення та реагування на них, у воєнній сфері зокрема, та розвитку військової науки в цілому.

### Література

1. Hybrid Warfare: The Next Generation Tool. Asian Warrior. Sp.13, 2016. 2. Заява за результатами саміту у Варшаві. URL: [nato.int/cps/uk/natohq/official\\_texts/133169.htm](https://www.nato.int/cps/uk/natohq/official_texts/133169.htm) (дата звернення: 26.08.2019). 3. Концепція НАТО 2010. cf BI-SC input for new NATO Capstone Concept for the Military contribution to countering hybrid enclosure 1 to 1500/CPPCAM/FCR/10-270038 and 5000 FXX/0100/IT-0651/SER:NU0040, 25 August 2010. 4. US Army's Training Circular 7-100. 5. Cyber War in Perspective: Russian Aggression Against Ukraine. Edited by Kenneth Geers. NATO Cooperative Cyber Defense Centre of Excellence. Tallinn, Estonia. 2015. 175 p. 6. Основи кібернетичної безпеки: монографія/за заг. ред. Ю. Г.

Даника. Житомир. 2016. 636 с. 7. Прес-конференція Віце-президента Єврокомісії Ірки Катаїнена, присвячена питанню гібридних загроз. URL: <https://www.5.ua/svit/yevrokomisiia-vyznachylasia-shcho-iavlivaie-soboiu-hibrydna-zahroza-150683.html> (дата звернення: 19.09.2018). 8 С. Вдовенко, Ю. Даник, С. Фараон. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення / Комп'ютерні науки та кібербезпека, (1), с. 18-30. 9. Andrei Josan, Cristina Voicu. Hybrid wars in the age of asymmetric conflicts. The Scientific Informative Review, №1(28) 2015, p. 49. 10. The U.S. Army Operating Concept: Win in a Complex World. 2020-2040. TRADOC Pamphlet



- 525-3-1. URL: [www.tradoc.army.mil/tpubs/pams/tp532-3-1.pdf](http://www.tradoc.army.mil/tpubs/pams/tp532-3-1.pdf) (дата звернення: 16.03.2018). **11. Larson Eric, Peters John.** Preparing the U.S. Army for Homeland Security. Concepts, Issues, and Options. URL: [books.google.com.ua](http://books.google.com.ua) (дата звернення: 16.03.2018). **12. Белоусова Н. Б., Афанасьєва П. А.** Основні вимоги щодо забезпечення безпеки інформаційного простору / Актуальні проблеми міжнародних відносин. 2017. Вип. 133. С. 95-98. **13.** Кіберпростір як новий вимір геополітичного суперництва: монографія/Дубов Д. В. Київ, 2015. 328 с. **14.** Гібридна війна: in verbo et in praxi: монографія/під заг. ред. Р. О. Додонова. Вінниця, 2017. 412 с. **15. Рибак В.** Гібридні виклики міжнародного гуманітарного права / Тиждень.UA/ URL: [tyzden.ua/World/145884](http://tyzden.ua/World/145884) (дата звернення: 11.10.2018). **16. Чуприна В.** Кіберпростір як поле битви. URL: [yur-gazeta.com/dumka-eksperta/kiberprostir-yak-pole-bitvi.html](http://yur-gazeta.com/dumka-eksperta/kiberprostir-yak-pole-bitvi.html) (дата звернення: 27.09.2018). **17.** Власюк В. В., Карман Я. В. Деякі основи поняття "гібридна війна" в міжнародному праві / Право і громадянське суспільство. 2015. № 1. С. 226. **18. Діордіца І.** Поняття і зміст кіберзагроз на сучасному етапі / Підприємництво, господарство і право. 2017. №4. С. 99. **19. Пузиренко О. Г.** Математична модель загроз інформаційній безпеці в інформаційно-телекомунікаційних системах спеціального призначення/Наука і техніка Повітряних Сил Збройних Сил України. 2015. № 3 (16). С. 57. **20. Бурячок В. Л., Толюпа С. В.** Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: навч. посіб. Київ. 2016. 14 с. **21.** Світова гібридна війна: український фронт: монографія/під заг. ред. В. П. Горбуліна. Київ. 2017. 496 с. **22. Кулицький С.** Економічна складова гібридної війни Росії проти України. <http://nbuviap.gov.ua/images/ukrain/2016/ukr20.pdf> (дата звернення: 14.03.2018). **23. Прозовський А.О.** форум по кібербезпеці в Європейському союзі і НАТО 2017. URL: <http://m.20minut.ua/Noviny-Vinnitsi/Vid-Chitachiv/artue-pruzovskiy-o-forume-po-kiberbezopasnosti-v-evropeyskom-soyuze-i-nato-10638382.html> (дата звернення: 18.09.2018). **24.** Угрозы безопасности в глобальном киберпространстве ИНЭУМ. URL: [www.ineum.ru/ugrozy-bezopasnosti-v-globalnom-kiberprostranstve](http://www.ineum.ru/ugrozy-bezopasnosti-v-globalnom-kiberprostranstve) (дата звернення: 08.06.2018). **25. Стиран В.** Дика природа кіберпростору. Стратегія виживання. URL:<http://blog.styran.com/2017-02-20-cyber-jungle-ids-talk/> (дата звернення: 20.02.2018). **26.** Про Стратегію кібербезпеки України: Рішення Ради національної безпеки і оборони України від 27 січня 2016 року. Київ. 2017. 11 с. **27.** Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства/Аналітичний документ. Київ. 2018. 106 с. **28.** Угрозы информационной безопасности в кризисах и конфликтах XXI века: монография/под общ. ред. А. В. Загорского, Н. П. Ромашкиной. Москва. 2015. 151 с. **29. Почепцов Г.** Інфовійни в кіберпросторі. URL: [https://ms.detector.media/ethics/manipulation/infoviyini\\_v\\_kiberprostori/](https://ms.detector.media/ethics/manipulation/infoviyini_v_kiberprostori/) (дата звернення: 28.05.2018). **30. Бартош А. А.** Смыслы гибридной войны. URL: [nic-pnb.ru/vneshnepoliticheskie-aspekty-bezopasnosti/smysly-gibridnoj-vojni](http://nic-pnb.ru/vneshnepoliticheskie-aspekty-bezopasnosti/smysly-gibridnoj-vojni) (дата звернення: 15.07.2018). **31.** Соціальні фактори, що впливають на життя і здоров'я людини. URL: [//studopedia.su/5\\_47912\\_sotsiani-faktori-shcho-vplivavut-na-zhittya-ta-zdorovya-ludini.html](http://studopedia.su/5_47912_sotsiani-faktori-shcho-vplivavut-na-zhittya-ta-zdorovya-ludini.html) (дата звернення: 16.03.2018). **32. Почепцов Г.** Гибридная война: когда население оказывается целью. [https://ms.detector.media/trends/1411978127/gibridnaya\\_voyna\\_kogda\\_naselenie\\_okazyvaetsya\\_tselyu/](https://ms.detector.media/trends/1411978127/gibridnaya_voyna_kogda_naselenie_okazyvaetsya_tselyu/) (дата звернення: 17.09.2018).

## ГИБРИДНЫЕ УГРОЗЫ В КИБЕРПРОСТРАНСТВЕ: ФАКТОРЫ ВЛИЯНИЯ НА ПРИРОДУ ВОЗНИКНОВЕНИЯ

*Руслан Валентинович Гришук (доктор технических наук, профессор)  
Руслан Михайлович Жовноватюк (кандидат технических наук, с.н.с.)  
Анна Дмитриевна Носова*

*Житомирский военный институт имени С. П. Королева, Житомир, Украина*

*Гибридная агрессия Российской Федерации против Украины поставила перед всем мировым сообществом новые вызовы как внутренней безопасности отдельных стран, так и коллективной безопасности межгосударственных организаций, реализация которых сместилась в кибернетическое пространство. Его активное влияние на все сферы жизни современного человека послужило причиной одновременно как развития его возможностей, так и возрастания уязвимости. Становление киберпространства как новейшего театра военных действий требует своевременного реагирования, которое невозможно без всестороннего изучения такого явления как гибридные угрозы в киберпространстве.*

*В статье рассмотрены исторические, правовые, политические, экономические, технологические, информационные и социальные факторы влияния на природу возникновения гибридных угроз в кибернетическом пространстве. Проведено анализ предпосылок появления гибридных угроз в кибернетическом пространстве. Отмечено, что они взаимосвязаны и их следует рассматривать через призму эволюционных процессов трансформации общества. Указано на то, что изменение геополитических конфигураций, перераспределение сфер влияния, политическая и стратегическая неопределенность приводят к постоянному политическому, экономическому и информационному давлению. Это в свою очередь влечет за собой создание зон повышенного риска, в которых возможно появление и реализация новейших гибридных угроз в кибернетическом пространстве, следовательно, требует адекватных действий по защите от них.*

*Определены актуальные проблемы защиты действующих и создаваемых баз данных в системе государственного управления Украины, в частности в системе управления Вооруженными Силами Украины.*

*Кроме того, освещены основные геополитические процессы, на которые осуществляют влияние ведущие станы мира с целью получения монополии на те или иные информационные ресурсы. Основными среди таких процессов, относительно которых необходимо проводить постоянный глобальный мониторинг, являются политические, экономические, военные и экологические.*

*Ключевые слова:* кибернетическое пространство, гибридная угроза, неконвенционные боевые действия.

## HYBRID THREATS IN CYBER SPACE: FACTORS OF INFLUENCE ON NATURE OF EMERGENCE

**Ruslan Hryshchuk** (Doctor of Technical Sciences, Professor)  
**Ruslan Zhovnovatiuk** (Candidate of Technical Sciences, Senior Research Scientist)  
**Hanna Nosova**

*Zhytomyr Military Institute n. a. S.P. Korolev, Zhytomyr, Ukraine*

*The hybrid aggression of the Russian Federation against Ukraine posed a new challenge to the entire world community, both for the internal security of individual countries and for the collective security of intergovernmental organizations, the implementation of which shifted into cyberspace. His active influence on all spheres of life of modern man was the cause of both the development of its capabilities and the increase in vulnerability. The emergence of cyberspace as the newest theater of war requires a timely response, which is impossible without a comprehensive study of the phenomenon of hybrid threats in cyberspace.*

*The article considers the historical, legal, political, economic, technological, informational and social factors influencing the nature of the emergence of hybrid threats in cyberspace. The analysis of the prerequisites for the emergence of hybrid threats in cyberspace. It is noted that they are interrelated and should be viewed through the prism of the evolutionary processes of transformation of society. It is noted that changes in geopolitical configurations, the redistribution of spheres of influence, political and strategic uncertainty lead to constant political, economic and informational pressure. This, in turn, entails the creation of high-risk areas in which the emergence and introduction of the newest hybrid threats in cyberspace is possible, therefore adequate actions are required to protect them.*

*The actual problems of protection of existing and created databases in the state administration system of Ukraine, in particular in the control system of the Armed Forces of Ukraine, are identified.*

*In addition, the main geopolitical processes that are influenced by the leading countries of the world for the purpose of obtaining a monopoly on certain information resources are covered. The main processes for which ongoing global monitoring is necessary are political, economic, military and environmental.*

**Keywords:** cyberspace, hybrid threat, non-conventional fighting.

### References

1. Hybrid Warfare: The Next Generation Tool. Asian Warrior. Sp.13, 2016. 2. Zajava za rezultatamy samitu u Varshavi. URL: [nato.int/cps/uk/natohq/official\\_texts\\_133169.htm](http://nato.int/cps/uk/natohq/official_texts_133169.htm) (data zvernennja: 26.08.2019). 3. Koncepcija NATO 2010. cf BI-SC input for new NATO Capstone Concept for the Military contribution to countering hybrid enclosure 1 to 1500/PPCAM/FCR/10-270038 and 5000 FXX/0100/IT-0651/SER:NU0040, 25 August 2010. 4. US Army's Training Circular 7-100. 5. Cyber War in Perspective: Russian Aggression Against Ukraine. Edited by Kenneth Geers. NATO Cooperative Cyber Defense Centre of Excellence. Tallinn. Estonia. 2015. 175 p. 6. Osnovy kibernetichnoji bezpeky: monohrafiya/za zagh. red. Ju. Gh. Danyka. Zhytomyr. 2016. 636 s. 7. Pres-konferencija Vice-prezidenta Jevrokomisiji Irky Katainenena, prysvjachena pytannju ghibrydnykh zaghroz. URL: <https://www.5.ua/svit/jevrokomisija-vyznachylasia-shcho-ivavliaie-soboiu-hibrydna-zahroza-150683.html> (data zvernennja: 19.09.2018). 8 S. Vdovenko, Ju. Danyk, S.Faraon. Definicijni problemy terminologhiji u sferi kiberbezpeky i kiberoborony ta shljakhy jikh vyrishennja / Komp'juterni nauky ta kiberbezpeka, (1), c. 18-30. 9. Andrei Josan, Cristina Voicu. Hybrid wars in the age of asymmetric conflicts. The Scientific Informative Review, #1(28) 2015, p. 49. 10. The U.S. Army Operating Concept: Win in a Complex World. 2020-2040. TRADOC Pamphlet 525-3-1. URL: [www.tradoc.army.mil/tpubs/pams/tp532-3-1.pdf](http://www.tradoc.army.mil/tpubs/pams/tp532-3-1.pdf) (data zvernennja: 16.03.2018). 11. Larson Eric, Peters John. Preparing the U.S. Army for Homeland Security. Concepts, Issues, and Options. URL: [books.google.com.ua](http://books.google.com.ua) (data zvernennja: 16.03.2018). 12. Bjelousova N. B., Afanasjjeva P. A. Osnovni vymoghy shhodo zabezpechennja bezpeky informacijnogho prostoru / Aktualjni problemy mizhnarodnykh vidnosyn. 2017. Vyp. 133. S. 95-98. 13. Kiberprostir jak novyj vymir gheopolitychnogho supernyctva: monohrafiya/Dubov D. V. Kyjiv, 2015. 328 s. 14. Ghibrydna vijna: in verbo et in praxi: monohrafiya/pid zagh. red. R. O. Dodonova. Vinnyca, 2017. 412 s. 15. Rybak V. Ghibrydni vyklyky mizhnarodnogho humanitamogho prava / Tyzhdenj.UA/ URL: [tyzdenj.ua/World/145884](http://tyzdenj.ua/World/145884) (data zvernennja: 11.10.2018). 16. Chupryna V. Kiberprostir jak pole bytvy. URL: [jur-gazeta.com/dumka-eksperta/kiberprostir-yak-pole-bitvi.html](http://jur-gazeta.com/dumka-eksperta/kiberprostir-yak-pole-bitvi.html) (data zvernennja: 27.09.2018). 17. Vlasjuk V. V., Karman Ja. V. Dejaki osnovy ponjattja "ghibrydna vijna" v mizhnarodnomu pravi / Pravo i ghomadjansjke suspiljstvo. 2015. № 1. S. 226. 18. Diordica I. Ponjattja i zmist kiberzagroz na suchasnomu etapi / Pidpryjemnyctvo, ghospodarstvo i pravo. 2017. №4. S. 99. 19. Puzrenko O. Gh. Matematychna modelj zagroz informacijnij bezpeky v informacijno-telekomunikacijnykh systemakh specialnogho pryznachennja/Nauka i tekhnika Povitrtjanykh Syl Zbrojnykh Syl Ukrajiny. 2015. # 3 (16). S. 57. 20. Burjachok V. L., Toljupa S. V. Informacijnyj ta kiberprostory: problemy bezpeky, metody ta zasoby borotjby: navch. posib. Kyjiv. 2016. 14 s. 21. Svitova ghibrydna vijna: ukrajinsjkyj front: monohrafiya/pid zagh. red. V. P. Ghorbulina. Kyjiv. 2017. 496 s. 22. Kulycjkyj S. Ekonomichna skladova ghibrydnoji vijny Rosiji proty Ukrajiny. <http://nbuviap.gov.ua/images/ukrain/2016/ukr20.pdf> (data zvernennja: 14.03.2018). 23. Pruzovskij A.O. forum po kyberbezopasnosti v Evropejskom sojuze y NATO 2017. URL: <http://m.20minut.ua/Noviny-Vinnitsi/Vid-Chitachiv/artue-pruzovskiy-o-forume-po-kiberbezopasnosti-v-evropejskom-soyuze-i-nato-10638382.html> 24. Ughrozy bezopasnosti v gholbalnom kyberprostranstve\_YNƏUM. URL: [www.ineum.ru/ugrozy-bezopasnosti-v-globalnom-kiberprostranstve](http://www.ineum.ru/ugrozy-bezopasnosti-v-globalnom-kiberprostranstve) 25. Styran V. Dyka pryroda kiberprostoru. Strateghija vyzhyvannja. URL:<http://blog.styran.com/2017-02-20-cyber-jungle-ide-talk/> (data zvernennja: 20.02.2018). 26. Pro Strateghiju kiberbezpeky Ukrajiny: Rishennja Rady nacionalnoji bezpeky i oborony Ukrajiny vid 27 sichnja 2016 roku. Kyjiv. 2017. 11 s. 27. Ghibrydni zagrozy Ukraini i suspiljna bezpeka. Dosvid JeS i Skhidnogho partnerstva/Analitychnyj dokument. Kyjiv. 2018. 106 s. 28. Ughrozy ynformacyonnoj bezopasnosti v kryzysakh y konfliktykh XXI veka: monohrafiya/pod obshh. red. A. V. Zagorskogho, N. P. Romashkynoj. Moskva. 2015. 151 s. 29. Pohepcov Gh. Infovijny v kiberprostori. URL: [https://ms.detector.media/ethics/manipulation/infovijny\\_v\\_kiberprostori/](https://ms.detector.media/ethics/manipulation/infovijny_v_kiberprostori/) 30. Bartosh A. A. Smysly ghybrydnoj vojny. URL: [nie-pnb.ru/vneshnepolitieskie-aspecty-bezopasnosti/smysly-gibridnoj-vojni](http://nie-pnb.ru/vneshnepolitieskie-aspecty-bezopasnosti/smysly-gibridnoj-vojni) 31. Socialjni faktory, shho vplyvajutj na zhyttja i zdorov'ja ljudyny. URL: [studopedia.su/5\\_47912\\_sotsiani-faktori-shcho-vplivaut-nazhyttja-ta-zdorovya-ludini.html](http://studopedia.su/5_47912_sotsiani-faktori-shcho-vplivaut-nazhyttja-ta-zdorovya-ludini.html) (data zvernennja: 16.03.2018). 32. Pohepcov Gh. Ghybrydna vijna: koghda naselenye okazyvaetsja celjju. [https://ms.detector.media/trends/1411978127/gibridnaya\\_voyna\\_kogda\\_naselenie\\_okazyvaetsya\\_tselyu/](https://ms.detector.media/trends/1411978127/gibridnaya_voyna_kogda_naselenie_okazyvaetsya_tselyu/)

*Микола Олександрович Гульков  
Віталій Станіславович Толкачов*

*Національний університет оборони України імені Івана Черняхівського, Київ, Україна*

## ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, У КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ УКРАЇНИ

*У сучасному світі дедалі більшого значення набуває поняття інформаційної безпеки. Разом з поширенням загального доступу до інформації, слідуючи за розвитком комунікаційних систем, розширюється коло можливих інформаційних загроз, з якими стикається держава.*

*Саме тому інформаційна безпека перетворюється на одну з ключових складових національної безпеки. Деякі дослідники вважають, що забезпечення інформаційної безпеки необхідно не тільки для того, щоб зберегти недоторканість національного інформаційного простору, але й наполягають на тому, що вірно сформульована національна інформаційна стратегія сприяла б більш успішному вирішенню задач у політичній, економічній, соціальній та інших сферах життя. Припускається також можливий вплив відповідної інформаційної політики на позитивний хід розв'язання як внутріполітичних так і зовнішніх конфліктів.*

*В статті здійснюється порівняльний аналіз організації захисту інформації в країнах - членах НАТО та організації технічного захисту інформації в Україні. Запропонований метод зіставлення наявних результатів оцінювання компонентів довіри до безпеки визначених ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99 надають можливість отримати більш об'єктивну та адекватну оцінку використання засобів та компонентів обчислювальної системи, що використовуються в Україні при побудові автоматизованих систем.*

**Ключові слова:** *інформаційна безпека, технічний захист інформації, політика безпеки.*

### Вступ

**Постановка проблеми.** Починаючи послідовну аргументацію необхідності підтримки заходів по забезпеченню інформаційної безпеки на теренах України, слід зазначити, що певні кроки в цьому напрямку вже було зроблено, починаючи з перших років незалежності. Так у статті 17 Конституції України зазначено: “Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу”. Чи означає це, що інформаційну безпеку поставлено на один рівень з такими важливими компонентами системи національних інтересів, як суверенітет та територіальна цілісність, і цей статус питання інформаційної безпеки є законодавчо закріпленим у найголовнішому нормативно-правовому акті? Саме так воно і є, адже інформаційна безпека, хоча і відрізняється за спрямуванням від інших складових цього твердження, тобто вона не належить до груп політичних та економічних національних інтересів, але не поступається ним за ступенем важливості.

**Аналіз останніх досліджень і публікацій.** В цілому співробітництво між НАТО та країнами-партнерами, одним з яких є і Україна, в рамках

Ради євроатлантичного партнерства та Програми “Партнерство заради миру” (ПЗМ) передбачає певні зобов'язання сторін щодо обміну та захисту інформації [5]. Для збільшення прозорості військового планування й оборонних бюджетів і забезпечення демократичного контролю над збройними силами сторони можуть брати участь у взаємному обміні інформацією про кроки, що вони почали або починають. Перед обміном будь-якою таємною інформацією між країною-учасницею ПЗМ і НАТО, органи по безпеці інформації повинні бути взаємно впевненими, що сторона, яка приймає інформацію, готова забезпечити захист інформації відповідно до вимог сторони, яка її передає.

Активізація інформаційного обміну потребує уніфікації термінів і понять у сфері технічного захисту та безпеки інформації, перегляду та вдосконалення нормативних документів та інструкцій у галузі інформаційних обмінів, їх гармонізації з міжнародними стандартами та створення сучасних механізмів моніторингу потоків інформації [2].

**Метою статті** є аналіз організації захисту інформації в країнах-членах НАТО та організації технічного захисту інформації в Україні.

## Виклад основного матеріалу дослідження

Особливості організації технічного захисту інформації в країнах-членах НАТО

Однією з передумов тісної співпраці між Україною та країнами-членами НАТО є дотримання вимог стандартів та інших нормативних документів. Технічний захист інформації є дуже важливою компонентою під час взаємодії інформаційних систем різних країн. Особливо це стосується тих випадків, коли в системах циркулює інформація з обмеженим доступом, тому надзвичайно важливим є аналіз документів НАТО, в яких наведено рекомендації та вимоги щодо технічного захисту інформації.

Велику увагу захисту інформації приділяють у країнах-членах НАТО. Там створено розгалужену систему органів, які мають забезпечувати належний рівень захищеності інформації. Слід зауважити, що терміну “технічний захист”, який використовується в Україні, документах НАТО та інших міжнародних нормативних документах, відповідає термін “security”, у перекладі з англійської мови “безпека”.

У нормативних документах НАТО вживається термін “ADP system” (automated data processing system), який у нашій державі тлумачать як автоматизована система (АС), відповідно до його поширення в нормативно-правових документах із технічного захисту інформації в Україні.

Завданням технічного захисту інформації є протидія загрозам безпеці АС.

Загрозами безпеці АС, згідно зі стандартом ISO 74982, є:

- порушення інформації і (або) інших ресурсів;
- спотворення і модифікація інформації;
- викрадення, вилучення або втрата інформації і (або) інших ресурсів;
- розкриття інформації;
- порушення послуги.

Загрози класифікують як:

*випадкові* – загрози, які існують без чітких намірів (наприклад, помилки функціонування технічних засобів, помилки оператора і помилки в програмному забезпеченні);

*навмисні* – загрози, які можуть змінюватися від непередбачених атак маніпулюванням легкодоступними засобами моніторингу до добре продуманих і підготовлених атак з використанням спеціального системного знання; спробу реалізації навмисної загрози називають атакою;

*пасивні* – загрози, які в результаті реалізації не модифікують інформацію в системі, не порушують операцій, що провадяться системою, і не змінюють стану системи (наприклад, пасивне списування інформації в процесі комунікації систем);

*активні* – загрози, які в результаті реалізації спричиняють модифікацію інформації, зміну стану системи і (або) операції, які провадить система. Приклад реалізації активної загрози - навмисна

несанкціонована зміна таблиці маршрутизації.

Внутрішні атаки виникають, коли легальні користувачі діють недозволеною або неавторизованим способом. Найбільш відомі комп’ютерні злочини містять внутрішні атаки, які компрометують систему безпеки.

До методів захисту, які використовуються проти внутрішніх атак, належать:

- ретельна комплектація персоналу;
- створення довірчої комп’ютерної бази;
- посилення служби аудиту проти означених атак.

Зовнішні атаки створюють за допомогою таких методів:

- фізичний доступ до ліній зв’язку (активний чи пасивний);
- перехоплення повідомлень;
- маскування під легального користувача або під компоненту системи;
- шунтування механізмів автентифікації або керування доступом.

Заходи і засоби безпеки завжди підвищують вартість системи і можуть робити її складною для використання. Тому ще до початку розроблення заходів і засобів безпеки треба чітко визначити ті загрози, проти яких система має бути захищеною. Цей процес називають оцінюванням загроз. Система є вразливою до різних загроз, але використовують тільки деякі з них, тому що атакуючий не має змоги це зробити або результат атаки не компенсує його зусиль і ризику розкриття його особи. Детальне дослідження загроз не є сферою застосування вищезазначеного стандарту, в загальному плані воно передбачає:

- ідентифікацію вразливостей системи;
- аналіз імовірності використання цих вразливостей;
- оцінювання наслідків успішного проведення кожного з видів атаки;
- оцінювання вартості кожного з видів атаки;
- визначення потенційної вартості кожного з видів контрзаходів;
- визначення множини механізмів безпеки, які себе виправдовують (можливо, на основі аналізу відповідних коштів).

Нетехнічні заходи безпеки, такі як страхове прикриття, можуть бути ефективнішими стосовно коштів, ніж технічні. Повної технічної безпеки, а також повної фізичної безпеки не може бути досягнуто. Доцільно встановити ціну атак достатньо високою, щоб знизити ризик до допустимого рівня.

Чільне місце в системі нормативних документів займає NATO security policy (С-М(55)15(Final)), в якому сформульовано основні принципи побудови системи забезпечення безпеки інформації, включаючи інформацію, що циркулює в АС. Між існуючими нормативними документами НАТО та різними стадіями життєвого циклу АС існує взаємозв’язок (див. рис. 1).

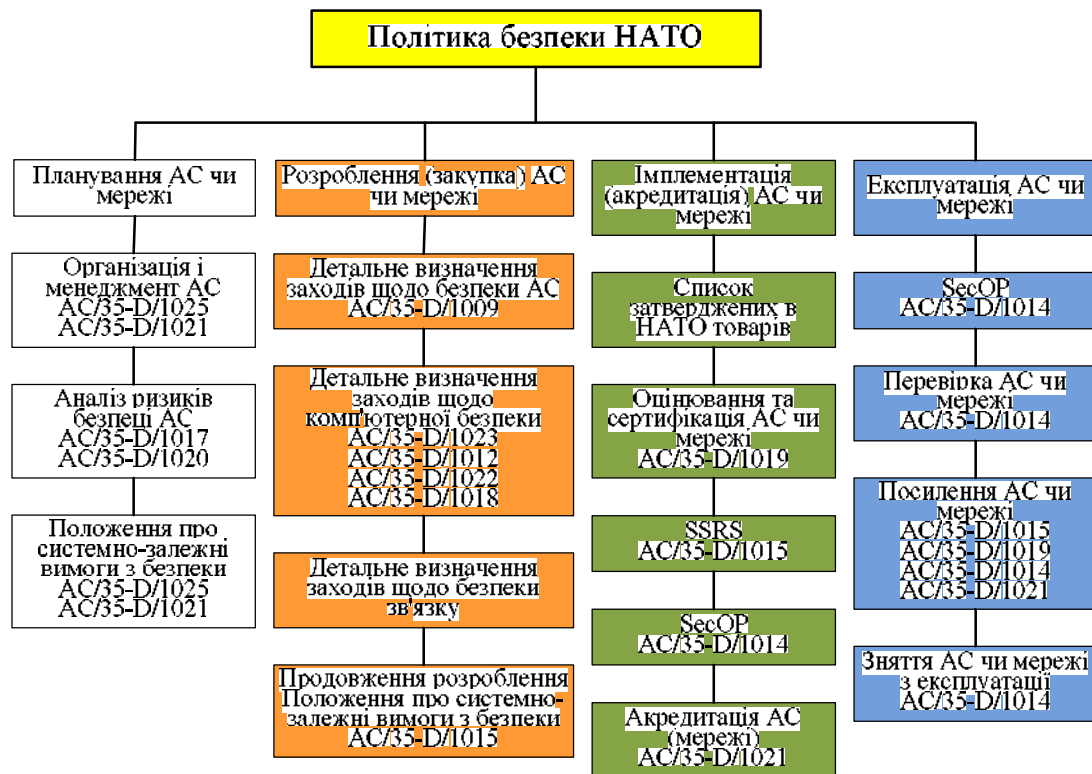


Рис. 1 Нормативно-технічні документи НАТО з безпеки АС, які використовуються протягом її життєвого циклу

Згідно з документом (С-М(55)15(Final)) необхідно створити Орган з безпеки, який відповідав би за утримання належного рівня безпеки і, зокрема, надати чинності визначеним у НАТО стандартам з безпеки та пов'язаних з ними настановній документації. Для кожної країни-члена НАТО, згідно з документом (С-М(55)15(Final)), необхідно створити національний орган з безпеки (NSA), який відповідав би за безпеку класифікованої інформації, що є власністю НАТО.

Головнокомандувачі НАТО та керівники військових агенцій НАТО, які діють під егідою Військового комітету НАТО, відповідають за безпеку в рамках своїх команд та агенцій. На них покладено відповідальність за створення організаційної структури з безпеки, за розроблення та реалізацію програм з безпеки відповідно до прийнятої Політики безпеки НАТО, а також за періодичне інспектування стану впровадження необхідних заходів з безпеки та підтримання її належного рівня.

Цивільні агенції НАТО відповідають перед Радою НАТО за підтримання належного рівня безпеки в рамках своєї сфери діяльності. Вони повинні встановити відповідну організаційну структуру безпеки згідно з прийнятими у НАТО правилами та належною системою нагляду за станом безпеки.

Для захисту конфіденційної інформації НАТО, яка зберігається, обробляється або передається в АС і мережах, у розділі X документа (С-М(55)15(Final)) визначено обов'язки

Головнокомандувачів, керівників військових і цивільних Агенцій та функції Органу Акредитації з безпеки (SAA), Органу з автоматизованої обробки даних, Органу, який відповідає за експлуатацію АС, офіцерів безпеки АС і мереж, офіцерів безпеки офісу.

У системі нормативних документів із забезпечення АС велику увагу приділено питанням менеджменту безпеки.

Завдання менеджменту тісно пов'язані з такими етапами життєвого циклу АС:

- планування АС;
- розроблення (закупівля) АС;
- імплементация АС;
- експлуатація АС (її посилення);
- зняття з експлуатації АС.

До завдань з менеджменту безпеки на етапі планування АС належать:

- установлення організаційних засад та визначення завдань з менеджменту безпеки;
- проведення аналізу ризиків безпеки АС для запланованої АС чи мережі;
- розроблення Положення про системно залежні і вимоги з безпеки (SSRS), якщо цього вимагає Політика безпеки НАТО.

До завдань з менеджменту безпеки на етапі розроблення (закупівлі) АС належать:

- розроблення детального визначення загальних заходів з безпеки, які покривають фізичну безпеку, безпеку персоналу, безпеку документів і процедурну безпеку;
- розроблення детального визначення заходів щодо комп'ютерної безпеки, а саме:

- 1) визначення класів функціональних послуг і рівнів гарантій;
- 2) визначення аспектів безпеки, пов'язаних з об'єднанням АС;
- 3) визначення характеристик безпеки в документах на закупівлю обладнання;
- 4) розроблення детального визначення заходів з безпеки зв'язку стосовно безпеки передавання, захисту від витоку конфіденційної інформації через технічні канали, криптографічного захисту;
- 5) продовження розроблення Положення про системно залежні вимоги з безпеки (SSRS), якщо цього вимагає Політика безпеки НАТО.

До завдань з менеджменту безпеки на етапі імплементації АС належать:

звернення до списку НАТО щодо продуктів з комп'ютерної безпеки та списку НАТО з комп'ютерної безпеки "Продукти, що знаходяться в стадії оцінювання" як основного джерела інформації стосовно комп'ютерної безпеки;

звернення до списку НАТО рекомендованих продуктів як основного джерела інформації стосовно продуктів, що захищають інформацію від витоків через технічні канали;

проведення оцінювання та сертифікації АС, якщо цього вимагає Політика безпеки НАТО;

завершення Положення про системно залежні вимоги з безпеки (SSRS), якщо цього вимагає Політика безпеки НАТО;

формулювання Процедур безпечної експлуатації (SecOP) АС;

акредитація АС, що уможливує зберігання, оброблення або передавання секретної інформації НАТО в цьому середовищі.

До завдань з менеджменту безпеки на етапі експлуатації АС належать:

зберігання, оброблення та передавання секретної інформації НАТО в експлуатаційному середовищі відповідно до затверджених Процедур безпечної експлуатації (SecOP);

проведення, згідно з Політикою безпеки НАТО, періодичних перевірок стану безпеки АС.

До завдань з менеджменту безпеки на етапі посилення АС належать:

перегляд Положення про системно залежні вимоги з безпеки (SSRS), якщо цього вимагає Політика безпеки НАТО;

проведення в разі виникнення потреби повторного оцінювання та повторної сертифікації АС;

перегляд Процедур безпечної експлуатації (SecOP) АС;

повторна акредитація АС, яка підтверджує можливість зберігання, оброблення та передавання секретної інформації НАТО в цьому експлуатаційному середовищі.

До завдань з менеджменту безпеки на стадії зняття з експлуатації АС належать:

проведення належної архівації або розсекречування (знищення) постійних чи змінних

носіїв зберігання комп'ютерної інформації;

проведення належної архівації або знищення паперової документації.

У нормативному документі НАТО С-М(2000)54 - NATO Policy for Standardization наведено механізми, за допомогою яких НАТО досягає взаємодії, використовуючи стандарти. Визнаючи важливість стандартизації для НАТО, Північноатлантична Рада заснувала Організацію НАТО зі стандартизації (NSO) з тим, щоб гармонізувати і координувати діяльність у галузі стандартизації. NSO охоплює:

комітет НАТО зі стандартизації (NCS);

представників країн-членів НАТО у NCS;

штатну групу НАТО зі стандартизації (NSSG);

агенцію НАТО зі стандартизації (NSA).

Кожен із цих органів відповідає за процес розроблення і перегляд стандартів, забезпечення механізмів, які сприяють обміну інформацією, необхідною для національних експертів у справі узгодження положень стандартів.

NCS наглядає за діяльністю NSO, яка відповідає за надання підтримки комітетам, призначеним перевіряти вимоги стандартів, затверджувати завдання стандартизації і розробляти та затверджувати стандарти. Ці комітети можуть передавати функції розроблення та затвердження стандартів підлеглим групам. Стандарти НАТО оформлюють у вигляді:

угод зі стандартизації (STANAGs);

публікацій Альянсу (APs);

міждержавних публікацій (MPs).

У рамках цих документів досягається взаємодія національних військових структур.

Вищезазначені документи розробляють згідно з правилами, сформульованими в AAP-03 - Directive for the Development and Production of STANAGs та APs. Як тільки STANAGs, APs або MPs прийнято, члени Альянсу повинні як найшвидше їх реалізувати, щоб побудувати та підтримувати основні елементи у взаємодії військових структур з метою оптимізації використання ресурсів.

До складу робочих груп, які розробляють стандарти, включають представників країн-членів НАТО, а також країн Партнерства заради миру, якщо це не суперечить Доктрині НАТО з безпеки. Діяльність робочих груп підтримує Агенція НАТО зі стандартизації, яка відповідає також за супроводження баз даних, що містять STANAGs, APs та MPs.

Оцінювання рівня захищеності АС і виконання робіт з сертифікації засобів технічного захисту інформації

Як відомо, у системі технічного захисту інформації України велике значення має проведення державної експертизи як комплексної системи захисту інформації (КСЗІ), яка є невід'ємною складовою частиною АС (коли планується оброблення інформації, порядок захисту якої регламентується законами України

або іншими нормативно-правовими актами), так і засобів технічного захисту інформації від несанкціонованого доступу (Положення про державну експертизу в сфері технічного захисту інформації, введено в дію наказом Адміністрації Держспецзв'язку України № 93 від 16.05.2007 р. (зі змінами)) та оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, введений в дію наказом Адміністрації Держспецзв'язку України № 112 від 04.07.2008 р.).

При проведенні експертних робіт із державної експертизи експерти керуються вимогами НД ТЗІ 2.5-004 - 99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу", введеного в дію наказом ДСТСЗІ СБУ № 22 від 28. 04. 1999 р.

У країнах-членах НАТО цим заходам також надають значну роль. Серед нормативних документів, які стосуються цього напряму, слід відзначити АС/35-D/1019 Guidelines for the evaluation and certification of ADP systems and networks and computer security (COMPUSEC) products. Крім того оцінювання (сертифікація) засобів технічного захисту інформації та компонентів обчислюваної системи АС здійснюється відповідно до вимог Єдиних критеріїв оцінки безпеки інформаційних технологій, встановлених міжнародним стандартом ISO/IEC 15408 Information technology. Security techniques. Evaluation criteria for IT security, більш відомий під назвою Common Criteria (CC).

Засоби та компоненти обчислюваної системи, які оцінені на відповідність стандарту ISO/IEC 15408, також широко використовуються в

Україні при побудові АС різного призначення. З метою спрощення процесу аналізу та прийняття рішення щодо можливого використання певного засобу (компонента обчислюваної системи) у складі комплексу засобу захисту КСЗІ було введено в дію ряд документів, а саме: НД ТЗІ 2.6-002-2015 "Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99", введений в дію наказом Адміністрації Держспецзв'язку України від 27.04.2016 р. № 293, НД ТЗІ 2.6-003-2015 "Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99", введений в дію наказом Адміністрації Держспецзв'язку України від 27.04.2016 р. № 294 та НД ТЗІ 2.7-013-2016 "Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99", введений в дію наказом Адміністрації Держспецзв'язку України від 27.04.2016 р. № 295.

Зазначені нормативні документи спрощують завдання експертам щодо проведення експертних робіт, шляхом зіставлення наявних результатів оцінювання компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99.

### Висновки й перспективи подальших досліджень

Формування і реалізація єдиної державної політики по забезпеченню захисту національних інтересів від загроз в інформаційній сфері, прийняття відповідних законодавчих актів, координація діяльності органів державної влади по забезпеченню інформаційної безпеки послідовно сприятимуть приведенню української національної системи інформаційної безпеки у відповідність зі світовими стандартами у даній сфері.

### Література

1. Закон України Про національну безпеку України від 21 червня 2018 року № 2469-VIII (Відомості Верховної Ради (ВВР), 2018, № 31). 2. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. *Офіц. вид.* Київ. КМ України, 2006. 8с. 3. Зячук Я.І. Аналіз та оцінка ризиків інформаційної безпеки локально-обчислюваної мережі. *Восточно-Европейский журнал передовых технологий.* 2012. № 58. С 40-43. 4. Василенко В.С. Оцінювання ризиків безпеки

інформації в локальних обчислювальних мережах. URL: [http://www.rusnauka.com/11\\_EISN\\_2010/Informatica/64-068.doc/htm](http://www.rusnauka.com/11_EISN_2010/Informatica/64-068.doc/htm) 5. Security within the North Atlantic Treaty Organisation (С-М(2002) 49). URL:<http://arhives.nato.int/amendments-to-nato-c-m-55-15-final>. 6. Анісімов А.В., Заславський В.А., Фаль О.М. Основи інформаційної безпеки та захисту інформації у контексті євроатлантичної інтеграції України. *Науково-методологічний посібник.* Київ, ДП "НВЦ "Євроатлантикінформ". 2006.

## ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ, КАК СОСТАВЛЯЮЩАЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, В КОНТЕКСТЕ ЕВРОАТЛАНТИЧЕСКОЙ ИНТЕГРАЦИИ УКРАИНЫ

*Николай Александрович Гульков  
Виталий Станиславович Толкачев*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

В современном мире все большее значение приобретает понятие информационной безопасности. Вместе с распространением общего доступа к информации, следуя за развитием коммуникационных систем, расширяется круг возможных информационных угроз, с которыми сталкивается государство.

Именно поэтому информационная безопасность превращается в одну из ключевых составляющих национальной безопасности. Некоторые исследователи считают, что обеспечение информационной безопасности необходимо не только для того, чтобы сохранить неприкосновенность национального информационного пространства, но и настаивают на том, что верно сформулирована национальная информационная стратегия способствовала бы более успешному решению задач в политической, экономической, социальной и других сферах жизни. Предполагается также возможное влияние соответствующей информационной политики на положительный ход решения как внутривнутриполитических так и внешних конфликтов.

В статье осуществляется сравнительный анализ организации защиты информации в странах - членах НАТО и организации технической защиты информации в Украине. Предложенный метод сопоставления имеющихся результатов оценки компонентов доверия к безопасности определенных ISO/IEC 15408 требованиям НД ТЗИ 2.5-004-99 предоставляют возможность получить более объективную и адекватную оценку использования средств и компонентов вычислительной системы, используемые в Украину при построении автоматизированных систем.

**Ключевые слова:** информационная безопасность, техническая защита информации, политика безопасности

### TECHNICAL PROTECTION OF INFORMATION AS A COMPONENT OF INFORMATION SECURITY, IN THE CONTEXT EURO-ATLANTIC INTEGRATION OF UKRAINE

*Mykola Hulkov  
Vitalii Tolkachov*

*National Defense University of Ukraine named by Ivan Cherniakhovsky, Kyiv, Ukraine*

*In today's world, the notion of information security is becoming increasingly important. Together with the dissemination of universal access to information, following the development of communication systems, the range of possible information threats facing the state is expanding.*

*This is why information security becomes one of the key components of national security. Some researchers believe that ensuring information security is necessary not only to preserve the integrity of the national information space, but also to insist that a properly formulated national information strategy would contribute to a more successful solution to the political, economic, social and other spheres of life. It is also possible to influence the relevant information policy on the positive course of resolving both internal and external conflicts.*

*The article provides a comparative analysis of the organization of information security in NATO member countries and the organization of technical protection of information in Ukraine. The proposed method of comparing the available results of the assessment of security components of the ISO / IEC 15408 defined with the requirements of ND TZI 2.5-004-99 provides an opportunity to obtain a more objective and adequate assessment of the use of the tools and components of the computer system used in Ukraine for the construction of automated systems.*

**Keywords:** information security, technical protection of information, security policy.

### References

1. Закон України Про національну безпеку України від 21 червня 2018 року № 2469-VIII (Vidomosti Verkhovnoji Rady (VVR), 2018, № 31).
2. Pravyla zabezpechnnja zakhystu informaciji v informacijnykh, telekomunikacijnykh ta informacijno-telekomunikacijnykh systemakh. Ofic. vyd. Kyjiv. KM Ukrainy, 2006. 8s.
3. Zajachuk Ja.I. Analiz ta ocinka ryzykiv informacijnoji bezpeky lokaljno-obchysljuvalnoji merezhi. Vostochno-Evropejskij zhurnal peredovykh tekhnologij. 2012. № 58. S 40-43.
4. Vasylenko V.S. Ocynjuvannja ryzykiv bezpeci informaciji v lokalnykh obchysljuvalnykh merezhakh. URL: [http://www.rusnauka.com/11\\_EISN\\_2010/Informatica/64-068.doc/htm](http://www.rusnauka.com/11_EISN_2010/Informatica/64-068.doc/htm)
5. Security within the North Atlantic Treaty Organisation (S-M(2002) 49). URL:<http://archives.nato.int/amendments-to-nato-c-m-55-15final>.
6. Anisimov A.V., Zaslavskij V.A., Falj O.M. Osnovy informacijnoji bezpeky ta zakhystu informaciji u konteksti jevroatlantychnoji integraciji Ukrainy. Naukovometodologichnyj posibnyk. Kyjiv, DP "NVC "Jevroatlantykinform". 2006.



*Віталій Володимирович Зуйко (кандидат військових наук, доцент)*

*Сергій Валентинович Зотов*

*Олександр Анатолійович Кошлянь*

*Національний університет оборони України імені Івана Черняховського, Київ, Україна*

## МЕТОДИКА ОЦІНЮВАННЯ НАДІЙНОСТІ ВИКОНАННЯ ЗАХОДІВ ТОПОГЕОДЕЗИЧНОГО ЗАБЕЗПЕЧЕННЯ

У статті розглянутий підхід до оцінювання надійності виконання заходів з топогеодезичного забезпечення шляхом представлення їх як системи масового обслуговування, яка дозволяє оцінити ймовірність обслуговування споживача відповідною інформацією та встановити, що виконання завдання не буде зірваним через відмови за наступними входними параметрами: наявність у банку даних топогеодезичної інформації на територію, яка необхідна споживачу; доступність та безвідмовна робота каналів зв'язку за якими проходить циркуляція топогеодезичної інформації; наявність необхідної кількості спеціалістів, які наповнюють бази даних топогеодезичною інформацією відповідно до існуючих вимог до її точності, наочності та оперативності.

**Ключові слова:** топогеодезичне забезпечення; ефективність заходів; система масового обслуговування; надійність системи.

### Вступ

Успішне ведення бойових дій у значній мірі залежить від правильної оцінки ситуації, яка склалася в районі збройного конфлікту, як перед його початком так і в ході його ведення. Досвід участі Збройних Сил України в операції Об'єднаних сил (АТО) показав, що ефективність застосування систем управління військами і зброєю знаходиться у прямій залежності від якості інформаційного забезпечення, і зокрема від повноти та достовірності забезпечення військ (сил) вихідними топогеодезичними даними, які використовується штабами і військами. Так, в умовах ведення збройної боротьби процес створення, доведення до військ та використання топогеодезичних даних є безперервним та має свої особливості і складності. Потреба у цих даних прив'язана до району проведення бойових дій та повинна бути актуальна на будь-який момент часу [1]. Особливістю діяльності топографічної служби є те, що вона крім виконання завдань топогеодезичного забезпечення військ (сил) в операціях (бойових діях) є також безпосереднім виконавцем і виробником усіх видів топогеодезичної та картографічної продукції для потреб Збройних Сил України (та інших силових відомств) [2].

Досвід проведення операції Об'єднаних сил (АТО) показав що необхідність забезпечення надійності виконання заходів з топогеодезичного забезпечення військ (сил), вимагає обґрунтованого оцінювання ймовірності отримання інформації про місцевість штабами і військами всіх рівнів.

**Постановка проблеми.** Ефективність системи топогеодезичного забезпечення залежить від наступних показників:

точності топогеодезичної інформації;  
оперативності виготовлення та доведення топогеодезичної інформації до користувачів;  
надійності топогеодезичного забезпечення.

Крім ефективності функціонування система характеризується деякими показниками надійності функціонування, які поділяються на два типу. Технічні показники надійності – це показники, пов'язані з параметрами системи, вони характеризують переходи системи з одного стану в інший і безпосередньо не відносяться до кінцевих результатів роботи. Наприклад, такими показниками є інтенсивність відмов або інтенсивність відновлення елементів системи. Оперативні показники надійності – це показники, які характеризують вплив даного стану на кінцевий ефект, тобто на критерії системи. До них відносяться, наприклад, ймовірність безвідмовної роботи системи [3].

У зв'язку з цим, актуальною є наукова проблема оцінювання ймовірності забезпечення топогеодезичною інформацією як фактору надійності функціонування системи топогеодезичного забезпечення.

**Аналіз останніх досліджень і публікацій.** Питанням оцінювання ефективності системи топогеодезичного забезпечення, вибору критерію та показників присвячені роботи [3,4]. За допомогою розроблених підходів встановлені показники за якими проводиться оцінювання заходів топогеодезичного забезпечення. Окреслені праці висвітлили фундаментальні підходи до питань оцінювання вищезазначених заходів, але питання оцінювання надійності як складової ефективності під час виконання заходів топогеодезичного забезпечення дій військ (сил) розглянуті не були.

**Мета статті** полягає у оцінюванні надійності виконання заходів з топогеодезичного забезпечення шляхом представлення їх як системи масового обслуговування, яка дозволяє оцінити ймовірність обслуговування споживача відповідною інформацією.

### Виклад основного матеріалу дослідження

Оцінювання ефективності функціонування будь-якої системи виконується за допомогою векторного критерію  $W = (W_1, W_2, \dots, W_n)$ , який є показником якості роботи системи. Складовими вектору  $W$  можуть бути різні характеристики, а саме: час надходження інформації  $W_1$ , ймовірність виконання завдання  $W_2$ , тощо.

Розглянемо більш докладно положення щодо надійності функціонування системи. Топогеодезичне забезпечення, як і будь-яка система характеризується вектором параметрів  $X = (X_1, X_2, \dots, X_k)$ , який належить деякій множині  $X$  і визначає стан системи. У найпростішому випадку це параметри, які визначають наявність та працездатність елементів системи. Внаслідок виходу елементів зі строю або їх відновлення параметри змінюються в часі  $t$ , тобто має місце випадковий процес зміни станів  $X(t)$ , який має назву траєкторії системи.

Множину станів системи позначимо:  $\{g\} = G$ , де  $g$  – траєкторії процесу зміни станів. Повній працездатності системи відповідає деяка траєкторія, яку позначимо  $g_0$ .

Крім параметрів, пов'язаних з надійністю системи, існують параметри  $y \in Y$  зовнішніх факторів: характеристики погодних умов, місцевості, особливості району ведення бойових дій, вплив противника на елементи системи, тощо. Вони також можуть змінюватися у часі, утворюючи подібні траєкторії  $y(t)$ , які належать множині  $Y (y \in Y)$ .

Так у загальному вигляді ефективність функціонування системи залежить від параметрів системи, а також від інших зовнішніх факторів, тобто  $W(t) = W(x(t), y(t))$ .

При деяких нежорстких обмеженнях функцію  $W(x(t), y(t))$  можливо представити у вигляді множини, виділивши в якості співмножника – номінальну ефективність системи  $W_0$ , тобто узагальнену ефективність системи при повній працездатності.

Номінальна ефективність системи  $W_0$  не залежить від надійності тому, що вона визначена для стану “абсолютної надійності” (повної працездатності системи):  $W(x, y) = R(x, y)W_0(y)$

або  $R(x, y) = \frac{W(x, y)}{W_0(y)} = K_{\text{еф}}$ , де  $K_{\text{еф}}$  – коефіцієнт збереження ефективності.

У теорії надійності цей коефіцієнт розглядається як показник оперативної надійності системи. Він має фізичний зміст – показує, яка частина номінальної ефективності системи зберігається при виході з ладу її елементів, які характеризують працездатність. При цьому, оскільки найбільша ефективність системи має місце при  $W = W_0$ , то вочевидь, що  $0 \leq K_{\text{еф}} \leq 1$ .

Якщо ефективність системи оцінюється по

ймовірності виконання нею визначеного завдання, то  $K_{\text{еф}}$  приймає значення ймовірності того, що виконання завдання не буде зірваним через відмови. При оцінюванні функціонування системи топогеодезичного забезпечення надійність її визначається, як ймовірність своєчасного доведення до споживачів топогеодезичної інформації.

Встановимо, що надійність функціонування системи топогеодезичного забезпечення буде оцінюватись величиною коефіцієнту збереження ефективності.

У загальному випадку встановимо, що надійність функціонування системи топогеодезичного забезпечення описується трьома параметрами:

$x_1$  – наявністю у банку даних топогеодезичної інформації на територію, яка необхідна споживачу;

$x_2$  – кількістю спеціалістів, які наповнюють бази даних топогеодезичною інформацією;

$x_3$  – кількістю каналів зв'язку за якими проходить циркуляція топогеодезичної інформації, яка необхідна споживачам.

Будемо вважати також, що системи топогеодезичного забезпечення відносяться до системи масового обслуговування, надійність функціонування якої розраховується за формулою.

$$W_2 = \sum_j \frac{n_{\text{вх}j} P_{0j} K_j}{N_0} = \sum_j \frac{n_{0j} K_j}{N_0} \quad (1)$$

де:  $n_{0j}$  – число вимог  $j$ -ї групи, що задовольняється повністю справною системою;

$n_{\text{вх}j}$  – число вимог  $j$ -ї групи, що поступили на вхід системи;

$N_0$  – загальна кількість отриманих системою вимог.

Відношення  $\frac{n_{0j}}{N_0}$  – визначає долю вимог  $j$ -ї групи в загальній кількості вимог, яка обслуговується повністю справною системою. Відповідно, воно визначиться як вірогідність  $K_j$ , що усереднена за всіма вимогами.

Вимогою будемо вважати номенклатурний аркуш електронної карти, який необхідно доставити споживачу.

Стосовно системи яка розглядається, коефіцієнт  $K_j$  в (1) буде мати зміст ймовірності доведення одного номенклатурного аркуша електронної карти, при якому повністю однаково здійснюється обробка тільки таких номенклатурних аркушів, які оброблялися в суміжні проміжки часу. Позначимо цей інтервал  $dt$ , доля  $dt$  в загальній кількості  $\frac{dt}{t_p}$ , де  $t_p$  – загальний час виконання задачі.

Даний коефіцієнт  $K_j$  буде відповідати безперервній функції  $K(t)$ , де  $t$  – дійсний час. Тому виникає завдання визначити дану функцію.

Оскільки кожний номенклатурний аркуш

попередньо проходить всі етапи обробки (створення/оновлення, зберігання, доставку), відповідно, контур обслуговування включає всі ці компоненти і

$$K_t = P(\omega_{xp})P(\omega_n / \omega_{xp})P(\omega_d / \omega_{xp}\omega_n) \quad (2)$$

де:  $\omega_{xp}$  – подія, яка пов'язана з не ураженням автомобіля штабного топографічного (АШТ) групи топогеодезичного та навігаційного забезпечення (ТГНЗ);

$P(\omega_{xp})$  – ймовірність не ураження АШТ групи ТГНЗ;

$\omega_n$  – успішне завантаження з бази даних номенклатурного аркушу електронної карти, або створення топографічного документу;

$P(\omega_n / \omega_{xp})$  – ймовірність завантаження з бази даних номенклатурного аркушу електронної карти, або створення топографічного документу при умові збереження АШТ групи ТГНЗ;

$\omega_d$  – успішна доставка номенклатурного аркушу електронної карти споживачу;

$P(\omega_d / \omega_{xp}\omega_n)$  – ймовірність доставки при умові збереження АШТ групи ТГНЗ та успішному завантаженню з бази даних номенклатурного аркушу електронної карти, або створення топографічного документу.

Будемо вважати, що знищення АШТ та ураження особового складу групи ТГНЗ взаємно не пов'язані між собою, що дозволяє вважати ці події незалежними. Тоді формула (2) прийме вигляд:

$$K(t) = P(\omega_{xp})P(\omega_n)P(\omega_d) \quad (3)$$

Оцінювання ймовірності не ураження АШТ групи ТГНЗ та ймовірність своєчасного відновлення апаратної та інформаційної складової групи ТГНЗ здійснюється за формулою:

$$P(\omega_{xp}) = 1 - (R_0 R_1)^k (1 - R_2) \quad (4)$$

де:  $R_0$  – ймовірність потрапляння АШТ групи ТГНЗ в зону ураження зброєю;

$R_1$  – умовна ймовірність ураження;

$R_2$  – ймовірність своєчасного відновлення апаратної та інформаційної складової групи ТГНЗ;

$k$  – кількість підгруп групи ТГНЗ.

В процесі отримання з бази даних номенклатурного аркушу електронної карти, або створення топографічного документу приймають  $x_2$  спеціалістів, які працюють паралельно. Якщо вважати, що ймовірність безпомилкової роботи  $i$ -го спеціаліста  $R_i$  буде виражатися:

$$R_i = e^{-\int_0^t c(t) dt} \quad (5)$$

де:  $c(t)$  – частота появи помилок, то ймовірність безпомилкової роботи всього колективу складатиме:

$$R_n = 1 - \prod_{i=1}^{x_2} (1 - R_i) \quad (6)$$

тоді

$$P(\omega_n) = E_n R_n = E_n \left( 1 - \prod_{i=1}^{x_2} (1 - R_i) \right) \quad (7)$$

де:  $E_n$  – ваговий коефіцієнт, який відповідає відносній ефективності роботи спеціалістів.

Приблизно його значення можна вважати спадаючим пропорційно виходу з ладу особового

$$\text{складу } E_n = \frac{x_2}{x_{2\max}}$$

Якщо вважати, що спеціалісти схильні до помилок в однаковій мірі, тобто частота виникнення помилок у всіх спеціалістів однакова та крім цього, незалежна від часу, то ймовірність успішного завантаження з бази даних номенклатурного аркушу електронної карти, або створення топографічного документу:

$$P(\omega_n) = \frac{x_2}{x_{2\max}} \left( 1 - (1 - e^{-ct})^{x_2} \right) \quad (8)$$

Доставка номенклатурного аркушу електронної карти здійснюється по  $x_3$  каналах зв'язку, які працюють одночасно, формула для оцінки ймовірності їх безвідмовної роботи подібна (8), але замість ( $c$ ) буде присутнім інтенсивність відмов каналу зв'язку  $-\lambda$ . Будемо вважати її однаковою для усіх каналів зв'язку та незмінною в часі, тоді:

$$P(\omega_d) = \frac{x_3}{x_{3\max}} \left( 1 - (1 - e^{-\lambda t})^{x_3} \right) \quad (9)$$

Співмножник  $\frac{x_3}{x_{3\max}}$  тут також має зміст вагового коефіцієнта та відображує зниження пропускну здатності каналів зв'язку при виході окремих каналів з ладу.

В (1) присутній помножувач  $n_{0j}/N_0$ , який визначає долю вимог  $j$ -ї групи в загальному потоці вимог. У даному випадку  $N_0$  має зміст замовлених споживачем номенклатурних аркушів електронних карт,  $n_{0j}$  – це реально наявні в базі даних електроні карти; складання повинно проводитися по кількості номенклатурних аркушів електронних карт, а так як ймовірність доставки кожного номенклатурного аркуша електронної карти співпадає і:

$$\sum_j n_{0j} = x_1; N_0 = x_{1\max}, \text{ то у кінцевому варіанті}$$

формула для оцінювання надійності функціонування системи топогеодезичного забезпечення прийме вигляд:

$$W = \frac{x_1}{x_{1\max}} \frac{1}{t_p} \int_0^{t_p} \left[ (1 - R_0 R_1)^k (1 - R_2) \right]^{\frac{x_2}{x_{2\max}}} x \quad (10)$$

$$\left( 1 - (1 - e^{-ct})^{x_2} \right) \frac{x_3}{x_{3\max}} \left( 1 - (1 - e^{-\lambda t})^{x_3} \right) dt$$

Як видно з (10),  $K_{\text{еф}}$  буде змінюватися від 0 до 1.

При цьому надійність дорівнює 100%, якщо усі канали зв'язку за якими проходить циркуляція топогеодезичної інформації функціонують справно, якщо у банку даних зберігається актуальна топогеодезична інформація, при цьому виключається можливість ураження споживачів противником.

### Висновки й перспективи подальших досліджень

Запропонований математичний підхід до

оцінювання ефективності функціонування системи топогеодезичного забезпечення, як системи масового обслуговування, дозволяє оцінити ймовірність обслуговування споживача відповідною інформацією та встановити, що виконання завдання не буде зірваним через відмови за наступними вхідними параметрами:

наявність у банку даних топогеодезичної

інформації на територію, яка необхідна споживачу; доступність та безвідмовна робота каналів зв'язку за якими проходить циркуляція топогеодезичної інформації;

наявність необхідної кількості спеціалістів, які наповнюють бази даних топогеодезичною інформацією відповідно до існуючих вимог до її точності, наочності та оперативності.

### Література

1. Чорнокнижний О. А. Теоретичні основи застосування за призначенням частин та підрозділів топографічної служби. *Вісник Київського національного університету імені Тараса Шевченка*. Київ: №2 (35), 2016. С. 43–45. 2. Положення про топографічну службу Збройних Сил України. Затв. Наказом ГШ ЗС України від 01.11.2018 р. №377. Київ: ГШ ЗС України. 2018. 3. Астахов А. Д. Пути создания модели оценки

эффективности системы топогеодезического обеспечения войск. Москва: *РИО ВТС*. 1984. 185 с. 4. Смаль С. В., Чорнокнижний О. А. Питання визначення раціонального способу виконання завдань навігаційного забезпечення. *Труди академії Національна академія оборони України*. Київ: НАОУ. 2005. С. 136-139.

## МЕТОДИКА ОЦЕНКИ НАДЕЖНОСТИ ВЫПОЛНЕНИЯ МЕРОПРИЯТИЙ ПО ТОПОГЕОДЕЗИЧЕСКОМУ ОБЕСПЕЧЕНИЮ

*Виталий Владимирович Зуйко (кандидат военных наук, доцент)*

*Сергей Валентинович Зотов*

*Александр Анатоліевич Кошлань*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*В статье рассмотрен подход к оцениванию надежности выполнения мероприятий по топогеодезическому обеспечению путем представления их как системы массового обслуживания, что дает возможность оценить вероятность обслуживания потребителя соответствующей информацией и установить, что выполнение мероприятия не будет сорванным из-за отказов по следующим входным параметрам: наличие в банке данных топогеодезической информации на территорию, которая необходима пользователю; доступность и безотказная работа каналов связи по которым происходит циркуляция топогеодезической информации; наличие необходимого количества специалистов, которые наполняют базы данных топогеодезической информацией в соответствии с требованиями к ее точности, наглядности и оперативности.*

**Ключевые слова:** топогеодезическое обеспечение; эффективность мероприятий; система массового обслуживания; надежность системы.

## METHOD OF ASSESSMENT OF RELIABILITY OF COMPLIANCE OF TOPOGEODESIC SECURITY MEASURES

*Vitalii Zuiko (Candidate of Technical Sciences, Associate Professor)*

*Serhii Zotov*

*Oleksandr Koshlan*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*The article discusses the approach to assessing the reliability of execution of topo-geodetic support measures by presenting them as a queuing system, which allows to estimate the probability of servicing the consumer with relevant information and to establish that the task performance will not be impeded due to the failure of the following input parameters: availability of topo-geodetic information in the data bank to the territory required by the consumer; availability and trouble-free operation of the communication channels through which the circulation of topo-geodetic information flows; the availability of the required number of specialists who fill the database with topo-geodetic information in accordance with the existing requirements for its accuracy, clarity and efficiency.*

**Key words:** topogeodetic support; effectiveness of measures; queuing system; system reliability.

### References

1. Chornoknyzhnyj O. A. Teoretychni osnovy zastosuvannja za pryznachennjam chastyn ta pidrozdiliv topoghrafichnoji sluzhby. *Visnyk Kyjivskogo nacionaljnogho universytetu imeni Tarasa Shevchenka*. Kyjiv: №2 (35), 2016. S. 43–45. 2. Polozhennja pro topoghrafichnu sluzhbu Zbrojnykh Syl Ukrainy. Zatv. Nakazom GhSh ZS Ukrainy vid 01.11.2018 r. №377. Kyjiv: GhSh ZS Ukrainy. 2018. 3. Astakhov A. D. Puty

sozdanyja modely ocenky efektyvnosti systemy topogheodezycheskogho obespechenija vojsk. Moskva: *RYO VTS*. 1984. 185 s. 4. Smalj S., Chornoknyzhnyj O. Pytannja vyznachennja racionaljnogho sposobu vykonannja zavdanj navighacijnogho zabezpechennja. *Trudy akademiji Nacionaljna akademija obrony Ukrainy*. Kyjiv: NAOU. 2005. S. 136-139.

Олександр Валерійович Крайнов (кандидат технічних наук, доцент)<sup>1</sup>  
 Роман Іванович Грозовський<sup>1</sup>  
 Анатолій Анатолійович Кравчук<sup>2</sup>

<sup>1</sup>Національний університет оборони України імені Івана Черняхівського, Київ, Україна

<sup>2</sup>Військовий інститут Київського національного університету ім. Т. Шевченка, Київ, Україна

## МЕТОДИКА ОЦІНКИ ЯКОСТІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОБОТИ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ УПРАВЛІННЯ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Одним із пріоритетних завдань оборонної реформи є створення ефективної системи управління військового призначення. Важливу роль у реалізації цього завдання відіграватимуть впровадження в діяльність органів управління та військ (сил) сучасних інформаційних технологій, адаптація найкращих практик та стандартів провідних країн-членів НАТО, комплексна автоматизація процесів оперативного (бойового) управління, зв'язку, розвідки та спостереження (C4ISR), обліку та управління оборонними ресурсами (DRMIS). Проблемним питанням залишається здійснення та виконання замовлень щодо створення автоматизованих інформаційних систем органів управління військового призначення, інформаційно-аналітичного забезпечення їх роботи та інформаційної інфраструктури, оскільки в Україні на цей час відсутні державні організації та приватні підприємства, які здатні самостійно виконувати увесь комплекс робіт і послуг із створення автоматизованих інформаційних систем та розгортання інформаційної інфраструктури.

**Ключові слова:** автоматизована інформаційна система; інформаційно-аналітичне забезпечення; орган військового управління; якість.

### Вступ

**Постановка проблеми.** Основна проблема організації інформаційно-аналітичного забезпечення сучасних інформаційних систем органів управління військового призначення – рішення протиріччя між збільшенням обсягу необхідної інформації і постійною вимогою до скорочення часу на її обробку. Причому саме вона визначає тенденції в розвитку цих систем, у тому числі, й підвищенні якості інформаційно-аналітичного забезпечення роботи автоматизованих інформаційних систем (АІС) органів управління військового призначення.

Розв'язання зазначеної проблеми потребує здійснення невідкладних, цілеспрямованих, скоординованих за термінами, обсягами ресурсного забезпечення заходів щодо створення АІС органів управління військового призначення, інформаційно-аналітичного забезпечення систем управління, інформаційної інфраструктури у рамках окремих відомчих програм, які мають стати основоположними документами для бюджетного планування на короткострокову та середньострокову перспективу. Інформаційно-аналітичне забезпечення роботи АІС органів управління військового призначення містить у собі комплекс заходів (сукупність усіх видів діяльності), спрямованих на збір, передачу, збереження, захист, обробку, видачу і надання даних споживачам інформації для виконання ними своїх функціональних обов'язків. У його здійсненні беруть участь різномірні по своєму складу і призначенню сили і засоби.

Важливою особливістю роботи органів управління з використанням автоматизованих систем управління військами (АСУВ) та АІС є те, що весь процес управління представляє собою інформаційно-аналітичний процес в єдиному інформаційному просторі системи управління, і який направлений на вирішення завдань інформаційно-аналітичного забезпечення органів управління військового призначення.

Інформаційно-аналітичне забезпечення органів управління військового призначення – це сукупність інформаційних продуктів, ресурсів і послуг, які надаються для забезпечення інформаційних потреб посадових осіб органів управління, і система підтримки ухвалення рішень їх управлінської діяльності.

### Аналіз остатніх досліджень і публікацій.

На даний час відомо три методи інформаційно-аналітичної підтримки роботи органів управління [1,3]: аналогія, метод статистичного аналізу і метод вивчення окремих випадків (рис. 1.).



Рис. 1. Методи інформаційно-аналітичної підтримки роботи органів управління.

Основним методом інформаційно-аналітичної підтримки роботи органів управління військового призначення доцільно вважати аналогію, так як даний метод дає найбільшу імовірність правильного кінцевого результату вивчення явища, що досліджується і надати необхідну інформацію командирів для прийняття рішення. Однак необхідно зауважити що невід'ємною задачею при обробці інформації буде оцінка її якості. Тому виникає необхідність розробки методики оцінки якості інформаційно-аналітичного забезпечення. Оцінити внесок інформаційно-аналітичного забезпечення в досягнення кінцевої мети підвищення якості роботи автоматизованих інформаційних систем органів управління військового призначення, з кількісної точки зору, на сучасному етапі розвитку теорії і практики управління військами є достатньо складною проблемою.

Тому, необхідно мати методику, за допомогою якої можна не тільки оцінити якість інформаційно-аналітичного забезпечення, але і обґрунтувати комплекс практичних рекомендацій спрямованих на його удосконалення.

### **Виклад основного матеріалу дослідження**

Оцінити якість інформаційно-аналітичного забезпечення можна різними способами, але найбільш доцільними є два. Перший полягає в тому, що інформаційно-аналітичне забезпечення оцінюється шляхом співставлення ступеню реалізації можливостей органів управління щодо інформаційно-аналітичного забезпечення організації бойових дій до потенційних можливостей. Другий полягає в тому, що оцінюється відповідність рівня інформаційно-аналітичного забезпечення вимогам, що висуваються до нього в конкретній обстановці організації бойових дій (операції). Цей спосіб під час організації бойових дій (операції) має суттєву перевагу над першим способом.

Таке положення визначає і різні потенційні можливості щодо інформаційно-аналітичного забезпечення в залежності від складу і можливостей розвідувальних органів. Тому вже потенційні можливості системи управління можуть не задовольняти необхідному рівню інформаційного забезпечення організації бойових дій (операції).

Другий спосіб дозволяє позбавитись недоліку першого способу і здійснити оцінку якості інформаційно-аналітичного забезпечення з позиції відповідності його вимогам, які висуваються під час організації бойових дій (операції):

- адекватності інформаційно-аналітичного забезпечення обстановці, що склалась;
- повноти інформаційно-аналітичного забезпечення;
- корисності інформаційно-аналітичного забезпечення;
- оперативності обробки інформації системою

інформаційно-аналітичного забезпечення органу управління .

Тому, пропонується використовувати другий підхід до оцінки якості інформаційно-аналітичного забезпечення органу управління під час організації бойових дій.

В якості критерію в цьому випадку доцільно прийняти вираз виду:

$$\Theta_{ІЗ} \geq \Theta_{ІЗ}^{\Pi} \quad (1)$$

де:  $\Theta_{ІЗ}$  – реалізуємий рівень інформаційно-аналітичного забезпечення;

$\Theta_{ІЗ}^{\Pi}$  – потрібний рівень інформаційно-аналітичного забезпечення.

В якості часткових показників оцінки інформаційно-аналітичного забезпечення обираємо адекватність інформації та оперативність обробки інформації [2,4].

Адекватність інформаційно-аналітичного забезпечення обстановці що склалась в роботі визначається ступенем адекватності інформаційно-аналітичного забезпечення, який характеризує ступінь відповідності інформації стану обстановці яка склалась.

Чисельне значення цього показника розраховується по залежності:

$$K_{ад} = \frac{\sum_{i=1}^N \sum_{j=1}^M P_{ij}}{D \cdot R} \quad (2)$$

де:  $K_{ад}$  – ступінь адекватності інформаційно-аналітичного забезпечення;

$D$  – кількість характеристик тематичного розділу інформації;

$P_{ij}$  – показник, який характеризує інформованість органів управління щодо  $i$ -ї характеристики  $j$ -го розділу інформації;

$R$  – кількість тематичних розділів інформації;

$N$  – кількість характеристик інформації;

$M$  – кількість розділів інформації.

Під раціональним рішенням розуміється рішення, яке відповідає обстановці, що склалася і реалізація якого приведе до виконання бойового завдання.

Оперативність обробки інформації системою інформаційно-аналітичного забезпечення органу управління оцінюється часом обробки інформації під час організації бойових дій (операції). Показник чисельно характеризує час, що витрачається органом управління на обробку інформації стану під час проведення процедур перетворення її в інформацію управління для виконання бойових завдань.

Використання цього показника обумовлено необхідністю урахування одного з найбільш важливих законів управління військами – відповідність потрібного часу і часу який є у розпорядженні.

Як правило, під часом який є у розпорядженні,

розуміється час директивно встановлений старшим начальником. Але в сучасних умовах, коли 70-80% об'єктів протиборчої сторони характеризуються як високоманеврені, необхідно враховувати час на протязі якого зміни обстановки не приведуть до значного зниження якості заходів організації бойових дій (операції) – критичний час ( $T_{кр}$ ). Тому спираючись на попередні дослідження [1,3] баланс часу під час організації бойових дій (операції) можна визначити:

$$T_{ou} \leq T_p, \text{ при } T_p \leq T_{кр}, \quad (3)$$

$$T_{ou} \leq T_{кр}, \text{ при } T_p > T_{кр}, \quad (4)$$

де:  $T_{ou}$  – потрібний час роботи органу управління для організації бойових дій (операції);

$T_p$  – час, що є в розпорядженні органу управління на організацію бойових дій (операції);

$T_{кр}$  – критичний час роботи органу управління для організації бойових дій (операції).

Інтегральний показник оцінки якості інформаційно-аналітичного забезпечення розраховується за наступним виразом:

$$\Theta_{із} = P_i K_{ад}, \quad (5)$$

де:  $P_i$  – імовірність прийняття рішення, що відповідає обстановці.

Кількісні показники оцінки якості інформаційно-аналітичного забезпечення розраховуються при наступних обмеженнях:

постановка бойового завдання вищим органом управління здійснюється своєчасно;

заходи, що проведені до отримання бойового завдання виконані своєчасно і в повному обсязі;

фізико-географічні фактори для усіх складових органу управління однакові і відповідають умовам оперативного напрямку.

В методиці постійними вихідними даними є:

бойовий склад угруповання протиборчої сторони і можливий характер його дій в збройному конфлікті;

склад військ (сил);

склад системи управління;

перелік заходів що виконуються органом управління під час організації бойових дій (операції);

вплив фізико-географічних умов району бойових дій (операції) на інформаційно-аналітичне забезпечення;

час, що є в розпорядженні органу управління для виконання завдань з організації бойових дій (операції);

можливості протиборчої сторони щодо ведення інформаційної боротьби;

професійна підготовка посадових осіб органу управління на рівні “задовільна”.

До змінної інформації відносяться:

обсяг інформації, яку використовує орган управління під час організації бойових дій (операції);

рівень оснащення органу управління засобами

електронно-обчислювальної техніки, зв'язку та АСУ;

організаційна структура органу управління.

Розроблена методика оцінки якості інформаційно-аналітичного забезпечення дозволяє:

визначити ступінь відповідності інформаційно-аналітичного забезпечення вимогам, що висуваються до нього під час організації бойових дій (операції);

розрахувати рівень інформаційно-аналітичного забезпечення організації бойових дій (операції);

оцінювати внесок розроблених рекомендацій в удосконалення інформаційно-аналітичного забезпечення;

оцінювати економічну доцільність впровадження практичних рекомендацій.

Схема методики оцінки якості інформаційно-аналітичного забезпечення організації бойових дій (операції) представлена на рис. 2.

В блоці 1 схеми методики формуються вихідні дані:

можливості протиборчої сторони щодо впливу на інформаційно-аналітичне забезпечення організації бойових дій (операції);

фізико-географічні умови району бойового застосування військ (сил);

склад угруповання військ (сил);

бойове завдання угруповання військ (сил і умови його виконання);

склад, стан і рівень обладнання системи управління органу управління.

В блоці 2 згідно з вихідними даними (блок 1) оцінюється обсяг корисної інформації, що є у органів управління під час організації бойових дій (операції) ( $P_i$ ).

В блоці 3 згідно з визначеною методикою і вихідними даними (блок 1) оцінюється адекватність інформації обстановці, що склалась ( $K_{ад}$ ).

В блоці 4 згідно з залежністю (1) оцінюється рівень інформаційно-аналітичного забезпечення організації бойових дій (операції) ( $\Theta_{із}$ ).

В блоці 5 на підставі вихідних даних, результатів опитування експертів розраховується потрібний рівень інформаційно-аналітичного забезпечення по залежності:

$$\Theta_{із}^{\Pi} = P_i^{\Pi} K_{ад}^{\Pi}, \quad (6)$$

де:  $\Theta_{із}^{\Pi}$  – потрібний рівень інформаційно-аналітичного забезпечення;

$P_i^{\Pi}$  – потрібна імовірність прийняття рішення, що відповідає обстановці;

$K_{ад}^{\Pi}$  – потрібний ступінь адекватності інформації.

В блоці 6 проводиться аналіз рівня інформаційно-аналітичного забезпечення і відповідність його вимогам, що висуваються під час організації бойових дій (операції).

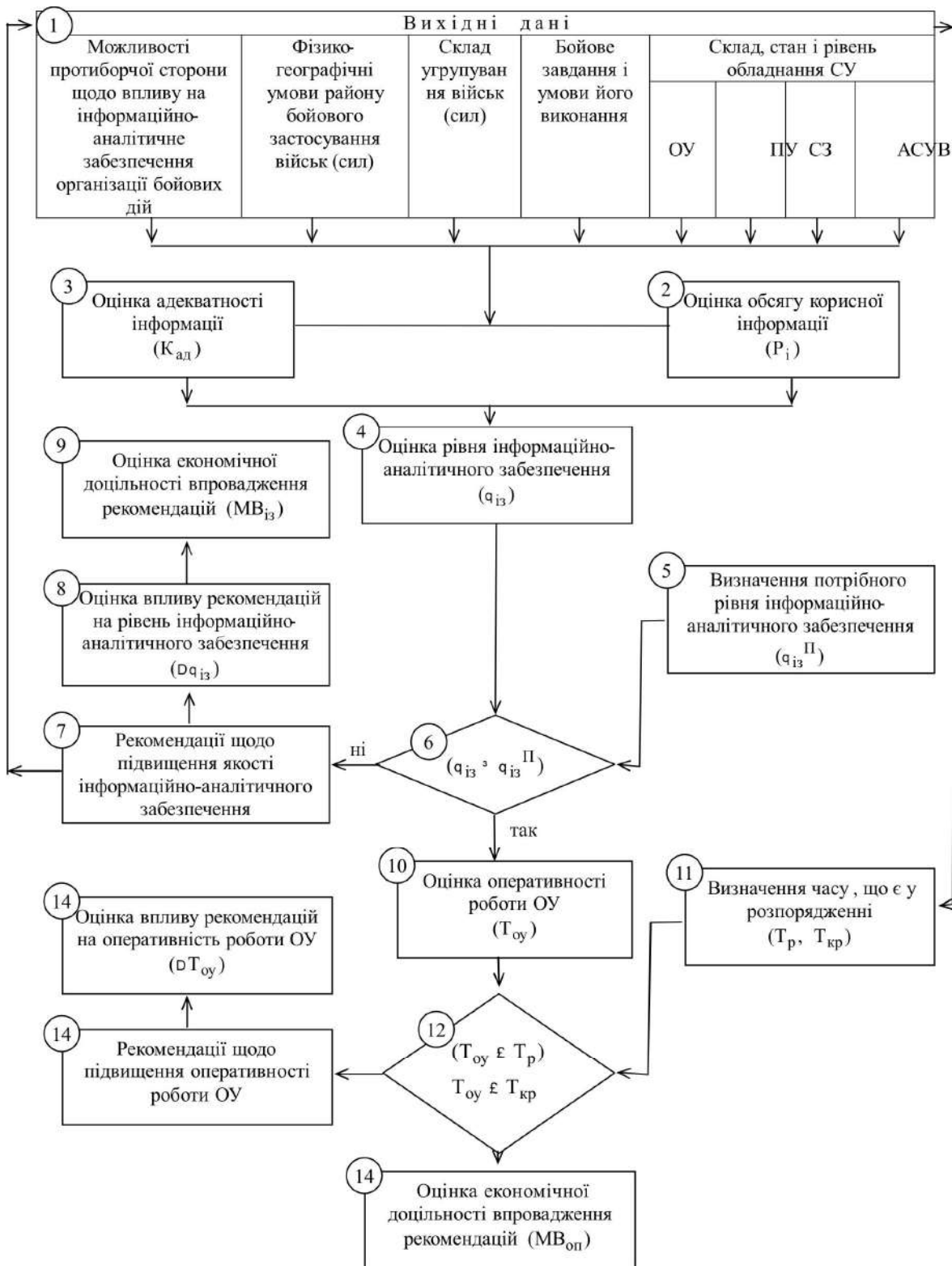


Рис. 2. Схема методики оцінки якості інформаційно-аналітичного забезпечення роботи органу управління

Якщо  $\theta_{і3} \geq \theta_{і3}^{\Pi}$  інформаційне забезпечення організації бойових дій (операції) відповідає вимогам, що до нього висуваються, якщо ні то його рівень не забезпечує повного виконання завдань організації бойових дій (операції). З метою підвищення рівня якості інформаційно-аналітичного забезпечення в блоці 7 визначаються

причини його невідповідності вимогам, що висуваються.

На підставі визначених причин невідповідності в цьому ж блоці розробляються рекомендації щодо зміни внутрішніх факторів, що впливають на рівень якості інформаційно-аналітичного забезпечення (блок 1) з метою його підвищення.



В блоці 8 проводиться оцінка впливу розроблених рекомендацій на рівень якості інформаційно-аналітичного забезпечення по залежності:

$$\Delta \theta_{13} = \frac{\theta_{13}^* - \theta_{13}}{\theta_{13}} \cdot 100\%, \quad (7)$$

В блоці 9 визначаються матеріальні витрати на одиницю приросту рівня якості інформаційно-аналітичного забезпечення по залежності:

$$MB_{13} = \frac{S}{\Delta \theta_{13}}, \quad (8)$$

В цьому ж блоці робляться висновки щодо доцільності практичного впровадження рекомендацій на підставі величини внеску в підвищення рівня якості інформаційно-аналітичного забезпечення і матеріальних витрат на їх реалізацію.

В блоці 10 проводиться оцінка оперативності обробки інформації органами управління під час організації бойових дій (операції) ( $T_{oy}$ ).

В блоці 11 визначається час, що є у розпорядженні органів управління на організацію бойових дій (операції) ( $T_p$ ) або критичний час. Після отримання абсолютної величини  $T_p$  і  $T_{kp}$  здійснюється їх порівняння. При отриманні балансу:  $T_p > T_{kp}$  на вхід блоку 12 надходить значення критичного часу. При отриманні балансу  $T_p \leq T_{kp}$ , на вхід блоку 12 надходить значення часу, що є у розпорядженні.

В блоці 12 проводиться аналіз балансу розрахованих показників, що відображають потрібну та реальну оперативність роботи органів управління під час обробки інформації при організації бойових дій (операції). Якщо баланс часу буде дорівнювати  $T_{oy} \leq T_p$ , або  $T_{oy} \leq T_{kp}$ , органи управління встигнуть своєчасно обробити інформацію під час організації бойових дій (операції). Якщо баланс часу буде іншим, потрібно визначити комплекс заходів (рекомендацій) спрямованих на зменшення потрібного часу роботи органів управління ( $T_{oy}$ ) до отримання балансу часу  $T_{oy} \leq T_p$  або  $T_{oy} \leq T_{kp}$ . Ці заходи (рекомендації) спрямовані на зміну внутрішніх факторів. Формування рекомендацій, спрямованих на підвищення оперативності обробки інформації органами управління (зменшення часу  $T_{oy}$ ) здійснюється в блоці 13.

В блоці 14 визначається внесок рекомендацій на оперативність роботи органів управління згідно з залежністю:

$$\Delta T_{oy} = \frac{T_{oy} - T_{oy}^*}{T_{oy}} \cdot 100\%, \quad (9)$$

В блоці 15 визначаються матеріальні витрати на одиницю зменшення часу на організацію бойових дій (операції) по залежності:

$$MB_{оп} = \frac{S}{\Delta T_{oy}} \cdot 100\%, \quad (10)$$

В цьому ж блоці робиться висновок щодо практичної доцільності впровадження рекомендацій на підставі внеску в зменшення часу

роботи органів управління і матеріальних витрат на їх реалізацію.

### Висновки й перспективи подальших досліджень

1. До методів інформаційно-аналітичної підтримки роботи органу управління слід віднести аналогію, метод статистичного аналізу і метод вивчення окремих випадків. Основним методом інформаційно-аналітичної підтримки роботи органу управління доцільно вважати аналогію.

2. Інформаційно-аналітичне забезпечення організації бойових дій (операції) доцільно оцінювати за допомогою показників, які характеризують вимоги, що до нього висуваються.

Кількісно оцінити ступінь відповідності інформаційно-аналітичного забезпечення вимогам, що до нього висуваються можна якщо використовувати в якості головного показника рівень інформаційно-аналітичного забезпечення роботи органу управління під час організації бойових дій (операції).

Критерієм якості інформаційно-аналітичного забезпечення обрано вираз виду (1).

3. Під час організації бойових дій (операції) до інформаційно-аналітичного забезпечення висуваються такі вимоги: адекватність інформаційно-аналітичного забезпечення обстановці, що склалась; оперативність обробки інформації системою інформаційно-аналітичного забезпечення органу управління.

Тому, частковими показниками оцінки якості інформаційно-аналітичного забезпечення обрані: ступінь адекватності інформаційно - аналітичного забезпечення; час, обробки інформації органами управління під час організації бойових дій (операції). Ці показники дозволяють з точністю, що допускається, оцінювати не тільки рівень відповідності інформаційно-аналітичного забезпечення вимогам, що до нього висуваються під час організації бойових дій (операції), але і про доцільність розроблених рекомендацій спрямованих на його удосконалення.

4. В основі оцінки якості інформаційно-аналітичного забезпечення організації бойових дій (операції) покладена логіко-аналітична методика.

Розроблена методика дозволяє визначити: ступінь відповідності інформаційно-аналітичного забезпечення вимогам, що висуваються до нього під час організації бойових дій (операції);

оцінити якість інформаційно-аналітичного забезпечення організації бойових дій (операції);

оцінювати внесок розроблених рекомендацій в удосконалення інформаційно-аналітичного забезпечення;

оцінювати економічну доцільність впровадження практичних рекомендацій.

5. Методика дає можливість дослідити якість інформаційно-аналітичного забезпечення не тільки під час організації бойових дій (операції), але і в цілому при їх підготовці.

### Література

1. Барабаш Ю.Л. Основи теорії оцінювання ефективності складних систем.-Київ:вид. НУОУ, 1999.-39с. 2. Положення про Інформаційно-аналітичний центр Головного командного центру Збройних Сил України.-К.: МОУ,2012.-51с. 3. Левкин И.М. Основы информационно-аналитической работы.-СПб.:СЗАГС, 2004.С.14-35. 4. Наказ МОУ від 29.01.14 №74.

Інструкція про порядок підготовки та надання інформаційно-аналітичних матеріалів про стан ЗСУ для інформування Адміністрації Президента України, Кабінету Міністрів України, Ради національної безпеки і оборони України, Міністра оборони України.-к.: МОУ, 2014.-155с.

## МЕТОДИКА ОЦЕНКИ КАЧЕСТВА ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАБОТЫ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ УПРАВЛЕНИЯ ВОЕННОГО НАЗНАЧЕНИЯ

*Александр Валериевич Крайнов (кандидат технических наук, доцент)<sup>1</sup>*

*Роман Иванович Грозовский<sup>1</sup>*

*Анатолий Анатольевич Кравчук<sup>2</sup>*

<sup>1</sup>*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

<sup>2</sup>*Военный институт Киевского национального университета имени Тараса Шевченко, Киев, Украина*

Одной из приоритетных задач оборонной реформы является создание эффективной системы управления военного назначения. Важную роль в реализации этой задачи играют внедрения в деятельность органов управления и войск (сил) современных информационных технологий, адаптация лучших практик и стандартов ведущих стран НАТО, комплексная автоматизация процессов оперативного (боевого) управления, связи, разведки и наблюдения (C4ISR), учета и управления оборонными ресурсами (DRMIS). Проблемным вопросом остается осуществления и выполнения заказов по созданию автоматизированных информационных систем органов управления военного назначения, информационно-аналитического обеспечения их работы и информационной инфраструктуры, поскольку в Украине в настоящее время отсутствуют государственные организации и частные предприятия, которые способны самостоятельно выполнять весь комплекс работ и услуг по созданию автоматизированных информационных систем и развертывания информационной инфраструктуры.

**Ключевые слова:** автоматизированная информационная система; информационно-аналитическое обеспечение; органа военного управления; качество.

## QUALITY ASSESSMENT METHOD OF INFORMATION-ANALYTICAL SUPPORT OF WORK OF AUTOMATED INFORMATION SYSTEMS OF MILITARY MANAGEMENT BODIES

*Oleksandr Krainov (Candidate of technical sciences, associate professor)<sup>1</sup>*

*Roman Hrozovskyi<sup>1</sup>*

*Anatolii Kravchuk<sup>2</sup>*

<sup>1</sup>*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

<sup>2</sup>*Military Institute, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine*

One of the priorities of defense reform is to create an effective military management system. An important role in the implementation of this task will be played by the introduction of modern information technologies into the management and forces (forces), adaptation of the best practices and standards of leading NATO member states, integrated automation of operational (combat) command, communication, intelligence and surveillance (C4ISR) processes. ), Defense Accounting and Management (DRMIS). The problem remains the implementation and implementation of orders for the creation of automated information systems for military administration, information and analytical support of their work and information infrastructure, since in Ukraine at present there are no state organizations and private enterprises that are able to independently perform the whole range of works and services with creation of automated information systems and deployment of information infrastructure.

**Keywords:** automated information system; information and analytical support; a military management body; quality.

### References

1. Barabash Yu.L. Fundamentals of the Theory of Estimating the Efficiency of Complex Systems. -Kyiv: View. NUOU, 1999.-39s. 2. Regulations on the Information and Analytical Center of the Main Command Center of the Armed Forces of Ukraine. -K. : MOU, 2012.-51s. 3. Levkin I.M. Fundamentals of information and analytical work. - Spb: SZAGS, 2004.S.14-35. 4. Order of the MOE of

January 29, 1474, No. 74. Instruction on the procedure for preparing and providing information and analytical materials on the state of the Armed Forces of Ukraine to inform the Administration of the President of Ukraine, the Cabinet of Ministers of Ukraine, the National Security and Defense Council of Ukraine, and the Ministry of Defense of Ukraine. -M. : MOE, 2014-2015.

**Вадим Володимирович Лук'янчук** (кандидат технічних наук, с.н.с)<sup>1</sup>

**Іван Михайлович Ніколаєв** (кандидат технічних наук, с.н.с)<sup>1</sup>

**Павло Вікторович Опенько** (кандидат технічних наук)<sup>2</sup>

**Юрій Анатолійович Дзюбенко** (кандидат військових наук, доцент)<sup>2</sup>

<sup>1</sup>Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків

<sup>2</sup>Національний університет оборони України імені Івана Черняхівського, Київ, Україна

## ШЛЯХИ І ПРИНЦИПИ РОЗВИТКУ ТЕХНОЛОГІЧНОГО БАЗИСУ ЗЕНІТНОГО РАКЕТНОГО ОЗБРОЄННЯ

На основі аналізу світових тенденцій розвитку технологій обґрунтовується структура технологічного базису, необхідного для створення і виробництва в Україні сучасних систем (комплексів) зенітного ракетного озброєння. Показано, що основу цього технологічного базису складають сукупності продуктивних і виробничих технологій, які визначають обрис складових частин (бойових і технічних засобів) зенітного ракетного озброєння, мають складну структуру і базуються на досягненнях науково-технічного прогресу у різних галузях знань. Наведені принципи розвитку технологічного базису і визначені критичні технології, розвиток яких дозволить створити науково-технологічні заділи, які можуть бути покладені в основу розробки і виробництва в Україні перспективних систем (комплексів) зенітного ракетного озброєння наступного покоління.

**Ключові слова:** зенітне ракетне озброєння; технологічний базис; макротехнологія; продуктова технологія; виробнича технологія; критична технологія; науково-технологічний заділ.

### Вступ

**Постановка проблеми.** Аналіз досвіду сучасних військових конфліктів показує, що системи (комплекси) зенітного ракетного озброєння (ЗРО) у першій чверті XXI століття будуть складати основу бойової потужності угруповань протиповітряної оборони (ППО) важливих адміністративних, промислових і військових об'єктів від ударів засобів повітряного нападу (ЗПН) противника [1]. Виходячи з цього, технологічно розвинені країни (США, Росія, Великобританія, Франція, Китай, Ізраїль, Південна Корея) активно розробляють системи (комплекси) ЗРО нового покоління. Основною тенденцією їх розвитку є підвищення ефективності боротьби з тактичними балістичними та крилатими ракетами, засобами високоточної зброї і нарощування можливостей зі знищення малопомітних аеродинамічних цілей [2, 3]. Найбільших успіхів у сфері ЗРО досягли США і Росія, які здатні здійснювати розробку і виробництво зенітних ракетних систем (комплексів) різного функціонального призначення [4]. До них належать ЗРК сімейства «Patriot», ЗРС С-300ПМУ, С-300ВМ, С-350, С-400, С-500. Країни Західної Європи (Великобританія, Франція, Італія, ФРН, Норвегія, Швейцарія, Швеція) ведуть коопераційні програми зі створення сучасних систем (комплексів) ЗРО. Так, наприклад, США, наряду з

удосконаленням ЗРК сімейства «Patriot» у даний час ведуть розробку комплексу ТНААД та у кооперації з Німеччиною та Італією – розробку ЗРК MEADS, у якому передбачається використовувати ракети PAC-3. Франція, Німеччина та Італія ведуть розробку ЗРК SAMP/T із ЗРК «Aster 30».

Сучасний етап розвитку систем (комплексів) ЗРО в провідних зарубіжних країнах здійснюється при потужній економічній підтримці держави на основі широкого використання нових знань і наукомістких технологій. При цьому ряд фахівців припускає, що широкомасштабне впровадження нових технологій змінить технічний обрис систем (комплексів) ЗРО нового покоління.

В Україні у зв'язку з різким зниженням державних асигнувань на дослідження і розробки у сфері ЗРО скоротилася кількість і масштабність науково-дослідних і дослідно-конструкторських робіт (НДДКР), що призводить до відставання від найбільш розвинених країн Заходу [5, 6]. У цих умовах пріоритетним шляхом створення ЗРО є пріоритетний розвиток наукового потенціалу України в напрямках, що визначатимуть технологічний обрис перспективних систем (комплексів) ЗРО. Реалізація цієї стратегії вимагає залучення значних ресурсів на проведення досліджень і створення нових технологій і виробництв, при цьому їх фінансування зв'язане з високим рівнем ризику. Обмеженість фінансових

ресурсів обумовлює необхідність обґрунтованого вибору раціональної кількості найбільш ефективних технологій для їх розвитку і впровадження в перспективні системи (комплекси) ЗРО. У зв'язку з цим, актуальним є аналіз сучасного стану і перспектив розвитку технологічного базису, необхідного для створення і виробництва в Україні систем (комплексів) ЗРО нового покоління.

#### **Аналіз останніх досліджень і публікацій.**

Аналіз відомих публікацій в спеціалізованих науково-технічних виданнях показав, що питанням розвитку новітніх технологій створення озброєння та військової техніки (ОВТ) в провідних країнах світу приділяється особлива увага. У монографіях [7, 8] розглянуті проблеми розвитку військових технологій у XXI столітті, питання удосконалення програмно-цільового планування і управління створенням науково-технічного заділу для перспективного і нетрадиційного озброєння. У аналітичному огляді [9] наведені перелік, характеристики, стан, перспективи розвитку і реалізації критичних технологій в США і країнах ЄС. В [10] досліджуються питання розвитку пріоритетних технологій подвійного призначення в США, Великобританії, Японії, Китаї, Німеччині, Франції, Ізраїлі та Індії. В [11] наведений прийнятий у Росії перелік базових (критичних) технологій, а також визначено поняття "науково-технічний заділ" як "накопичення знань, технологій, виробів, напівфабрикатів та інших видів продукції понад потреби". Показано, що основними елементами науково-технічного заділу є науковий, науково-технологічний і виробничо-технологічний заділи. В [12] аналізується стан і стратегія спільного розвитку вітчизняної мікроелектроніки і радіоелектроніки. В [13] наведені пропозиції щодо вдосконалення науково-методичного апарату обґрунтування складу НДДКР з розвитку радіолокаційних технологій на основі побудови структурних функціонально-технологічних схем перспективних зразків радіолокаційного озброєння. В [14] розглянуті проблемні аспекти розвитку технологій, орієнтованих на створення і застосування перспективних засобів збройної боротьби. В [15] аналізуються критичні технології, як інструмент забезпечення обороноздатності України.

В той же час у відомій науково-технічній літературі відсутні публікації, в яких розглядаються питання формування технологічного базису, необхідного для створення сучасних і перспективних систем (комплексів) ЗРО.

**Метою статті** є визначення структури і основних тенденцій розвитку технологічного базису систем (комплексів) ЗРО, як найбільш складних і науковомістких виробів військової

техніки, при створенні яких використовується широкий спектр критичних військових технологій.

#### **Виклад основного матеріалу дослідження**

Створення систем (комплексів) ЗРО нового покоління можливе при наявності у держави високорозвиненого технологічного базису, основу якого складають сукупність найбільш важливих технологій, необхідних для створення усієї номенклатури перспективних зенітних ракетних систем (комплексів) різного цільового призначення. Це обумовлює необхідність визначення пріоритетних напрямів розвитку в Україні технологічної бази створення і виробництва ЗРО нового покоління.

Досвід розвинених країн світу свідчить, що в основу розвитку технологічного базису ЗРО, слід покласти розробку базових (критичних) військових технологій і створення науково-технічного заділу у різних галузях науки і техніки. У розвинених країнах світу своєчасне створення науково-технічного заділу служить предметом особливої турботи держави. При цьому задільна фаза поглинає в цих країнах приблизно 10% від загальних бюджетних витрат на розвиток ЗРО. Досвід США свідчить, що завчасне створення необхідних технологій у формі науково-технічного заділу сприяє зменшенню витрат і скороченню термінів створення нових зразків ОВТ [9-11].

Сукупність технологій, що використовуються при створенні сучасного ЗРО, поділяються на продуктові і виробничі. Під продуктовими технологіями розуміють сукупності знань і документованих даних про принципи побудови та конструктивні, функціональні і експлуатаційні особливості конкретних систем (комплексів) ЗРО та їх складових частин як виробів військової техніки, що мають певні бойові властивості та відповідні тактико-технічні характеристики (ТТХ). Виробничі технології описують різні види технологічних процесів, які використовуються при виготовленні конкретних систем (комплексів) ЗРО, їх складових частин, функціональних вузлів, комплектуючих виробів та елементної конструкторської бази. Як продуктові, так і виробничі технології, необхідні для створення і виробництва сучасних та перспективних систем (комплексів) ЗРО, є складними об'єктами.

Для зручності аналізу тенденцій розвитку усе різноманіття технологій, які використовуються при створенні ЗРО, доцільно розбити на три групи:

1) технології створення і виробництва конкретних комплексів (систем) ЗРО та їх складових частин;

2) технології створення і виробництва функціональних систем, комплектуючих виробів та інших конструктивних елементів для систем (комплексів) ЗРО та їх складових частин;

3) технології створення і виробництва ЕКБ, нових матеріалів і речовин.

Першу групу складають технології, що описують конструктивно-технологічні особливості і способи бойового застосування систем (комплексів) ЗРО конкретного цільового призначення. Ці технології є, по суті, макротехнологіями, які включати в себе інші, так звані вкладені технології, склад і взаємозв'язки яких визначають архітектуру цих технологій в цілому [19].

Структурними компонентами макротехнологій є технології, що описують принципи побудови, функціонування, способи бойового застосування та створення складових частин ЗРО, до яких відносяться:

- 1) зенітні керовані ракети;
- 2) пускові пристрої (установки);
- 3) оглядові та стрільбові РЛС;
- 4) пункти управління;
- 5) допоміжні технічні засоби. До складу цих технологій в якості структурних елементів входять технології другої та третьої груп.

До другої групи відносяться технології, що описують конструкцію, функціонування, застосування і виробництво функціональних систем, комплектуючих виробів та інших конструктивних елементів для сучасних та перспективних систем (комплексів) ЗРО конкретного цільового призначення. До них відносяться технології створення антенних, передавальних та приймальних систем РЛС, їх функціональних вузлів, засобів обчислювальної техніки, засобів зв'язку, електроживлення, засобів рухомості та інші технології.

До третьої групи відносяться технології, що є сукупністю документованих даних і знань в галузі мікро- та наноелектроніки, оптоелектроніки і лазерної техніки, комп'ютерних та інформаційних технологій, нових матеріалів і речовин.

Структура технологічного базису створення і виробництва перспективних систем (комплексів) ЗРО, якій складається з перерахованих груп технологій, наведена на рис. 1.

Особливе місце у технологічному базису сучасного ЗРО займають технології створення і виробництва зенітних керованих ракет (ЗКР). Задоволення вимог щодо кардинального підвищення точності наведення ЗКР і зниження їх маси з одночасним збільшенням дальності і висоти ураження цілей може бути досягнуте за рахунок застосування нових ключових технологій, що забезпечують якісно вищі рівні інформаційності і маневреності ЗКР завдяки прогресу в створенні малогабаритних активних головок радіолокаційного самонаведення, бортових інерціальних систем, бортових комп'ютерів і ракетних двигунів управління [16-18]. Застосування нових ключових технологій на борту

ЗКР дозволяє об'єднати в єдину управляючу систему інформаційні і обчислювальні засоби газодинамічні і аеродинамічні пристрої управління. При цьому завдання управління вирішується на борту ЗКР, а радіолокатор системи (комплексу) ЗРО стає джерелом інформації про координати і швидкість цілі (можливо, про координати і швидкість ЗКР на початковій фазі польоту), яка передається на борт ЗКР по радіолінії.



Рис. 1. Структура технологічного базису ЗРО

ЗКР, призначені для боротьби з високоточною зброєю, крилатими ракетами і балістичними цілями, повинні підривати їх бойову частину для виключення її падіння на об'єкт, що захищається. Для досягнення цього результату потрібне пряме попадання ЗКР. Потенційна можливість кінетичного ураження цілі шляхом прямого попадання може бути забезпечена шляхом впровадження режиму надманевреності ЗКР, який реалізується газодинамічним способом створення сил і моментів. На сучасних ракетах цей режим реалізується за допомогою двигунів поперечного управління і наведення, що розташовуються поблизу центру мас і служать для усунення помилки на кінцевій ділянці польоту. Надманеврені ЗКР з газодинамічним управлінням володіють часом реакції в 10-20 разів меншим, а переваженнями на граничних висотах польоту в 10-20 разів більшими, ніж ЗКР з традиційним аеродинамічним способом створення сил і моментів.

Досвід провідних країн світу свідчить, що в основу створення технологічного базису ЗРО в Україні повинні бути покладені принципи, які

характеризують найбільш загальні риси обрис перспективних систем (комплексів) цього виду озброєння. До цих принципів належать:

- базово-модульний принцип побудови систем (комплексів) ЗРО, реалізація якого дозволяє при мінімальному типажі (базовому наборі) засобів (модулів) формувати різні за призначенням зенітні ракетні системи (комплекси);

- принцип оперативної реконфігурації систем (комплексів) ЗРО, реалізація якого дозволяє забезпечити високу ефективність і бойову стійкість перспективних систем (комплексів) ЗРО в умовах прогнозованого вогневого і радіоелектронного подавлення противника залежно від оперативно-тактичної обстановки, що складається;

- принцип багатофункціональності систем (комплексів) ЗРО, який полягає в можливості боротьби з різними типами цілей: аеродинамічними (в т. ч. що знаходяться за лінією радіогоризонту), аеробалістичними і балістичними;

- принцип міжвидової і внутрішньосистемної уніфікації, що дозволяє скоротити номенклатуру ЗРО, що розробляється, та забезпечити можливість застосування в зенітних ракетних військах, військовій ППО і ВМС одних і тих же ракет, обчислювальних засобів, засобів зв'язку, електроживлення, уніфікованих типових елементів і пристроїв. При цьому необхідний тип шасі для засобів ЗРО визначається, виходячи з фізико-географічних особливостей району можливого застосування, розвиненості дорожньої мережі та інших чинників;

- принцип мобільності, реалізація якого забезпечує можливість ведення частинами і підрозділами, оснащеними перспективними системами (комплексами) ЗРО, маневрених бойових дій без втрати зв'язку і управління, розгортання в бойовий порядок з маршру на непідготовлених позиціях і приведення їх в бойову готовність без прокладання кабельних ліній зв'язку і електроживлення;

- принцип мережевої структури побудови системи управління, реалізація якого забезпечує отримання інформації від різних джерел і обмін даними між споживачами системи, а також своєчасну видачу цілевказівки на необхідні засоби ураження і протидії в реальному масштабі часу;

- принцип інтеграції перспективних систем (комплексів) ЗРО із засобами РЕБ, авіаційними комплексами ППО;

- принцип забезпечення високої експлуатаційної надійності перспективних систем (комплексів) ЗРО упродовж усього терміну служби.

Можливість реалізації цих принципів у конкретному зразку ЗРО оцінюється на етапі зовнішнього проектування за допомогою системи

математичного моделювання, яка дозволяє формувати обрис перспективних систем (комплексів) ЗРО відповідно до їх цільового призначення, оцінювати їх основні ТТХ та обрис і ТТХ їх бойових і технічних засобів, обґрунтовувати обрис і льотно-технічні характеристики ЗКР (у тому числі за рахунок впровадження технології електронних пусків), оцінювати показники бойової ефективності в прогнозованих умовах ведення бойових дій з урахуванням вогневої і радіоелектронної протидії повітряного противника.

Використання системи математичного моделювання дозволяє за допомогою відповідних моделей оцінювати можливість і ефективність застосування таких технічних рішень, як використання активних ФАР; уніфікація приймальних і передавальних модулів, пристроїв обробки сигналів, комп'ютерів, робочих місць, шасі; автоматизація процесів бойової роботи, функціонального контролю і пошуку несправностей; застосування базово-кореляційних методів визначення координат постановників активних перешкод; застосування методу інерціального наведення ЗКР у сполученні з високоточним газодинамічним управлінням на кінцевій ділянці траєкторії.

Технічний рівень сучасних систем (комплексів) ЗРО у значній мірі залежить від номенклатури і параметрів елементної конструкторської бази (ЕКБ), виробництво якої в Україні практично відсутнє. Тому одним з актуальних питань є відновлення технологічної бази ЕКБ. Пріоритетними напрямками у цій галузі слід вважати розробку і освоєння у виробництві надвисокочастотної техніки, радіаційно-стійкої ЕКБ, мікросистемної техніки, мікроелектроніки, електронних матеріалів і структур, створення уніфікованих електронних модулів, типових базових технологічних процесів.

Аналіз існуючого науково-технологічного потенціалу свідчить про те, що в Україні для створення систем (комплексів) ЗРО потенційні розробники використовують науково-технічні заділи, які розроблені ще у радянські часи [12]. При цьому не приділяється достатньої уваги проведенню досліджень у напрямку створення сучасного науково-технологічного заділу, який може бути використаний для розробки і виробництва перспективних систем (комплексів) ЗРО конкретного цільового призначення. Одним з шляхів вирішення цього питання є визначення і затвердження на державному рівні переліку критичних технологій, що дозволить сконцентрувати існуючі фінансові і матеріальні ресурси на найбільш пріоритетних напрямках національного технологічного розвитку ЗРО.

Під критичними розуміються технології, які забезпечують істотний приріст тактико-технічних

характеристик (ТТХ) систем (комплексів) ЗРО або значне зниження необхідних ресурсних витрат на їх розробку або модернізацію [9]. Досвід розвинених країн свідчить, що до переліку критичних технологій, розробка яких дозволить Україні істотно просунути на шляху створення сучасного технологічного базису у сфері ЗРО, доцільно віднести:

- у сфері радіолокації та радіолокаційної техніки:

1) генерування, випромінювання і прийом широкопasmових зондуючих сигналів з внутрішньо-імпульсною лінійно-частотною модуляцією і фазо-ковою маніпуляцією, сигналів, що дискретно-кодуються по частоті, багаточастотних сигналів, наддовгих і надкоротких сигналів;

2) створення антенних систем з активними фазованими антенними решітками (АФАР);

3) впровадження базово-кореляційних методів визначення координат постановників активних радіоперешкод;

4) впровадження адаптивних алгоритмів обробки радіолокаційної інформації для оптимального виявлення і вимірювання координат цілей;

5) уніфікація приймальних і передавальних модулів, пристроїв обробки сигналів, обчислювальних засобів, робочих місць;

- у сфері ракетобудування:

1) створення високошвидкісних ЗКР з інерційно-активним наведенням та високоточним газодинамічним управлінням на кінцевій ділянці траєкторії;

2) розробка активно-напівактивних радіолокаційних та багатоспектральних оптико-електронних ГСН;

- у сфері інформаційних технологій:

1) автоматизація процесів бойової роботи, контролю технічного стану та пошуку місця відмов; 2) створення високошвидкісних цифрових обчислювальних комплексів;

- у сфері телекомунікаційних технологій – створення систем зв'язку і передачі даних при реалізації принципів їх мережевої побудови;

- у сфері створення нових матеріалів і комплектувальних виробів – створення і виробництво нової ЕКБ, кристалічних матеріалів, мікросистемної техніки, композиційних і керамічних матеріалів, металів і сплавів із спеціальними властивостями.

Організація і проведення досліджень у перелічених сферах вимагає істотного зростання витрат на НДДКР, створення необхідної науково-технологічної бази. Тому актуальним є формування раціонального переліку критичних технологій, розробка яких забезпечить створення перспективних систем (комплексів) ЗРО в умовах фінансових і ресурсних обмежень. Для

обґрунтування такого переліку необхідно мати відповідний методичний апарат.

В основу розробки такого апарату може бути використана ідеологія функціонально-технологічних особливостей систем (комплексів) ЗРО, яка передбачає представлення їх у вигляді “типових зразків” і структурних функціонально-технологічних схем (СФТС) [13]. При такому підході будь-яка система ЗРО може бути описана “типовим зразком”, який має максимальну функціональну і структурну спільність з системами (комплексами) ЗРО певної групи.

Аналіз структури сучасних систем (комплексів) ЗРО свідчить, що типовий зразок ЗРО може бути представлений у вигляді сукупності функціонально пов'язаних елементів, до яких відносяться:

а) базовий носій – колісне або гусеничне шасі будь-якої конфігурації, призначене для застосування в різних середовищах;

б) бойові засоби, призначені для виявлення і знищення ЗПН;

в) засоби забезпечення і обслуговування, призначені для підготовки до застосування і технічної експлуатації зразка ЗРО.

Склад бойових засобів зразка ЗРО конкретного типа встановлюється, виходячи з його функціонального призначення і може включати [2]:

1) пункти бойового управління;

2) оптико-електронні і/або радіолокаційні засоби розвідки ЗПН, які працюють у різних діапазонах хвиль (метровому, дециметровому, сантиметровому або міліметровому);

3) один або декілька типів ЗКР, які розміщуються у ТПК;

4) оптико-електронні і/або радіолокаційні засоби наведення ЗКР на цілі;

5) багатозарядні пускові установки (пристрої). Важливими елементами цих засобів є навігаційні пристрої, засоби зв'язку, спеціалізовані обчислювачі з програмно-алгоритмічним забезпеченням, автономні засоби електроживлення.

СФТС, сформована з урахуванням структури системи (комплексу) ЗРО, що пропонується для розробки (модернізації), є основою для формування раціонального варіанту НДДКР з розробки необхідних технологій.

При наявності сформованої СФТС системи (комплексу) ЗРО для відбору необхідних технологій можуть бути використані методи багатокритерійної колективної експертизи. Найбільш відомим серед цих методів є метод аналізу ієрархій (МАІ), розроблений Т. Сааті. У загальному випадку цей метод включає наступні етапи:

1) підготовка початкових даних;

2) формування груп експертів по кожному науково-технологічному напрямку, проведення

анкетування або опитування і формування бази експертних оцінок;

3) побудова матриці безпосередніх оцінок критичних технологій;

4) аналіз отриманих результатів.

Схема відбору технологій для їх реалізації на етапах розробки і постановки на виробництво виробів ЗРО наведена на рис. 2.

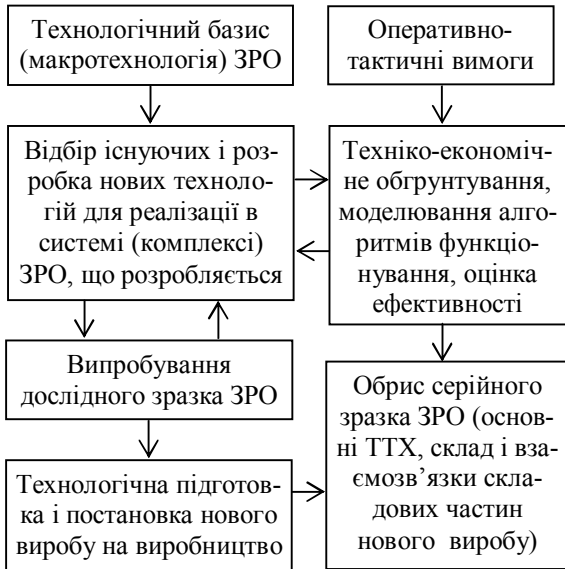


Рис. 2. Схема відбору технологій на етапах розробки і постановки на виробництво виробів ЗРО

Кількісний аспект витрат на розвиток технологічного базису ЗРО в Україні може бути сформульований у вигляді оптимізаційної задачі таким чином з безлічі можливих технологій необхідно вибрати такий перелік критичних технологій, який би забезпечив виконання завдань ППО з ефективністю, не нижче потрібної, при мінімальних витратах (втратах) сил і засобів на розробку і виробництво потрібної кількості систем (комплексів) ЗРО різного цільового призначення:

$$\hat{j} = \arg \min_{j=1,2,\dots,m} \varphi(C_j, N_j, S_j) \quad (1)$$

при

$$\vartheta(C_j, N_j, S_j) \geq \vartheta_{tr}, \quad (2)$$

де:  $C_j$  – фінансові витрати на реалізацію  $j$ -го варіанту переліку критичних технологій;

$N_j$  – кількість систем (комплексів) ЗРО, в яких може бути використаний  $j$ -й варіант переліку критичних технологій;

$S_j$  – витрати на розробку і виробництво потрібної кількості систем (комплексів) ЗРО при  $j$ -у варіанті переліку критичних технологій;

$\vartheta(C_j, N_j, S_j)$  – показник ефективності угруповання ЗРВ при  $j$ -у варіанті переліку критичних технологій;

$\vartheta_{tr}$  – необхідне значення показника ефективності угруповання ЗРВ.

### Висновки й перспективи подальших досліджень

1. Проведений аналіз свідчить, що без опори на новітні технології не може бути забезпечене подальше істотне просування України на шляху розвитку перспективних систем (комплексів) ЗРО, ефективність яких не поступається найкращим світовим зразкам.

Для вирішення цього завдання необхідно:

а) забезпечити ефективне використання і нарощування науково-технічного заділу в області технологій ракетобудування, радіолокації, інформатики, обчислювальної техніки та інших “проривних” технологій, що дозволяють створити нову матеріальну базу для розвитку ОВТ ЗРВ Повітряних Сил ЗС України;

б) відновити або розгорнути необхідні виробничі потужності в сфері мікроелектроніки, приладів надвисокої частоти, ракетних палив і вибухових речовин, спеціальних матеріалів для ракет і пускових установок;

в) створити кооперацію підприємств, наукових колективів, технологічної і експериментальної бази, яка має забезпечити модернізацію, розробку і виробництво вітчизняних зразків ЗРО.

2. Для обґрунтування пріоритетних напрямів розвитку в Україні технологічного базису у сфері створення і виробництва ЗРО нового покоління потрібні адекватний науково-методичний апарат, нормативно-методичне і нормативно-правове забезпечення. Розробка такого апарату є одним із важливих напрямів подальших досліджень у сфері розвитку технологічного базису ЗРО.

### Література

1. Ненартович Н. Э. Современные зенитные ракетные системы ПВО и нестратегической ППО // Информационно-аналитическое издание “Воздушно-космическая оборона”, 2010. 2. Коровин А. Н. Ракетные комплексы ПВО: тенденции развития. <https://topwar.ru/2217-raketnye-kompleksy-pvo-tendencii-ravzviya.html>. 3. Алексеев П., Данилов О. Состояние и перспективы развития зарубежных ЗРК большой и средней дальности // Зарубежное военное обозрение. 2006. № 11. С. 35- 43. <http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2006-zvo/7419-sostojanie-i-perspektivy->

4. Барабанов М. Зенитные ракетные системы: ситуация на мировом рынке, 2010. <https://topwar.ru/19-zenitnye-raketnye-sistemy-situaciya-na-mirovom-rynke.html>. 5. Заблоцкий В. “Оборонка” Украины: что сделано и что сделать только предстоит. <http://argumentua.com/stati/oboronka-ukrainy-cto-sdelano-i-cto-sdelat-tolko-predstoit>. 6. Щит и меч Украины: основные достижения оборонно-промышленного комплекса за 2017 год. Часть III. 7. Буренок В. М. Развитие военных технологий XXI века: проблемы, планирование, реализация / В. М. Буренок, А. А. Ивлев,



В. Ю. Корчак. – Тверь: Издательство ООО "КУПОЛ", 2009. – 624 с. **8. Буренок В. М.** Программно-целевое планирование и управление созданием научно-технического задела для перспективного и нетрадиционного вооружения / В. М. Буренок, А. А. Ивлев, В. Ю. Корчак. —М.: ИД Граница, 2007. – 408 с. **9.** Критические технологии США и стран ЕС. Аналитический обзор. <http://textarchive.ru/c-1307239-pall.html>. **10.** Приоритеты зарубежных НИОКР двойного назначения. Отв. ред. Л. В. Панкова, С. Ю. Казеннов. ИММО РАН. 2016. 236 с. [https://www.imemo.ru/files/File/ru/publ/2016/2016\\_039.pdf](https://www.imemo.ru/files/File/ru/publ/2016/2016_039.pdf) **11. Евстигнеев В.** Состояние и стратегия совместного развития отечественной микроэлектроники и радиоэлектроники //Компоненты и технологии, № 5, 2005г. С. 10-13. **12. Николаев А. И.** Совершенствование научно-методического аппарата обоснования состава научно-исследовательских и опытно-конструкторских работ по развитию радиолокационных технологий на основе построения структурных функционально-технологических схем перспективных образцов радиолокационного вооружения / А. И. Николаев, А. Д. Юрин, А. И. Полубехин // Вооружение и экономика: электронный журнал.– 2009, № 2 (6). – С. 31-39. **13. Демидов Б. А.** Проблемные аспекты развития

технологий, ориентированных на создание и применение перспективных средств вооруженной борьбы / Б. А. Демидов, С. И. Хмелевский, О. А. Хмелевская, Т. В. Кулешова // Системы озброєння і військова техніка. – 2012. – № 1 (29). – С. 101-109. **14. Величко О. Ф.** Критичні технології як національний пріоритет у забезпеченні обороноздатності держави / О. Ф. Величко, О. І. Затайнако, П. П. Скурський // Наука і оборона, 2011. – №4. – С. 23-30. **15. Болотов Е. Г., Мизрохи Б. Я.** Новое поколение зенитных управляемых ракет средней дальности // Специальный выпуск журнала «Повет» к 50-летию МКБ «Факел», 2003 г. [http://pvo.guns.ru/book/fakel/new\\_gen.htm](http://pvo.guns.ru/book/fakel/new_gen.htm). **16.** Проектирование зенитных управляемых ракет // Под ред. И.С. Голубева и В.Г. Светлова. М.: Изд-во МАИ, 2001. 732 с. **17. Акоюн И.** Мозг ракеты: особенности построения и тенденции развития головок самонаведения для ракет класса “поверхность-воздух” и “воздух-воздух”. *Воздушно-космическая оборона*, №3 (28) 2006. <http://militaryarticle.ru/voenno-kosmicheskaya-oborona/2006/12386-mozg-rocket>. **18. Ланецкий Б., Чепков І., Лук'янчук В., Николаев І.** Структура і тенденції розвитку технологічного базису сучасного зенітного ракетного озброєння середньої та великої дальності / Наука і оборона, № 4, 2013.– с 56-62.

## ПУТИ И ПРИНЦИПЫ РАЗВИТИЯ ТЕХНОЛОГИЧЕСКОГО БАЗИСА ЗЕНИТНОГО РАКЕТНОГО ВООРУЖЕНИЯ

*Вадим Владимирович Лук'янчук (кандидат технических наук, с.н.с)<sup>1</sup>*

*Иван Михайлович Николаев (кандидат технических наук, с.н.с)<sup>1</sup>*

*Павел Викторович Опенько (кандидат технических наук)<sup>2</sup>*

*Юрий Анатольевич Дзюбенко (кандидат военных наук, доцент)<sup>2</sup>*

<sup>1</sup>*Харьковский национальный университет Воздушных Сил имени Ивана Кожедуба, г. Харьков*

<sup>2</sup>*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

На основе анализа мировых тенденций развития технологий обосновывается структура технологического базиса, необходимого для создания и производства в Украине современных систем (комплексов) зенитного ракетного вооружения. Показано, что основу этого технологического базиса составляет совокупность продуктовых и производственных технологий, описывающих облик составных частей (боевых и технических средств) зенитного ракетного вооружения, имеет сложную структуру и базируется на достижениях научно-технического прогресса в разных областях знаний. Приведены принципы развития технологического базиса и определены критические технологии, развитие которых позволит создать научно-технологические заделы, которые могут быть положены в основу разработки и производства в Украине перспективных систем (комплексов) зенитного ракетного вооружения следующего поколения.

**Ключевые слова:** зенитное ракетное вооружение; технологический базис; макротехнология; продуктовая технология; производственная технология; критическая технология; научно-технологический задел.

## WAYS AND PRINCIPLES OF DEVELOPMENT OF ANTI-AIRCRAFT MISSILE SYSTEMS TECHNOLOGICAL BASE

*Vadim Lukyanchuk (Candidate of Technical Sciences, Senior Researcher)<sup>1</sup>*

*Ivan Nikolaev (Candidate of Technical Sciences, Senior Researcher)<sup>1</sup>*

*Pavlo Open'ko (Candidate of Technical Sciences)<sup>2</sup>*

*Yuri Dzubenko (Candidate of Military Sciences, Associate Professor)<sup>2</sup>*

<sup>1</sup>*Kharkiv National University of Air Force named by Ivan Kozhedub, Kharkiv, Ukraine*

<sup>2</sup>*National Defense University of Ukraine named by Ivan Cherniakhovsky, Kyiv, Ukraine*

*On the basis of analysis of world progress of technologies trends the structure of technological base, necessary for creation and production in Ukraine of the modern anti-aircraft missile systems (complexes) is substantiated. It is shown that basis of this technological base is made by the aggregate of food and productive technologies, describing the look of component parts (battle and technical facilities) of anti-aircraft rocket weapons, has a difficult structure and is based on achievements of scientific and technical progress in the different areas of knowledge. Principles over of development of technological base are brought and critical technologies, development of which will allow to create scientifically-technological reserves which can be fixed in basis of development and production in Ukraine of perspective systems (complexes) of the next generation anti-aircraft rocket weapon are presented.*

**Key words:** anti-aircraft missile system; technological base; macrotechnology; food technology; productive technology; critical technology; scientifically-technological reserve.

### References

- 1. Nenartovych N.** Sovremennye zenytnye raketnye systemy PVO y nestrategycheskoj PRO// Ynformacyonno-analytycheskoe yzdanye "Vozdushno-kosmycheskaja oborona", 2010. **2. Korovyn A. N.** Raketnye komplekсы PVO: tendency razvytyja. <https://topwar.ru/2217-raketnye-komplekсы-pvo-tendencii-razvitiya.html>. **3. Alekseev P., Danylov O.** Sostojanye y perspektivy razvytyja zarubezhnykh ZRK boljšoj y srednej daljnosty // Zarubezhnoe voennoe obozrenye. 2006. № 11. S. 35- 43. <http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2006-zvo/7419-sostojanie-i-perspektivy-razvitiya-zarubezhnyh-zrk>. **4. Barabanov M.** Zenytnye raketnye systemy: sytuacija na myrovom rynke, 2010. <https://topwar.ru/19-zenitnye-raketnye-sistemy-situaciya-na-mirovom-rynke.html>. **5. Zablockyj V.** "Oboronka" Ukrainy: chto sdelano y chto sdelatj toljko predstoyt. <http://argumentua.com/stati/oboronka-ukrainy-chto-sdelano-i-chto-sdelat-tolko-predstoyt>. **6.** Shhyt y mech Ukrainy: osnovnye dostyžhenija oboronno-promyshlennogho kompleksa za 2017 ghod. Chastj III. **7. Burenok V. M.** Razvytje voennykh tekhnologhyj XXI veka: problemy, planirovanye, realizacija / V. M. Burenok, A. A. Yvlev, V. Ju. Korchak. – Tverj: Yzdateljstvo OOO "KUPOL", 2009. – 624 s. **8. Burenok V. M.** Proghrammno-celevoe planirovanye y upravlenye sozdanyem nauchno-tekhnicheskogho zadela dlja perspektynogho y netradycyonnogho vooruzhenija / V. M. Burenok, A. A. Yvlev, V. Ju. Korchak. —M.: YD Ghranyca, 2007. – 408 s. **9.** Krytycheskye tekhnologhyj SShA y stran ES. Analytycheskyj obzor. <http://textarchive.ru/c-1307239-pall.html>. **10.** Pryorytety zarubezhnykh NYOKR dvojnogho naznachenija. Otv. red. L. V. Pankova, S. Ju. Kazennov. YMJemo RAN. 2016. 236 s. [https://www.imemo.ru/files/File/ru/publ/2016/2016\\_039.pdf](https://www.imemo.ru/files/File/ru/publ/2016/2016_039.pdf) **11.** Evstyghneev V. Sostojanye y strategyja sovместnogho razvytyja otechestvennoj mykroelektroniky y radyoelektroniky //Komponenty y tekhnologhyj, №5, 2005. S. 10-13. **12. Nykolaev A. Y.** Sovershenstvovanye nauchno-metodycheskogho apparata obosnovanyja sostava nauchno-issledovateljskykh y opytно-konstruktorskykh rabot po razvytyju radyolokacyonnykh tekhnologhyj na osnove postroenija strukturnykh funkcyonaljno-tekhnologhycheskykh skhem perspektynnykh obrazcov radyolokacyonnogho vooruzhenija / A. Y. Nykolaev, A. D. Juryn, A. Y. Polubekhyh // Vooruzhenie y ekonomyka: elektronnyj zhurnal.– 2009, № 2 (6). – S. 31-39. **13. Demydov B. A.** Problemnye aspekty razvytyja tekhnologhyj, oryentirovannykh na sozdanye y prymenenye perspektynnykh sredstv vooruzhennoj borjby / B. A. Demydov, S. Y. Khmelevskyj, O. A. Khmelevskaja, T. V. Kuleshova // Systemy ozbroennija i vijsjkova tekhnika. – 2012. – № 1 (29). – S. 101-109. **14. Velychko O. F.** Krytychni tekhnologhiji jak nacjonalnyj ppiopytet u zabezpečenni oboronozdatnosti derzhavy /O. F. Velychko, O.I. Zatynajko, P.P. Skursjkyj // Nauka i oborona, 2011. – #4. – S. 23-30. **15. Bolotov E., Myzrokhy B.** Novoe pokolenie zenytnykh upravljaemykh raket srednej daljnosty // Specyalnyj vyypusk zhurnala «Polet» k 50-letyju MKB «Fakel», 2003 gh. [http://pvo.guns.ru/book/fakel/new\\_gen.htm](http://pvo.guns.ru/book/fakel/new_gen.htm). **16.** Proektyrovanye zenytnykh upravljaemykh raket // Pod red. Y.S. Gholubeva y V.Gh. Svetlova. M.: Yzd-vo MAY, 2001. 732 s. **17. Akopjan Y.** Mozgh rakety: osobennosty postroenija y tendency razvytyja gholovok samonavedenija dlja raket klassa "poverkhnostj-vozdukh" y "vozdukh-vozdukh". Vozdushno-kosmycheskaja oborona, #3 (28) 2006. <http://militaryarticle.ru/voenno-kosmicheskaya-oborona/2006/12386-mozg-rakety>. **18. Lanecjkyj B., Chepkov I., Lukjanchuk V., Nikolajev I.** Struktura i tendenciji rozvytku tekhnologhichnogho bazysu suchasnogho zenitnogho raketnogho ozbrojennija serednjoji ta velykoji daljnosti / Nauka i oborona, № 4, 2013.– s 56-62.

*Іван Юрійович Марко* (доктор економічних наук, професор)<sup>1</sup>

*Ірина Матвіївна Чернишова* (кандидат військових наук, с.н.с.)<sup>1</sup>

*Андрій Віталійович Муштук*<sup>2</sup>

*Євген Іванович Марко* (кандидат економічних наук, с.н.с.)<sup>3</sup>

<sup>1</sup>Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

<sup>2</sup>Департамент фінансів Міністерства оборони України, Київ, Україна

<sup>3</sup>Національний університет оборони України імені Івана Черняхівського, Київ, Україна

## МЕТОДИКА ВИЗНАЧЕННЯ ОБСЯГУ ФІНАНСОВИХ РЕСУРСІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ З'ЄДНАННЯ (ЧАСТИНИ) ЗБРОЙНИХ СИЛ УКРАЇНИ НЕОБХІДНОЮ КІЛЬКІСТЮ ТЕХНІЧНО ГОТОВОГО ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

У статті представлена удосконалена методика визначення обсягу фінансових ресурсів для забезпечення з'єднання (частини) необхідною кількістю технічно готового озброєння та військової техніки (ОВТ) з метою підтримання певного рівня боєздатності цих з'єднань (частин). Методика призначена для обґрунтування обсягу фінансових ресурсів необхідних для забезпечення певного з'єднання (частини) потрібною кількістю технічно готового ОВТ з метою підтримання заданого рівня боєздатності цим з'єднанням (частиною) під час ведення бойових дій. Застосовувати її пропонується у відповідних штабах (службах) для визначення потрібного рівня фінансування під час забезпечення з'єднань (частин) технічно готовими ОВТ, що у подальшому дасть змогу підтримувати заданий рівень боєздатності. Запропонована методика має певні переваги: по-перше, запропоновано оцінювати втрати бронетанкового озброєння з'єднання (частини) на основі теорії відверненого збитку; по-друге, містить в собі механізм розрахунку необхідних фінансових ресурсів для забезпеченості з'єднання (частини) технічно готовим ОВТ з метою досягнення ним заданого рівня боєздатності; по-третє, формалізовано взаємозв'язок між обсягом фінансових ресурсів, що визначає рівень забезпеченості з'єднання (частини) технічно готовим ОВТ, та досяжним рівнем боєздатності. Застосування удосконаленої методики надасть можливість уникнути помилок під час визначення необхідних фінансових ресурсів для забезпечення з'єднань (частин) технічно готовими ОВТ.

**Ключові слова:** відвернений збиток; технічно готове озброєння та військова техніка; обсяг фінансових ресурсів; рівень боєздатності.

### Вступ

**Постановка проблеми.** Більшість країн світу прагнуть, щоб їх збройні сили мали необхідний рівень боєздатності. Україна не виключення, нині особлива увага зосереджена на питаннях витрачання бюджетних коштів для забезпечення Збройних Сил України (далі – ЗС України) та підтримання їх бойової здатності. Основною умовою забезпечення високого рівня боєздатності є наявність озброєння та військової техніки (далі – ОВТ) в необхідній кількості та належної якості. Тому, розгляд питань із обґрунтування обсягу фінансових ресурсів для забезпечення з'єднань (частин) необхідною кількістю технічно готового ОВТ з метою досягнення ними заданого рівня боєздатності є актуальним завданням сьогодення.

**Аналіз останніх досліджень і публікацій.** Питання забезпечення армій відповідними ОВТ розглядається в багатьох працях вітчизняних та зарубіжних науковців [1]–[11]. У зазначених роботах, зокрема, розглянуті питання воєнно-економічного аналізу забезпечення ЗС України в особливий період, а також і в мирний час.

Визначені проблеми забезпечення військ (сил) необхідною кількістю пально-мастильних матеріалів (далі – ПММ), іншими витратними матеріально-технічними засобами (далі – МтЗ), а також запропоновані пропозиції щодо усунення зазначених проблем в довгостроковій перспективі. Проте питання обґрунтування обсягу фінансових ресурсів для забезпечення з'єднання (частини) необхідною кількістю технічно готового ОВТ з метою досягнення заданого рівня боєздатності певних військових формувань потребують більш детального дослідження.

Враховуючи це мета статті полягає у представленні удосконаленої методики визначення обсягу фінансових ресурсів для забезпечення з'єднання (частини) необхідною кількістю технічно готового ОВТ.

### Виклад основного матеріалу дослідження

Методика визначення обсягу фінансових ресурсів для забезпечення з'єднань (частин) ЗС

України необхідною кількістю технічно готових ОВТ (далі – Методика) призначена для обґрунтування обсягу фінансових ресурсів для забезпечення певного з'єднання (частини) потрібною кількістю технічно готового ОВТ з метою підтримання заданого рівня боєздатності цим з'єднанням (частиною) під час ведення бойових дій. Застосовувати Методику пропонується у відповідних штабах (службах) для визначення потрібного рівня фінансування під час забезпечення з'єднань (частин) технічно готовими ОВТ, що у подальшому дасть змогу підтримувати заданий рівень боєздатності.

Методика надасть можливість встановити взаємозв'язок між потрібним рівнем боєздатності з'єднання (частини) та обсягом фінансових ресурсів, які необхідно виділити для забезпечення цього рівня.

Передумовами застосування Методики доцільно вважати таке.

1. Під боєздатністю слід розуміти такий стан військ (сил), який дозволяє їм успішно вести бойові дії в будь-яких умовах обстановки й реалізувати свої бойові можливості [12]. Якщо прийняти, що з'єднання (частина) повністю укомплектоване підготовленим особовим складом, забезпечене МтЗ, тоді можна вважати, що рівень боєздатності з'єднання (частини) залежить лише від забезпеченості технічно готовим ОВТ.

2. Під технічно готовим ОВТ тут розуміється працездатне ОВТ, яке заправлене ПММ та забезпечене боєкомплектами відповідно до норм забезпечення.

3. Потрібний рівень боєздатності  $\theta_{\text{вим}}$  з'єднання (частини) визначається командиром. Для забезпечення заданого рівня боєздатності необхідно мати на початок бойових дій таку кількість технічно готових ОВТ, яка в ході ведення бойових дій надасть можливість утримувати рівень боєздатності не нижче заданого. Така умова виконується, якщо з'єднання (частина) в ході бойових дій забезпечить деяку величину відверненого збитку [7].

4. За з'єднання (частину) обрано військово-формування типу механізованої бригади (далі – омбр). Основним видом забезпечення ОВТ для неї є бронетанкове озброєння (БТОТ). Розглядаються такі основні типи груп БТОТ ( $i = \overline{1,3}$ ): група № 1 – танки, група № 2 – бронетранспортери (БТР), група № 3 – броньовані машини піхоти (БМП), які, в свою чергу, розподіляються за типами.

Методика реалізується в чотири етапи. Схема Методики визначення обсягу фінансових ресурсів для забезпечення з'єднань (частин) ЗС України необхідною кількістю технічно готових ОВТ представлено на рис. 1.

На першому етапі формуються вихідні дані для певного з'єднання (частини), в даному випадку щодо окремої омбр, по групах БТОТ, які, в свою чергу групуються за типами:

$T$  – тривалість бойових дій ( $t = \overline{1, \dots, 5}$ ) (діб);

$\theta^{\text{вим}}$  – заданий рівень боєздатності омбр;

$N_{0i}$  – штатна кількість БТОТ  $i$ -го типу (од.);

$$N_0 = \sum_{i=1}^3 N_{0i} \text{ – загальна кількість БТОТ в омбр}$$

(од.);

$\beta_{0i}$  – прогнозована величина середньодобових витрат БТОТ  $i$ -го типу;

$c_i$  – вартість придбання та утримання працездатного БТОТ  $i$ -го типу (грн);

$P_{0i}$  – норма заправки ПММ БТОТ  $i$ -го типу (л);

$q_{0i}^{\text{ПММ}}$  – прогнозована величина середньодобових витрат ПММ для БТОТ  $i$ -го типу (л);

$c_{pi}$  – вартість палива для заправки БТОТ  $i$ -го типу (грн);

$BK_{0i}$  – нормативна кількість боєкомплектів для БТОТ  $i$ -го типу (од.);

$q_{0i}^{\text{БК}}$  – прогнозована величина середньодобових витрат боєприпасів для БТОТ  $i$ -го типу (доля боєкомплекту);

$cBK_i$  – вартість боєкомплекту для БТОТ  $i$ -го типу (грн).

На другому етапі визначається поточний рівень боєздатності омбр по групах БТОТ.

Для цього спочатку визначається кількість  $\Delta N_{0i}$  витрат БТОТ  $i$ -го типу протягом бойових дій тривалістю  $T$  діб:

$$\Delta N_{0i} = N_{0i} \beta_{0i} T.$$

Відповідно поточна кількість БТОТ  $i$ -го типу

$N_i^{\text{п}}$  буде становити:

$$N_{0i}^{\text{п}} = N_{0i} - \Delta N_{0i}.$$

Далі розраховується поточний рівень боєздатності омбр по групах БТОТ  $i$ -го типу, таким чином:

$$\theta_i^{\text{п}} = \frac{N_i^{\text{п}}}{N_{0i}} = \frac{N_{0i} - \Delta N_{0i}}{N_{0i}} = \frac{N_{0i} - N_{0i} \cdot \beta_{0i} \cdot T}{N_{0i}} = 1 - \beta_{0i} \cdot T.$$

Поточний рівень боєздатності за омбр розраховується за формулою:

$$\theta^{\text{п}} = \frac{\sum_{i=1}^3 N_{0i}^{\text{п}}}{N_0} = \frac{\sum_{i=1}^3 N_{0i}^{\text{п}}}{\sum_{i=1}^3 N_{0i}}.$$

Потім визначаємо, чи відповідає поточний рівень боєздатності за омбр заданому. Якщо  $\theta^{\text{п}} \geq \theta^{\text{вим}}$ , то штатної кількості техніки достатньо для досягнення заданого рівня боєздатності, якщо ні, то необхідно збільшити штатну кількість БТОТ омбр до  $N_0^{\text{вим}}$ .

На третьому етапі визначається необхідна кількість БТОТ за кожним типом техніки, наявність якої забезпечить досягнення заданого рівня боєздатності за омбр  $\theta^{\text{вим}}$ .

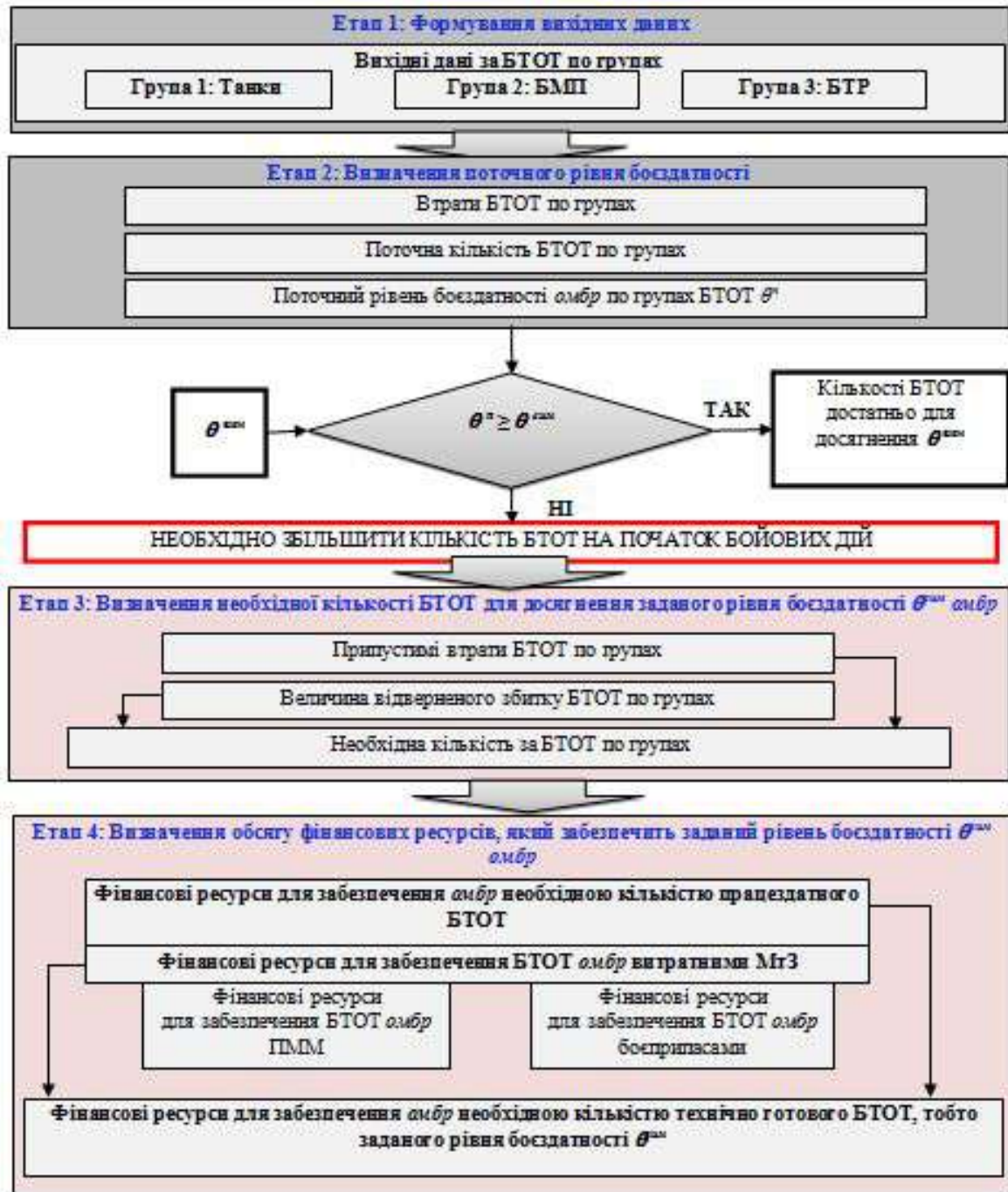


Рис. 1. Схема визначення обсягу фінансових ресурсів для забезпечення з'єднань (частин) ЗС України необхідною кількістю технічно готових ОБТ

Спочатку визначається припустиме значення середньодобових втрат  $\beta_i^p$  БТОТ і-го типу за період  $T$  бойових дій:

$$\beta_i^p = \frac{1 - \theta_i^{вум}}{T},$$

де:  $\theta_i^{вум}$  – заданий рівень боєздатності БТОТ і-го типу.

Далі розраховується величина відверненого збитку  $\delta\Pi_i$  БТОТ і-го типу за період  $T$  бойових дій:

$$\delta\Pi_i = N_{0i} \cdot (\beta_{0i} - \beta_i^p) \cdot T.$$

Наприкінці цього етапу визначається необхідна кількість БТОТ і-го типу:

$$N_{0i}^{вум} = N_{0i} + \delta\Pi_i.$$

На четвертому етапі визначається обсяг фінансових ресурсів, який забезпечить заданий рівень боєздатності  $\theta^{вум}$ . Розрахунки відбуваються покроково.

На першому кроці розраховуються кошти  $C_{inp}^{вум}$  на придбання та утримання усього потрібного працездатного БТОТ за типами:

$$C_{inp}^{вум} = N_{0i}^{вум} \cdot c_i = (N_{0i} + \delta\Pi_i) \cdot c_i.$$

Далі визначаються фінансові ресурси  $C_{np}^{вим}$  для забезпечення омбр необхідною кількістю працездатних БТОТ, що надасть можливість досягти заданого рівня боєздатності омбр  $\theta^{вим}$ :

$$C_{np}^{вим} = \sum_{i=1}^3 C_{inp}^{вим}.$$

Наступним кроком на цьому етапі є розрахунок фінансових ресурсів для забезпечення БТОТ витратними МтЗ. При цьому спочатку розраховуються кошти  $C_{ПММ}^{вим}$  для забезпечення БТОТ ПММ:

$$C_{ПММ}^{вим} = \sum_{i=1}^3 C_{iПММ}^{вим},$$

$$C_{iПММ}^{вим} = N_{0i}^{вим} \cdot P_{0i} \cdot c_{pi} + N_{0i}^{вим} \cdot q_{0i}^{ПММ} \cdot T \cdot c_{pi},$$

де:  $C_{iПММ}^{вим}$  – кошти для забезпечення БТОТ і-го типу необхідною кількістю ПММ.

Потім розраховуються кошти  $C_{БК}^{вим}$  для забезпечення БТОТ боеприпасами:

$$C_{БК}^{вим} = \sum_{i=1}^3 C_{iБК}^{вим},$$

$$C_{iБК}^{вим} = N_{0i}^{вим} \cdot BK_{0i} \cdot c_{BK_i} + N_{0i}^{вим} \cdot q_{0i}^{БК} \cdot T \cdot c_{BK_i},$$

де:  $C_{iБК}^{вим}$  – кошти для забезпечення БТОТ і-го типу необхідною кількістю боекомплектів.

Далі визначаються кошти  $C_{МтЗ}^{вим}$  для забезпечення БТОТ витратними МтЗ:

$$C_{МтЗ}^{вим} = \sum_{i=1}^3 C_{iМтЗ}^{вим}, \quad C_{iМтЗ}^{вим} = C_{iПММ}^{вим} + C_{iБК}^{вим},$$

де:  $C_{iМтЗ}^{вим}$  – кошти для забезпечення БТОТ і-го типу необхідною кількістю МтЗ.

Заключним кроком є розрахунок фінансових ресурсів для забезпечення омбр необхідною кількістю технічно готового БТОТ, тобто заданого рівня боєздатності  $\theta^{вим}$ . Для цього спочатку визначаємо кошти  $C_i^{вим}$  для забезпечення омбр необхідною кількістю технічно готового БТОТ і-го типу:

$$C_i^{вим} = C_{inp}^{вим} + C_{iМтЗ}^{вим}.$$

Потім розраховуємо кошти для забезпечення омбр усюю необхідною кількістю технічно готового БТОТ:

$$C^{вим} = \sum_{i=1}^3 C_i^{вим} \cdot C_{np}^{вим} + C_{МтЗ}^{вим}.$$

Таким чином, застосування запропонованої методики надасть можливість встановити взаємозв'язок між заданим рівнем боєздатності з'єднання (частини) та обсягом фінансових ресурсів, які потрібно виділити для забезпечення цього з'єднання (частини) необхідною кількістю технічно готових ОВТ.

### Висновки й перспективи подальших досліджень

Таким чином, запропонована методика дозволить уникнути помилок під час визначення необхідних фінансових ресурсів для забезпечення з'єднання (частини) необхідною кількістю технічно готового ОВТ, який, на відміну від існуючих, має такі переваги:

1) запропоновано оцінювати втрати БТОТ з'єднання (частини) на основі теорії відверненого збитку;

2) представлено механізм розрахунку необхідних фінансових ресурсів для забезпеченості з'єднання (частини) технічно готовим ОВТ з метою досягнення ним заданого рівня боєздатності;

3) формалізовано взаємозв'язок між обсягом фінансових ресурсів, що визначає рівень забезпеченості з'єднання (частини) технічно готовим ОВТ, та досяжним рівнем боєздатності.

Подальші наукові дослідження будуть пов'язані з проведенням чисельного експерименту, а також розробленням рекомендацій щодо визначення обсягу ресурсів для забезпечення з'єднання (частини) необхідною кількістю технічно готового ОВТ, що буде сприяти підвищенню боєздатності цих з'єднань (частин).

### Література

1. Проблеми ефективності використання військово-економічних ресурсів Збройних Сил України на сучасному етапі. Навч. посібник / За ред. М. М. Кирієнка. Київ: КВГІ, 1998. 180 с.  
 2. Викулов С.Ф. Экономика военного строительства: эволюция взглядов на проблемы, методы, решения. Москва: «Граница», 2013. 608 с.  
 3. Каневський І.Н. Разработка методического аппарата военно-экономического обоснования вариантов развития радиолокационного вооружения радиотехнических войск: дис. ... канд. техн. наук: 20.02.14 / Каневский Игорь Николаевич. Киев, 1996. 217 с.  
 4. Шевченко В.Л. Розвиток методів моделювання стану Збройних Сил України на основі логістичних функцій за умови можливих змін цілей та пріоритетів довгострокового планування: дис. ... д-ра техн. наук:

01.05.02 / Шевченко Віктор Леонідович. Київ, 2006. 421 с.  
 5. Гаврилюк І.Ю. Обґрунтування рекомендацій щодо забезпечення своєчасного підвезення потрібних матеріально-технічних засобів під час застосування оперативного угруповання військ: дис. канд. військ. наук: 20.01.05 / Гаврилюк Іван Юрійович. ЦНДІ ЗС України. Київ, 2018. 162 с.  
 6. Кубаль Р.В. Обґрунтування вимог до технічних засобів системи забезпечення військ (сил) паливом для підтримання їх боєздатності: дис. канд. військ. наук: 20.01.05 / Кубаль Руслан Володимирович. ЦНДІ ЗС України. Київ, 2018. 167 с.  
 7. Романченко І. С., Шуськін В. О., Можаровський В. М. Теорія відверненого збитку: моногр. Львів: НАСВ ЗС України, 2017. 244 с.  
 8. Теорія озброєння. Науково-технічні проблеми та завдання. Т. 6. Воєнно-економічний аналіз життєвого циклу озброєння

та військової техніки: теоретико-методологічні засади: моногр. / І. Б. Чепков, В. В. Зубарев, В. К. Борохвостов та ін. Київ: ЦНДІ ОВТ ЗС України, 2018. 475 с. 9. Методологічні засади обґрунтування складу угруповання військ (сил) для відбиття агресії: военно-теоретична праця / Телелим В. М., Загорка О. М., Стрижевський В. В. та ін. Київ: НУОУ ім. Івана Черняхівського, 2013. 368 с. 10. **Можаровський В. М.** Проблемні питання проведення мобілізаційного

розгортання ЗС України та пропозиції щодо їх вирішення. Проблемні питання підготовки військ (сил) Збройних Сил України та виконання ними завдань в особливий період: матер. наук.-практ. конф. Київ: ЦНДІ ЗС України, 2014. 11. **Шуєнкін В. О.** Щодо забезпечення боєздатності військових формувань на заданому рівні. // Зб. наук. пр. ЦНДІ ЗС України. 2016. № 3 (77). С. 45–57. 12. Военный энциклопедический словарь. Москва: Воениздат, 1983. 624 с.

## МЕТОДИКА ОПРЕДЕЛЕНИЯ ОБЪЕМА ФИНАНСОВЫХ РЕСУРСОВ ДЛЯ ОБЕСПЕЧЕНИЯ СОЕДИНЕНИЯ (ЧАСТИ) ВООРУЖЕННЫХ СИЛ УКРАИНЫ НЕОБХОДИМЫМ КОЛИЧЕСТВОМ ТЕХНИЧЕСКИ ГОТОВОГО ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ

*Иван Юрьевич Марко (доктор экономических наук, профессор)<sup>1</sup>*

*Ирина Матвеевна Чернышова (кандидат военных наук, с.н.с.)<sup>1</sup>*

*Андрей Витальевич Муштук<sup>2</sup>*

*Евгений Иванович Марко (кандидат экономических наук, с.н.с.)<sup>3</sup>*

<sup>1</sup> *Центральный научно-исследовательский институт Вооруженных Сил Украины, Киев, Украина*

<sup>2</sup> *Департамент финансов Министерства обороны Украины, Киев, Украина*

<sup>3</sup> *Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

В статье представлена усовершенствованная методика определения объема финансовых ресурсов для обеспечения соединения (части) необходимым количеством технически готового вооружения и военной техники (ВВТ) с целью поддержания определенного уровня боеспособности этих соединений (частей). Методика предназначена для обоснования объема финансовых ресурсов, необходимых для обеспечения определенного соединения (части) нужным количеством технически готового ВВТ с целью поддержания заданного уровня боеспособности этим соединением (частью) во время ведения боевых действий. Применять ее предлагается в соответствующих штабах (службах) для определения нужного уровня финансирования при обеспечении соединений (частей) технически готовыми ВВТ, что в дальнейшем позволит поддерживать заданный уровень боеспособности. Предложенная методика имеет определенные преимущества: во-первых, предложено оценивать потери бронетанкового вооружения соединения (части) на основе теории отвлеченного ущерба; во-вторых, содержит в себе механизм расчета необходимых финансовых ресурсов для обеспечения соединения (части) технически готовым ВВТ с целью достижения им заданного уровня боеспособности; в-третьих, формализовано взаимосвязь между объемом финансовых ресурсов, определяет уровень обеспеченности соединения (части) технически готовым ВВТ, и достижимым уровнем боеспособности. Применение усовершенствованной методики позволит избежать ошибок при определении необходимых финансовых ресурсов для обеспечения соединений (частей) технически готовыми ВВТ.

**Ключевые слова:** предотвращенный ущерб; технически готово вооружение и военная техника; объем финансовых ресурсов; уровень боеспособности.

## THE METHOD OF DETERMINING THE VOLUME OF FINANCIAL RESOURCES FOR THE PROVISION OF THE ARMED FORCES OF THE UKRAINE OF THE NECESSARY

*Ivan Marco (Doctor of Economic Sciences, Professor)<sup>1</sup>*

*Iryna Chenyshova (Candidate of Military Sciences, Senior Research Fellow)<sup>1</sup>*

*Andrii Mushtuk<sup>2</sup>*

*Yevhen Marco (Candidate of Economic Sciences, Senior Research Fellow)<sup>3</sup>*

<sup>1</sup> *Central Scientific Research Institute of Armed Forces of Ukraine, Kyiv, Ukraine*

<sup>2</sup> *Department of Finance, Ministry of Defense of Ukraine, Kiev, Ukraine*

<sup>3</sup> *National Defence University of Ukraine named after Ivan Cherniakhovskiy, Kyiv, Ukraine*

The article introduces an advanced technique for determining the amount of financial resources to provide a compound (part) with the required amount of technically advanced weapons and military equipment (OVT) in order to maintain a certain level of combat capability for these units (units). The technique is designed to justify the amount of financial resources needed to provide a specific (part) connection with the required

number of technically-prepared OVTs in order to maintain a given combat capability for that connection (part) during combat operations. It is proposed to be deployed at appropriate headquarters (services) to determine the required level of funding while securing joints (units) with technically ready OVTs, which will further support the required level of combat capability. The proposed method has certain advantages: First, it is proposed to estimate the loss of armor of a compound (part) on the basis of the theory of deterrent damage; secondly, it contains a mechanism for calculating the necessary financial resources to ensure the connection (part) of a technically-prepared IAF in order to achieve a given level of combat capability; third, the relationship between the amount of financial resources is formalized, which determines the level of security of the connection (part) of the technically ready IAU and the attainable level of combat capability. The use of advanced techniques will help to avoid errors in the determination of the necessary financial resources to provide joints (parts) of technically ready ATS.

**Keywords:** damage reversed; technically prepared weapons and military equipment; volume of financial resources; level of combat ability.

### References

1. Problems of efficiency of use of military-economic resources of the Armed Forces of Ukraine at the present stage. Educ. manual / Edited by M. Kirienko. Kyiv: KBGI, 1998. 180 p.
2. **S. Vikulov** Economics of military construction: the evolution of views on problems, methods, solutions. Moscow: Border, 2013. 608 p.
3. **I. Kanevsky** Development of a methodological apparatus of military-economic substantiation of options for the development of radar armament of radio-technical troops: diss. ... Cand. tech. Sciences: 20.02.14 / Igor Kanevsky. Kiev, 1996. 217 p.
4. **V. Shevchenko** Development of methods of modeling the state of the Armed Forces of Ukraine on the basis of logistical functions, subject to possible changes in the goals and priorities of long-term planning: diss. ... Dr. Tech. Sciences: 01.05.02 / Victor Shevchenko. Kyiv, 2006. 421 p.
5. **I. Havrylyuk** Substantiation of recommendations for providing timely transportation of the necessary material and technical means during the application of the operational grouping of troops: diss. Cand. troops. Sciences: 20.01.05 / Ivan Gavrilyuk. CSRI of the Armed Forces of Ukraine. Kyiv, 2018. 162 p.
6. **R. Kubal** Substantiation of requirements to the technical means of the system of providing troops (forces) with fuel to maintain their combat capability: dis. Cand. troops. Sciences: 20.01.05 / Ruslan Kubal. CSRI of the Armed Forces of Ukraine. Kyiv, 2018. 167 p.
7. **I. Romanchenko, V. Shuykinin, V. Mozharovsky** The theory of deterrent damage: monogr. Lviv: NASA Armed Forces of Ukraine, 2017. 244 p.
8. Theory of arms. Scientific and technical problems and tasks. Vol. 6. Military-economic analysis of the life cycle of weapons and military equipment: theoretical and methodological principles: monogr. / I. Chepkov, V. Zubarev, V. Borokhvostov and others. Kiev: CNII OVT Armed Forces of Ukraine, 2018. 475 p.
9. Methodological basis for the justification of the composition of the grouping of troops (forces) to repel aggression: military-theoretical work / V. Telelim, O. Zagorka, V. Strizhevsky and others. Kyiv: Ivan Chernyakhovsky, 2013. 368 p.
10. **V. Mozharovsky** Problematic issues of mobilization deployment of the Armed Forces of Ukraine and proposals for their solution. Problems of training the troops (forces) of the Armed Forces of Ukraine and performing their tasks in a special period: Mater. Research Practice Conf. Kiev: Central Research Institute of the Armed Forces of Ukraine, 2014.
11. **V. Shuenkin** On ensuring combat capabilities of military formations at a given level. // Coll. Sciences. ave the Central Research Institute of the Armed Forces of Ukraine. 2016. No. 3 (77). Pp. 45–57.
12. Military Encyclopedic Dictionary. Moscow: Voenizdat, 1983. 624 p.



Володимир Олександрович Дачковський (кандидат технічних наук)<sup>1</sup>

Лариса Михайлівна Родченко (доктор наук з державного управління, професор)<sup>2</sup>

<sup>1</sup>Національний університет оборони України імені Івана Черняхівського, Київ, Україна

<sup>2</sup>Східно-європейський слов'янський університет, Ужгород, Україна

## МЕТОДИКА ОЦІНЮВАННЯ ВІДНОВЛЮВАНOSTI ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

Особливості ведення війн та збройних конфліктів вказують на те, що для забезпечення живучості військових формувань, які приймають участь в операціях (бойових діях), одним із пріоритетів є своєчасне повернення до строю пошкоджених зразків озброєння та військової техніки. Успіх виконання завдань під час ведення збройного протистояння в значній мірі буде залежати не тільки від вогневих і ударних можливостей угруповань військ (сил), але і від того, як швидко ремонтно-відновлювані органи зможуть своєчасно відновити максимальну кількість озброєння та військової техніки, які вийшли з ладу від бойових пошкоджень або експлуатаційних несправностей.

Для зразків озброєння та військової техніки які знаходяться на озброєння ЗС України та тих які допущені до експлуатації за останні п'ять років запропоновано методику оцінювання відновлюваності озброєння та військової техніки. Згідно запропонованої методики основним оціночним параметром відновлюваності зразків ОВТ може служити середній час простою ОВТ в ремонті. Це не єдиний критерій але більш відповідний для оцінювання відновлюваності, оскільки його можна задати, виміряти або розрахувати. Дана обставина багато в чому буде сприяти і визначенню ймовірності відновлення, так як від середнього часу простою можна легко переходити до визначення ймовірності відновлення якщо відомо розподіл часу простою.

**Ключові слова:** відновлюваність, відновлення, озброєння та військова техніка, матеріально-технічні засоби, час ремонту.

### Вступ

Досвід війн та збройних конфліктів сучасності, ведення операції Об'єднаних сил на території Донецької та Луганської областей свідчить, що успіх у виконанні завдань військами (силами) під час ведення бойових дій (операції) значною мірою залежить від функціонування системи відновлення озброєння та військової техніки (ОВТ), яка є однією із функцій системи логістики Збройних Сил (ЗС) України [1]. Тому, питання, які пов'язані з удосконаленням методичних підходів щодо функціонування системи відновлення ОВТ є досить актуальними та потребують дослідження.

**Постановка проблеми.** Боездатність Збройних Сил України, ефективність їх застосування за призначенням вирішальною мірою залежить від рівня їх забезпеченості ОВТ, матеріально-технічними засобами (МТЗ), ракетами і боеприпасами, тощо [2]. У сучасних умовах ведення бойових дій (операцій) провідні країни світу зосереджують свою увагу на пошуку нових методів та способів, які б дозволили покращити функціонування системи забезпечення своїх ЗС, як в цілому, так і за їх ключовими підсистемами. Серед них особливе місце займає система відновлення ОВТ, одним із головних завдань якої

є підтримання високого рівня забезпеченості військ (сил) за рахунок своєчасного та якісного відновлення ОВТ. В свою чергу ефективність функціонування системи відновлення значною мірою буде залежати від часу повернення зразків ОВТ, які отримали бойові пошкодження або вийшли з ладу з технічних причин у підрозділи (військові частини). Виходячи з цього час повернення зразка ОВТ буде залежати від такої якості як відновлюваність. Яка залежить від навченості особового складу, часу знаходження зразка ОВТ у ремонті наявності МТЗ, оснащеності рухомих засобів ремонту тощо. Саме тому виникає низка проблемних питань серед яких особливе місце займає своєчасність та повнота відновлення ОВТ.

**Аналіз останніх досліджень і публікацій.**

Дослідженню питань відновлюваності зразків ОВТ присвячена ціла низка робіт, зокрема робота [3–4] присвячені розглянуто питання про поняття відновлюваності як однієї з найважливіших техніко-експлуатаційних властивостей машин військового призначення та визначена типова структура вимог, яка має враховуватися при розробці тактико-технічного завдання на створення новітнього озброєння і військової

техніки, а робота [5] запропоновано метод моделювання на основі комплексного підходу, що базується на побудові і дослідженні математичної моделі системи забезпечення боєздатності парку ОВТ угруповання військ. У роботі [6] проведено порівняльний аналіз сучасних систем технічного обслуговування і ремонту ОВТ ЗС України та встановлено, що прийнята в ЗС України планово-попереджувальна система технічного обслуговування і ремонту не повністю забезпечує працездатність зразків ОВТ на необхідному рівні про те яка система забезпечуватиме працездатність зразків ОВТ у роботі не розглянуто. Так у роботі [7] запропонована методика визначення складу фахівців з відновлення ОВТ, при цьому який рівень навченості спеціалістів ремонтників має бути невизначено, а у роботах [2, 8–9] запропоновано підхід до визначення трудовитрат ремонтно-відновлювальними органами під час відновлення ОВТ. В роботі [10] розглянуто порядок обґрунтування економічної доцільності проведення певного планового ремонту зразка ОВТ. В роботі [11] наводиться методика визначення обсягу обмінного фонду агрегатів для ремонту ОВТ. В літературних джерелах [12–13] запропоновані методики визначення можливостей ремонтно-відновлюваних органів з евакуації пошкоджених зразків ОВТ, при цьому не розглядаються питання, як підсистема ремонту буде залежати від підсистеми евакуації. Роботи [14–16] присвячені порядку застосування ремонтно-відновлюваних підрозділів (військових частин) при цьому, дані роботи не дають чіткої відповіді як зменшити час перебування пошкодженого зразка ОВТ у ремонтному підрозділі.

**Мета статті.** Мета статті полягає у розробленні методики оцінювання відновлюваності зразків ОВТ, які знаходяться на озброєнні ЗС України та модернізуються або заново розробляються.

Дослідження проводилося в рамках науково-дослідної роботи шифр “Потенціал”. У ході дослідження використовувалися такі методи: аналіз теоретичних джерел з проблем розвитку системи відновлення ОВТ, метод багаторазової регресії та кореляційного аналізу для встановлення математичної залежності між окремими факторами і часом ремонту ОВТ, факторний аналіз для визначення взаємодії факторів.

### **Виклад основного матеріалу дослідження**

Істотним фактором, що визначає живучість ОВТ в ході ведення бойових дій (операції), є їх відновлюваність.

Відновлюваність – порівняно нове поняття, яке отримує тепер все більше і більше поширення. Під відновлюваністю розуміється комплекс властивостей зразка ОВТ, які скорочують тривалість ремонту і економічні витрати на

ремонт [3].

Іншими словами, відновлюваність визначає такі властивості зразка ОВТ, які характеризують його пристосованість до виконання будь-якого виду ремонту.

Відновлюваність зразків ОВТ, є реальним заходом їх живучості, оскільки вона визначає можливість і тривалість їх бойового використання після ремонту. Тому розробка і модернізація зразків ОВТ з високими параметрами відновлюваності є настільки ж важливим завданням, як і забезпечення їх високих бойових і експлуатаційно-технічних якостей.

Відновлюваність ОВТ залежить від ряду факторів, найважливішими з яких є: доступність до деталей, вузлів, агрегатів, їх взаємозамінність, наявність і величина так званих баластних робіт. (слюсарно-підгінних, кріпильних, тощо).

Крім того необхідно звернути увагу, що поряд з відновлюваністю велике значення на тривалість простою зразків ОВТ в ремонті мають зовнішні умови роботи, обладнання, інструмент і кваліфікація особового складу. Перераховані вище фактори і будуть робити істотний вплив як на витрати часу, так і на якість ремонту. Тому, визначаючи відновлюваність зразка ОВТ який аналізується, необхідно враховувати вплив цих факторів.

На підставі вивчення різних видів ремонту зразків ОВТ було встановлено, що багато факторів, що впливають на терміни простою ОВТ в ремонті, можуть бути вимірянні часом і пов’язані між собою.

У загальному випадку час, що витрачається на ремонт ОВТ, залежить від трьох чинників конструкції зразка ОВТ, МТЗ та підготовки особового складу.

Конструкція зразка ОВТ – фактор, який об’єднує властивості об’єкта, до яких можна віднести: доступність, ступінь заміненості деталей, вузлів, агрегатів, наявність і величина баластних робіт, тощо. Це так званий внутрішній фактор.

Матеріально-технічне забезпечення та підготовка особового складу – це зовнішні фактори. До них відносяться наявність інструменту, обладнання та запасних частин, керівництв та інструкцій, а також кваліфікація і досвід особового складу. Визначення впливу цих факторів на час ремонту необхідно починати з вивчення числових показників ремонту [4].

Якщо вимірювати ремонтні роботи часом, то необхідно ввести числові показники, на підставі яких можна було б належним чином планувати і самі роботи і МТЗ.

До таких показників можна віднести:

час простою зразка ОВТ в ремонті (в людино-годинах);

середній час простою припадає на одну відмову (в людино-годинах)

діапазон часу простою, що припадає на відмову (пошкодження);

обсяг профілактичного обслуговування, яке виконується при даному виді ремонту (в людино-годинах), тощо.

Не менш важливою обставиною є визначення логічних етапів ремонту і розподіл часу на виконання цих етапів. У загальному випадку логічні етапи ремонту та розподіл ремонтного часу можуть бути представлені у вигляді поточного графіка ремонту [14-15].

Графік містить усі логічні етапи, а саме:

виявлення несправної деталі (вузла) шляхом аналізу роботи зразка ОВТ в момент відмови;

встановлення характеру несправності;

усунення несправності шляхом заміни або відновлення деталі (вузла);

остаточна перевірка з метою визначення працездатності.

Подібні потокові графіки можуть бути побудовані і для інших видів ремонту – середнього і капітального.

Щоб виміряти відновлюваність зразка ОВТ, необхідно розрахувати в часі ці етапи і знайти середні значення, а також функції розподілу при робочих умовах, заданих або отриманих на практиці. Така програма вимірювань, розроблена для відповідного графіка буде включати наступні дії:

вимірювання середнього значення і розподіл простоїв для кожного етапу (відшукування, усунення, перевірка) і для обраних груп деталей (вузлів);

вимірювання затрат праці для виконання кожного етапу (в людино-годинах);

облік важливості порушення функції;

оцінка впливу кваліфікації особового складу;

визначення впливу різних методів і оснащення.

За даними, отриманим згідно з пунктом І, відновлюваність визначається як час повернення спочатку для кожної окремої деталі (вузла, агрегату), а потім для зразка ОВТ в цілому. Після цього результати вимірювань можна зіставити з вимогами, складеними для проектного завдання, якщо мова йде про розробку зразка ОВТ, або намітити організаційні заходи для скорочення часу простою ОВТ в ремонті.

На підставі детального зіставлення часу повернення схожих типів агрегатів, вузлів і деталей (пункти 2–5) можна оцінити, а в подальшому і поліпшити відновлюваність зразка ОВТ шляхом зменшення часу повернення даного агрегату, вузла або деталі.

Визначаючи математичне очікування часу простою зразка ОВТ в ремонті, необхідно мати на увазі, що ремонт може бути плановим і відбуватися через правильні проміжки часу або може бути неплановим, викликаним різними відмовами, в тому числі і бойовими

пошкодженнями.

Середній час планового ремонту може бути визначено як добуток числа заміни деталей, вузлів і агрегатів при даному виді ремонту і середнього часу, який потрібен для кожної заміни. Математично це може бути представлено як

$$T_o = N_1 T_1 + N_2 T_2 + \dots + N_n T_n \quad (1)$$

де:  $N_1, N_2, N_n$  – число заміни;

$T_1, T_2, T_n$  – середній час, який необхідний для кожної заміни.

Середній час непланового ремонту може бути визначено як добуток числа заміни і суми середніх загальних витрат часу, необхідних для заміни, регулювань і введення в дію. Математично це може бути представлено як

$$T_o = N_1(T_1 + T_{a_1}) + N_2(T_2 + T_{a_2}) + \dots + N_n(T_n + T_{a_n}) \quad (2)$$

де:  $T_{a_1}, T_{a_2}, T_{a_n}$  – середній час, необхідний для проведення припасувань, регулювань і введення в дію.

Середній час простою зразка ОВТ в ремонті, отриманий таким шляхом, може служити критерієм оцінки відновлюваності зразка ОВТ який аналізується.

Поряд із середнім часом простою зразка ОВТ в ремонті для оцінки його відновлюваності може бути використаний коефіцієнт відновлюваності, що є відношенням робочого часу до загального часу ремонту.

Для того щоб визначити коефіцієнт відновлюваності, необхідно знайти робочий час, потім розділити його на повний час ремонту і отримати показник відновлюваності зразка ОВТ.

Зауважимо, що відновлюваність зразка ОВТ пов'язується з ремонтним часом певною залежністю. Функція розподілу ймовірності відновлення зразка ОВТ є інтегральна ймовірність того, що несправний зразок ОВТ повернеться в робочий стан за час простою не більше заданого. Відповідна щільність ймовірності називається щільністю ймовірності часу ремонту [2]

Тому заміряний експериментальним шляхом або отриманий методом розрахунку час ремонту має бути обов'язково пов'язаний з розподілом ймовірності відновлення, яка зазвичай логарифмічно нормальна.

Визначаючи розрахунковим шляхом відновлюваність ОВТ або вимірюючи її на практиці, необхідно мати на увазі, що ця величина багато в чому залежить від зовнішніх факторів. Оцінка відновлюваності безпосередньо пов'язана з особовим складом, з рівнем його кваліфікації, з обладнанням, інструментом і цілим рядом інших факторів.

Вимірювання відновлюваності ОВТ матиме сенс лише тоді, коли воно проводиться за певних умов, а також при використанні особового складу,

обладнання та методів, запропонованих для виконання певних завдань.

Разом з тим необхідно відзначити, що відновлюваність ОВТ залежить від того, наскільки ефективно вирішуються питання, пов'язані з кожним з цих факторів, а також наскільки враховано їх відносне значення в процесі розробки або модернізації ОВТ. Шляхом дослідження різних співвідношень між рівнем тактико-технічних параметрів і працездатністю, з одного боку, ураженістю і відновлюваністю, з іншого боку, можна досягти максимального ефекту в процесі створення (модернізації) ОВТ і випробування дослідних зразків ОВТ.

Практика лабораторних і польових випробувань показує, що існують дві групи відомостей про ремонт ОВТ, кожна з яких містить два види вихідних даних: дані про час ремонту і облік впливу окремих факторів на нього. Щоб скласти критерій для розрахунку, необхідно знайти математичну залежність між окремими факторами і часом ремонту. Статистика вказує два підходи до вирішення цього завдання: використання методу багаторазової регресії; використання кореляційного аналізу. Перший підхід дозволяє знайти кількісне співвідношення, другий дає можливість встановити, чи існує кореляція між двома випадковими величинами. Кожен з них має свої переваги, що визначають область його застосування.

Застосовуючи метод багаторазової регресії, необхідно мати на увазі, що він заснований на наступних припущеннях:

усі випадкові величини розподілені нормально;  
усі випадкові величини, які вважаються незалежними, дійсно незалежні;

окремі групи спостережень також незалежні.

Для вивчення питань відновлюваності ОВТ був обраний саме цей метод по наступних основних причинах:

ремонтний час залежить від декількох факторів;

ці фактори вважаються незалежними;

ступінь незалежності можна визначити шляхом аналізу багаторазової кореляції, що є розвитком регресивного аналізу;

ремонтний час вважається розподіленим нормально або по логарифмічно-нормальному закону;

вважається, що послідовні спостереження незалежні.

Відомо, що регресивний метод походить від методу найменших квадратів. При цьому методі складається вираз для співвідношення між відхиленнями залежних і незалежних випадкових величин від середнього, тобто

$$\sum (y - b_1 x_1 - b_2 x_2 - \dots - b_n x_n) \quad (3)$$

Потрібно знайти коефіцієнти  $(b_1, b_2, \dots, b_n)$ , при

яких це відхилення мінімально.

Диференціюючи цей вираз по кожному змінному коефіцієнту, отримуємо рівняння для кожного невідомого. Рішуючи ці рівняння, знаходимо коефіцієнти зв'язку  $x$ .

Остаточне рівняння, що зв'язує величини пошуку, знаходимо підставляючи отримані коефіцієнти в наступне рівняння

$$M_t = \bar{M}_t = a + b_1(x_1 - \bar{x}_1) + b_2(x_2 - \bar{x}_2) + \dots \quad (4)$$

яке в свою чергу дає

$$M_t = C + b_1 x_1 + b_2 x_2 + \dots \quad (5)$$

де:  $M$  – час ремонту, год.;

$x_1, x_2$  – оцінки впливу факторів;

$b_1, b_2$  – коефіцієнти, що зв'язують оцінки (факторів з часом ремонту);

$C$  – постійна величина.

Звідси видно, що знаючи коефіцієнти, постійний член і, ввівши будь-який набір оціночних факторів, можна визначити час ремонту. Для регресивного аналізу потрібно представити кількісний фактор, для якого потрібно знайти зв'язок з часом ремонту. У деяких випадках виконати це нелегко. Однак кореляційний аналіз дозволяє досліджувати фактори, які важко виділити, щоб встановити, чи існує значущий зв'язок.

Більш складний різновид цього методу – так званий факторний аналіз, при якому знаходять не тільки дисперсію кожного фактора, а й визначають взаємодію факторів. Крім того, цей метод дозволяє застосувати математичний підхід при побудові експерименту, що в багатьох випадках може привести до спрощення процесу випробування.

Застосовуючи два вищевказаних методи, можна обчислити числові показники ремонту, які в подальшому можуть увійти в технічні вимоги на розробку (модернізацію) зразків ОВТ.

У нашому випадку розрахункове рівняння для трьох основних чинників (конструкція, особовий склад, МТЗ) може бути виражено як

$$M_t = b_1 x_k + b_2 x_{oc} + b_3 x_{MT3} + C \quad (6)$$

Застосовуючи операції розрахунку до нового об'єкту, при розгляді конструкції можна прямо впливати на фактор  $x_k$ . Природно, що необхідно враховувати і особовий склад і матеріально-технічне забезпечення, але в стадії розробки зразка ОВТ їх неможливо безпосередньо виміряти.

Тому вираз (32) найкраще представити у вигляді наступного рівняння, що зв'язує час ремонту з конструкцією зразка ОВТ

$$M_t = b_1 x_k + C. \quad (7)$$

Оскільки за даними, отриманими в польових умовах, зазвичай визначаються середні оцінки впливу МТЗ та особового складу, то їх можна

використовувати при оцінюванні конструкції зразка ОБТ, який розробляється.

Розрахункове рівняння (6) дозволяє зв'язати час ремонту з визначальним його чинником. Однак потрібно ще розробити практичний метод використання цього рівняння. Такий метод складається з огляду конструкції, аналізу вибіркового завдань, оцінки і обчислень.

В огляд конструкції входить встановлення однорідності деталей, вузлів, агрегатів зразка ОБТ який аналізується. При огляді повинні бути враховані відмінності способів їх виготовлення, компонування та інші чинники, що впливають на відновлюваність.

При наявності істотних відмінностей на ділянках розмірних ланцюгів необхідно провести аналіз кожної ділянки окремо і з окремих результатів скласти загальну оцінку. За допомогою перевіркового списку конструкції зразка ОБТ можна буде встановити, чи буде необхідність в подальшому аналіз окремих ділянок. Після цього необхідно скласти відповідний план вибірок для визначення відновлюваності зразка ОБТ. Такий план повинен, включати типові несправності (пошкодження), для кожної з яких встановлюється, оцінний критерій. Ввівши ці оцінки в рівняння розрахунку, можна знайти очікуваний час ремонту для кожної операції.

Ці визначені витрати часу необхідно буде уточнити за чинниками навколишніх умов. Оскільки ремонтні операції в умовах бойової діяльності військ обумовлені інтенсивністю відмов (пошкоджень), то за цими операціями можна відібрати типові несправності. Після відбору операцій потрібно застосувати оцінки конструкцій до кожної несправності. Потім оцінки вводяться в розрахункове рівняння і визначається час, необхідний для кожної операції.

Підсумовуючи витрати часу, можна знайти повний час усіх операцій. Це можна виразити як

$$M_{\text{ит}} = \sum M_t \quad (8)$$

Оскільки ремонтні операції виникають не лише через відмови запасних частин тоді потрібно ввести у величину знайденого часу відповідну поправку. З цією метою вводиться певний коефіцієнт  $K$ , що дорівнює відношенню часу ремонту, внаслідок істинно випадкових операцій на часі операцій, викликаних іншими причинами.

Вводячи цей коефіцієнт, отримуємо наступне рівняння

$$M_{\text{ат}} = M_{\text{ит}}(1 + K) \quad (9)$$

При використанні цього рівняння необхідно виключити час, витрачений випадковим причин, так як його не можна пов'язати з факторами які вимірюються. Відношення цього часу до загального часу ремонту зазвичай відомо. Отже, можна отримати остаточну оцінку часу, необхідного для виконання відібраних операцій.

Вона може бути виражена в загальному випадку як

$$M_t = M_{\text{ат}}(B + 1) \quad (10)$$

Однак отриманий розрахунковим шляхом час ремонту ще не може в достатній мірі служити показником відновлюваності зразка ОБТ який розробляється або модернізується, хоча б тому, що він не враховує рівні і вплив баластних робіт. У зв'язку з цим необхідно розрахунковий час висловити через показник відновлюваності. Для цього необхідно знайти еквівалентну робочого часу шляхом зменшення середнього часу між двома відмовами (ураженнями) на певну кількість відмов. Потім розділити робочий час на розрахунковий ремонтний і отримати показник відновлюваності.

Слід зауважити, що отриманий розрахунком час ремонту доцільно розбити на дискретні елементи, а потім, узагальнивши відповідні дані випробувань, скласти, показники часу простою для заміни стандартних деталей, вузлів, агрегатів. З цього випливає, що час простою для заміни деталі, вузла або агрегату можна розрахувати після того, як конструктор описав окремі стадії, необхідні для виконання даної операції.

Даний спосіб має переваги, основна з яких полягає в тому, що опис кожної елементарної операції змушує конструктора враховувати побудову завдань, які він покладає на обслуговуючий персонал.

Таким чином, першу наближену оцінку відновлюваності зразка ОБТ конструктор може зробити при первісному задумі, помноживши середній час простою який припадає на відмову, на коефіцієнт розподілу деталей і на відповідну інтенсивність відмов.

Описаний метод розрахунку дає найбільшу точність, коли його застосовують до дослідних зразків ОБТ. При використанні цього методу для серійних машин, що знаходяться в експлуатації, його точність значно знижується. Пояснюється це в першу чергу тим, що відновлюваність зразків ОБТ не є величиною постійною і незмінною. Вона погіршується в процесі експлуатації зразка ОБТ.

При напрацюванні до міжремонтного строку зразком ОБТ середній час, необхідний для заміни деталі, вузла, агрегату, а також на взаємну установку, виставку і центрування агрегатів, вузлів, в значній мірі збільшується за рахунок збільшення слюсарно-підгінних робіт. Збільшується також середній час, необхідний для підключення контрольно-регулювальних пристроїв і на приведення зразка ОБТ в робочий стан. У зв'язку з цим в практиці експлуатації ОБТ з метою визначення показника їх відновлюваності доцільно користуватися рівняннями (1) і (2) в залежності від того, який вид ремонту проводиться на зразку ОБТ (плановий або позаплановий) і який термін роботи зразок ОБТ до цього часу відпрацював.

## Висновки й перспективи подальших досліджень

Таким чином, основним оціночним параметром відновлюваності зразків ОВТ може служити середній час простою ОВТ в ремонті. Це не єдино можливий критерій але більш відповідний для оцінки відновлюваність, оскільки його можна задати, виміряти або розрахувати. Остання обставина багато в чому буде сприяти і визначенню ймовірності відновлення, так як від середнього часу простою можна досить легко переходити до визначення ймовірності відновлення якщо відомо розподіл часу простою, а його, як вказувалося вище, можна вважати логарифмічно нормальним. Всі показники, необхідні для визначення робочого часу та

повного часу ремонту, можуть бути отримані дослідним шляхом в процесі експлуатації і ремонтів зразків ОВТ.

Цілком природно, що подібний метод мало прийнятний до дослідних зразків, не кажучи про заново створених, оскільки за цими зразками конструктор не буде мати у своєму розпорядженні дослідні дані. В цьому випадку теоретичні розрахунки, вироблені за допомогою рівнянь (9) і (10), є єдиним шляхом, що дає можливість отримати оцінку відновлюваності.

В подальшому, необхідно розробити методичку оцінювання захищеності зразка ОВТ та визначити як захищеність зразка ОВТ впливатиме на його відновлюваність.

## Література

**1. Павловський О.В.** Метод прогнозування обсягів завдань, що покладатимуться на ремонтно-відновлювальні органи під час операції (бойових дій) / О. В. Павловський // Збірник наукових праць Харківського університету Повітряних Сил. - 2016. - Вип. 2. - С. 15-18. - Режим доступу: [http://nbuv.gov.ua/UJRN/ZKhUPS\\_2016\\_2\\_6](http://nbuv.gov.ua/UJRN/ZKhUPS_2016_2_6).

**2. Дачковський В.О.** Оперативні розрахунки завдань технічного забезпечення (методика та приклади) / В.О. Дачковський, І.В. Овчаренко, О.В. Ярошенко, Н.К. Багдасарян – К.: НУОУ ім. Івана Черняховського, 2018. – 116 с.

**3. Шишанов М. О.** Відновлюваність як одна з найважливіших техніко-експлуатаційних властивостей машин військового призначення / М. Шишанов, С. Котлярєвський, М. М. Шевцов, Л. Кобяков // Social development & Security. - 2017. - Vol. 1, Iss. 1. - С. 3-13. - Режим доступу: [http://nbuv.gov.ua/UJRN/socdevsec\\_2017\\_1\\_1\\_3](http://nbuv.gov.ua/UJRN/socdevsec_2017_1_1_3)

**4. Дачковський В.О.** Підходи щодо відновлюваності озброєння та військової техніки / Дачковський В.О., Сампір О.М., Веретнов А.О. // Проблеми якості оборонної продукції: організаційні, технічні та фінансово-економічні аспекти НУОУ міжгалузева науково-практична конференція 22–23 травня 2019 тези. доп. – Київ, 2019 – С. 25.

**5. Шишанов М.О.** Обґрунтування методу моделювання процесу функціонування системи відновлення озброєння та військової техніки угруповання військ / М.О. Шишанов, А.В. Гуляєв, М.М. Шевцов // Озброєння та військова техніка. - 2017. - № 1. - С. 75-77. - Режим доступу: [http://nbuv.gov.ua/UJRN/ovt\\_2017\\_1\\_14](http://nbuv.gov.ua/UJRN/ovt_2017_1_14)

**6. Кривцун В. І.** Порівняльний аналіз існуючих систем технічного обслуговування і ремонту машин інженерного озброєння [Текст] / В. І. Кривцун, В. Й. Нагачевський, А. М. Баранов // Вісник машинобудування та транспорту. - 2015. - № 1. - С. 33-45.

**7. Морозов О. О.** Методика визначення складу фахівців з відновлення озброєння і військової техніки / О. О. Морозов // Збірник наукових праць Національної академії Національної гвардії України. - 2015. - Вип. 1. - С. 69-72. - Режим доступу: [http://nbuv.gov.ua/UJRN /znpravs\\_2015\\_1\\_14](http://nbuv.gov.ua/UJRN /znpravs_2015_1_14)

**8. Шишанов М. О.** Методичні основи розрахунку трудовитрат на виконання відновлювального ремонту бронетанкового озброєння та техніки [Електронний ресурс] / М. О. Шишанов, В. Г. Козлов, М. М. Шевцов

// Збірник наукових праць Військової академії (м. Одеса). Технічні науки. - 2017. - Вип. 1. - С. 50-53. - Режим

доступу: [http://nbuv.gov.ua/UJRN/zbnpva\\_2017\\_1\\_1](http://nbuv.gov.ua/UJRN/zbnpva_2017_1_1)

**9. Дачковський В.О.** Шляхи підвищення ефективності відновлення озброєння та військової техніки / Дачковський В.О., Сампір О.М. // Службово-бойова діяльність Національної гвардії України: сучасний стан, проблеми та перспективи Збірник тез доповідей науково-практична конф. 14 березня 2019 тези доп. – Харків, 2019 – С. 50.

**10. Закусило П. С.** Метод визначення економічної доцільності проведення планового ремонту на зразках озброєння та військової техніки / П. С. Закусило // Системи озброєння і військова техніка. - 2016. - № 1. - С. 21-24. - URL: [http://nbuv.gov.ua/UJRN/soivt\\_2016\\_1\\_7](http://nbuv.gov.ua/UJRN/soivt_2016_1_7)

**11. Морозов О.О.** Методика визначення обсягу обмінного фонду агрегатів для ремонту озброєння і військової техніки / О. О. Морозов // Військово-технічний збірник. - 2017. - № 16. - С. 55-59. - URL: [http://nbuv.gov.ua/UJRN/vtzb\\_2017\\_16](http://nbuv.gov.ua/UJRN/vtzb_2017_16)

**12. Дачковський В.О.** Основи евакуації озброєння та військової техніки / В.О. Дачковський, І.В. Овчаренко, О.В. Ярошенко – К.: НУОУ ім. Івана Черняховського, 2017. – 180 с.

**13. Коваленко О. А.** Оцінювання можливостей ремонтно-відновлювальних органів з евакуації пошкоджених зразків озброєння та військової техніки / О.А. Коваленко, // Сучасні інформаційні технології у сфері безпеки та оборони. – К., 2016. – № 2 (22). – С. 149 – 154.

**14. Застосування підрозділів та військових частин технічного забезпечення** / І.Б. Кузнецов, О.В. Ярошенко, І.В. Овчаренко, В.О. Дачковський, О.Д. Яльницький, Н.К. Багдасарян, Б.Т. Кузнецов Ч. І: Підрозділи технічного забезпечення: навч. посіб. – К.: НУОУ ім. Івана Черняховського, 2017. – 136 с.

**15. Кузнецов І.Б.** Застосування підрозділів та військових частин технічного забезпечення. Ч. II: Ремонтно-відновлювальна військова частина: навч. посіб. / [І.Б. Кузнецов, О.В. Ярошенко, І.В. Овчаренко, В.О. Дачковський]. – К. : НУОУ ім. Івана Черняховського, 2018. – 80 с.

**16. Управління ремонтно-відновлювальною військовою частиною** / І.Б. Кузнецов, С.А. Копашинський, О.В. Ярошенко, А.М. Терещенко, І.В. Овчаренко, О.Д. Яльницький, В.О. Дачковський К.: НУОУ ім. Івана Черняховського, 2016. – 64 с.

**МЕТОДИКА ОЦЕНКИ ВОССТАНАВЛИВАЕМОСТИ  
ВООРУЖЕНИЕ И ВОЕННАЯ ТЕХНИКА**

*Владимир Александрович Дачковский (кандидат технических наук)<sup>1</sup>  
Лариса Михайловна Родченко (доктор наук по государственному управлению, профессор)<sup>2</sup>*

<sup>1</sup> *Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*  
<sup>2</sup> *Восточно-европейский славянский университет, Ужгород, Украина*

*Особенности ведения войн и вооруженных конфликтов указывают на то, что для обеспечения живучести военных формирований, участвующих в операциях (боевых действиях), одним из приоритетов является своевременное возвращение в строй поврежденных образцов вооружения и военной техники. Успех выполнения задач при ведении вооруженного противостояния в значительной степени будет зависеть не только от огневых и ударных возможностей группировок войск (сил), но и от того, как быстро ремонтно-восстановительные органы смогут своевременно восстановить максимальное количество вооружения и военной техники, которые вышли из строя от боевых повреждений или эксплуатационных неисправностей.*

*Для образцов вооружения и военной техники находящихся на вооружение ВС Украины и тех, которые допущены к эксплуатации за последние пять лет предложена методика оценки восстанавливаемости вооружения и военной техники. Согласно предложенной методике основным оценочным параметром восстанавливаемости образцов ВВТ может служить среднее время простоя ВВТ в ремонте. Это не единственный критерий но более подходящий для оценки восстанавливаемости, поскольку его можно задать, измерить или рассчитать. Данное обстоятельство во многом будет способствовать и определению вероятности восстановления, так как от среднего времени простоя можно легко переходить к определению вероятности восстановления если известно распределение времени простоя.*

**Ключевые слова:** *восстанавливаемость, восстановление, вооружение и военная техника, материально-технические средства, время ремонта.*

**RECOVERY METHODOLOGY  
WEAPONS AND MILITARY EQUIPMENT**

*Volodymyr Dachkovskiy (Candidate of Technical Sciences)<sup>1</sup>  
Larisa Rodchenco (Doctor of Sciences in Public Administration, Professor)<sup>2</sup>*

<sup>1</sup> *National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*  
<sup>2</sup> *East European Slavic University, Uzhhorod, Ukraine*

*Features of warfare and armed conflict indicate that, in order to ensure the viability of military units participating in operations (combat operations), one of the priorities is the timely return to service of damaged weapons and military equipment. The success of the missions in conducting armed confrontation will largely depend not only on the firing and strike capabilities of the troop (forces), but also on how quickly the repairing and repairing bodies will be able to timely restore the maximum number of weapons and military equipment withdrawn. damage from combat damage or operational failure.*

*For samples of weapons and military equipment that are in service with the Armed Forces of Ukraine and those that have been commissioned in the last five years, a method for assessing the recoverability of weapons and military equipment is proposed. According to the proposed method, the average estimation parameter of the reproducibility of the IAU samples can serve as the average time for an IAO to be repaired. This is not the only criterion but more suitable for assessing reproducibility because it can be set, measured or calculated. This fact will greatly contribute to the determination of the probability of recovery, since from the average downtime can easily go to determining the probability of recovery if you know the distribution of downtime.*

**Keywords:** *recoverability, renewal, weapons and military equipment, logistical equipment, repair time.*

## References

- 1. Pavlovsky O.V.** The method of forecasting the volume of tasks that will be entrusted to the repair and restoration organs during the operation (combat operations) / O.V. Pavlovsky // Collection of scientific papers of Kharkov University of the Air Force. - 2016. - VIP. 2, pp. 15-18. - Access mode: [http://nbuv.gov.ua/UJRN/ZKhUPS\\_2016\\_2\\_6](http://nbuv.gov.ua/UJRN/ZKhUPS_2016_2_6).
- 2. Dachkovskiy V.A.** Operational calculations of technical support tasks (methodology and examples) / V.A. Dachkovskiy, I.V. Ovcharenko, O.V. Yaroshenko, N.K. Baghdasaryan - K.: NGO Ivan Chernyakhovsky, 2018. - 116 p.
- 3. Shishanov M.A.** Reproducibility as one of the most important technical and operational properties of military vehicles / M. Shishanov, S. Kotlyarevsky, MM Shevtsov, L. Kobayakov // Social development & Security. - 2017. - Vol. 1, Iss. 1. - P. 3-13. - Access mode: [http://nbuv.gov.ua/UJRN/socdevsec\\_2017\\_1\\_1\\_3](http://nbuv.gov.ua/UJRN/socdevsec_2017_1_1_3)
- 4. Dachkovskiy V.A.** Approaches to the renewability of weapons and military equipment / Dachkovskiy V.A., Sampir O.M., Veretnov A.A. // Problems of quality of defense products: organizational, technical and financial and economic aspects of NGOs Inter-sectoral scientific-practical conference May 22-23, 2019 abstract. ext. - Kyiv, 2019 - P. 25.
- 5. Shishanov M.O.** Substantiation of the method of modeling of the process of functioning of the system of renewal of arms and military equipment of the grouping of troops / MO. Shishanov, AV Gulyaev, N.M. Shevtsov // Weapons and military equipment. - 2017. - № 1. - P. 75-77. - Access mode: [http://nbuv.gov.ua/UJRN/ovt\\_2017\\_1\\_14](http://nbuv.gov.ua/UJRN/ovt_2017_1_14)
- 6. Kryvtsun V.I.** Comparative Analysis of Existing Systems of Maintenance and Repair of Engineering Weapons [Text] / VI Krivtsun, VY Nagachevsky, AM Baranov // Bulletin of Mechanical Engineering and Transport. - 2015. - № 1. - P. 33-45.
- 7. Morozov O.O.** Methods of determining the composition of specialists in the restoration of weapons and military equipment / OO Morozov // Collection of scientific papers of the National Academy of the National Guard of Ukraine. 2015. Vip. 1, pp. 69-72. Access mode: [http://nbuv.gov.ua/UJRN/znpavs\\_2015\\_1\\_14](http://nbuv.gov.ua/UJRN/znpavs_2015_1_14)
- 8. Shishanov M.** Methodical bases of calculation of labor costs for performing repair of armored weapons and equipment [Electronic resource] / MA Shishanov, VG Kozlov, MM Shevtsov // Collection of scientific works of the Military Academy (Odessa). Engineering sciences. - 2017. - Vip. 1, pp. 50-53. - Access mode: [http://nbuv.gov.ua/UJRN/zbnpva\\_2017\\_1\\_1\\_9](http://nbuv.gov.ua/UJRN/zbnpva_2017_1_1_9)
- 9. Dachkovskiy V.A.** Ways to Improve the Effectiveness of Recovering Weapons and Military Equipment / Dachkovskiy V.A., Sampir O.M. // Service and combat activity of the National Guard of Ukraine: current status, problems and prospects Collection of abstracts scientific and practical conf. March 14, 2019 these add. - Kharkiv, 2019 - P. 50.
- 10. Zakusilo P.S.** The method of determining the economic feasibility of carrying out routine repairs on samples of weapons and military equipment / PS Zakusylo // Weapons systems and military equipment. - 2016. - № 1. - P. 21-24. - URL: [http://nbuv.gov.ua/UJRN/soivt\\_2016\\_1\\_7](http://nbuv.gov.ua/UJRN/soivt_2016_1_7).
- 11. Morozov O.O.** Methods of determining the volume of the stock exchange of units for the repair of weapons and military equipment / OO Morozov // Military Technical Collection. - 2017. - № 16. - P. 55-59. - URL: [http://nbuv.gov.ua/UJRN/vtzb\\_2017\\_16](http://nbuv.gov.ua/UJRN/vtzb_2017_16)
- 12. Dachkovskiy V.A.** Fundamentals of the evacuation of weapons and military equipment / V.A. Dachkovskiy, IV Ovcharenko, OV Yaroshenko - K.: NGO. Ivan Chernyakhovsky, 2017. - 180 p.
- 13. Kovalenko O.A.** Evaluation of the Possibilities of Repair and Recovery Bodies for Evacuation of Damaged Weapons and Military Equipment / OA. Kovalenko, // Modern information technologies in the field of security and defense. - K., 2016. - № 2 (22). - P. 149 - 154.
- 14.** Application of units and military units of technical support / IB. Kuznetsov, OV Yaroshenko, IV Ovcharenko, V.A. Dachkovskiy, OD Yalnytsky, NK Baghdasaryan, B.T. Kuznetsov CHI: Technical Support Units: Teach. tool. - K.: NGO them. Ivan Chernyakhovsky, 2017. - 136 p.
- 15. Kuznetsov I.B.** The use of units and military units of technical support. Part II: Reconstruction and Recovery Unit: Teach. tool. / [IB Kuznetsov, OV Yaroshenko, IV Ovcharenko, V.A. Dachkovskiy]. - K.: NGO them. Ivan Chernyakhovsky, 2018. - 80 p.
- 16.** Management of the repair and restoration unit / IB Kuznetsov, S.A. Kopashynskiy, OV Yaroshenko, A.M. Tereshchenko, IV Ovcharenko, OD Yalnytsky, V.O. Dachkovskiy K.: NGO Ivan Chernyakhovsky, 2016. - 64 p..



*Анатолій Олександрович Бабарика**Національна академія Державної прикордонної служби України, Хмельницький, Україна*

## ОБГРУНТУВАННЯ ПОКАЗНИКА ВИБОРУ ОПТИМАЛЬНОГО АЛГОРИТМУ ВИДІЛЕННЯ ФОНУ У ВІДЕОПОСЛІДОВНОСТЯХ З КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ ВІДОМЧИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Виділення фону у відеопослідовностях, що отримані зі стаціонарних (нерухомих) камер відеоспостереження є важливим етапом в процесі виявлення рухомих об'єктів на цих відео послідовностях. Різноманітність підходів до вирішення задачі виділення фону у відеопослідовностях з стаціонарних (нерухомих) камер відеоспостереження створила необхідність проведення досліджень щодо вибору оптимальних алгоритмів. Такі дослідження проводяться шляхом порівняльного аналізу відомих методів та їх оцінювання за певними метриками. На основі робіт "A Benchmark Dataset for Outdoor Foreground/Background Extraction", "CDnet 2014: An Expanded Change Detection Benchmark Dataset", "Evaluation of Background Subtraction Techniques for Video Surveillance" та "Comparative study of background subtraction algorithms" нами проведено порівняльний аналіз найбільш поширених алгоритмів виділення фону. Також за результатами аналізу розміщення камер відеоспостереження розгорнутих у складі ПТС «Гарт» на визначених об'єктах та секторів їх огляду, визначено, що умови їх застосування суттєво не відрізняються від умов функціонування камер відеоспостереження, що розгортаються в громадських місцях, на вулицях, автошляхах та інших об'єктах.

В даній роботі запропоновано удосконалений показник для вибору оптимальних алгоритмів виділення фону у відеопослідовностях зі стаціонарних (нерухомих) камер систем відеоспостереження. В якості оцінних критеріїв роботи алгоритму використано такі метрики рішень класифікатора як істинно позитивно (TP – true positive), істинно негативно (TN – true negative), хибно позитивно (FP – false positive), хибно негативно (FN – false negative). Суть удосконалення полягає у розрахунку загального показника ефективності роботи алгоритму виділення фону  $W(a)$ , який відрізняється від показника, запропонованого Sobral Andrews та Vacavant Antoine в роботі "A comprehensive review of background subtraction algorithms evaluated with synthetic and real videos" використанням в якості однієї з метрик коефіцієнта кореляції Метьюса для врахування всіх можливих варіантів рішень алгоритму.

**Ключові слова:** відеоспостереження, VSS, фон, передній план, рухомі об'єкти, різниця кадрів, dataset, алгоритм, коефіцієнт кореляції Метьюса, Sobral Andrews, Vacavant Antoine.

### Вступ

**Постановка проблеми.** Виділення фону є важливим етапом в процесі виявлення рухомих об'єктів у відеопослідовності, що отримана зі стаціонарних (нерухомих) камер відеоспостереження. Різноманітність підходів до вирішення задачі виділення фону у відеопослідовностях з стаціонарних (нерухомих) камер відеоспостереження створила необхідність проведення досліджень щодо вибору оптимальних алгоритмів. Такі дослідження проводяться шляхом порівняльного аналізу відомих методів та їх оцінювання за певними метриками.

Отже, актуальним завданням є розробка показника для вибору оптимальних алгоритмів виділення фону у відеопослідовностях зі стаціонарних (нерухомих) камер систем відеоспостереження.

**Аналіз останніх досліджень і публікацій.** Питанням дослідження алгоритмів виділення фону

присвячені праці широкого кола науковців, таких як Sobral Andrews, Vacavant Antoine, Bouwmans Thierry, Babae M. та ін. [1; 2; 5; 6; 12]. У роботах зазначених авторів приділяється значна увага порівняльному аналізу відомих алгоритмів виділення фону. Проте використані результуючі показники ефективності роботи алгоритмів не в повній мірі характеризують ефективність їх роботи. Отже, вважається за доцільне продовжити дослідження зазначених вище авторів у напрямку аналізу та вдосконалення методів вибору оптимальних алгоритмів виділення фону у відеопослідовностях з камер відеоспостереження відомих систем відеоспостереження.

**Метою статті** є дослідження та вибір оптимальних алгоритмів виділення фону на відеопослідовностях з метою використання в інтелектуальних системах аналізу даних систем відеоспостереження Держприкордонслужби.

## Виклад основного матеріалу дослідження

Важливим етапом в процесі виявлення рухомих об'єктів у відеопослідовності, що отримана з стаціонарних (нерухомих) камер відеоспостереження є виділення фону (background). Загальний підхід полягає у виділенні частин на відеокадрі, які істотно відрізняються від фонові моделі, тобто створенні маски переднього

плану (foreground). Найпростішим алгоритмом виділення фону є використання відеокадру, який не містить жодного рухомого об'єкту у якості еталону. Після чого, віднімаючи фон від наступних відеокадрів, ми можемо виявляти рухомі об'єкти. Але, в реальних умовах існує низка проблем, котрі ускладнюють процес виділення фону [1] (рис. 1).



Рис. 1. Проблемні фактори, що ускладнюють процес виділення фону

Дослідження щодо вирішення задачі виділення фону у відеопослідовності розпочалися ще у 1990-х роках. На даний час існує велика кількість алгоритмів виділення фону. У найпростішому випадку, процес створення фонові моделі полягає в обчисленні абсолютної різниці між поточним кадром та попередньо визначеним статичним зображенням, яке не містить рухомих об'єктів. Такий метод має назву кадрової різниці (Frame Difference). Такий метод використовує лише один попередній кадр, отже, він не в змозі визначати рух пікселів всередині великого рівномірно рухомого об'єкта.

Для прикладу, С. Stauffer та W. E. L. Grimson в роботі [13] запропонували метод, в якому розподіл кольорів кожного пікселя представляється сумою нормальних розподілів інтенсивностей випромінювання пікселів. Пізніше цей алгоритм був удосконалений Eric Yueman and Jan-Olof Eklundh [10]. Ці алгоритми одержали назву Mixture of Gaussian (MOG). Зазначений підхід став досить поширеним завдяки тому, що здатен виділяти фонову модель при наявності таких завад як невеликі коливання освітлення сцени. Але при різних змінах освітлення чи зашумленості кадру даний алгоритм помилково визначає фонову модель. Для вирішення цих проблем вказаний тип алгоритмів продовжував вдосконалюватися багатьма науковцями [15], [16] та ін. Результатом досліджень стали удосконалені алгоритми MOG, MOG-2, GMM, GMG, TLGMM, STGMM, SKMGM, TAPPMOG тощо.

Усе різноманіття методів та алгоритмів виділення фону за використаними теоріями [1], [3], [5], [6], [9], [12] можна поділити на категорії, такі що основані на:

- базових методах та методах, що оперують середніми та дисперсійними значеннями;
- методах нечіткої логіки;
- Гаусівських процесах;
- непараметричних методах;
- використанні нейронних мереж та ін.

За результатами аналізу розміщення камер відеоспостереження на визначених об'єктах та секторів їх огляду визначено головні умови їх застосування:

- всередині приміщень та ззовні на вулиці як під накриттями так і під відкритим небом (в умовах достатнього освітлення, недостатнього освітлення та «осліплення» джерелами світла);
- ззовні на вулиці як під накриттями так і під відкритим небом
- в різних погодних умовах;
- при різних видах та інтенсивностях освітлення;
- з використанням різнотипових камер відеоспостереження;
- в різних температурних режимах.

Отже, умови функціонування камер відеоспостереження розгорнутих у складі ПТС «Гарт» суттєво не відрізняються від умов функціонування камер відеоспостереження, що розгортаються в громадських місцях, на вулицях, автошляхах та інших об'єктах. Для адекватності оцінки характеристик різних методів необхідно

здійснювати порівняльний аналіз на певних типових наборах даних. Для цього були створені такі Інтернет-ресурси як ChangeDetection.net [8], Stuttgart Artificial Background Subtraction (SABS) [14], Wallflower Test Images Sequences, BMC 2012 Background Models Challenge Dataset, SBM-RGBD 2017 Dataset, VSSN 2006 Test Images Sequences, OTCBVS 2006 Test Images Sequences, MAR - Maritime Activity Recognition Dataset, UCSD Background Subtraction Dataset та ін. [3].

Для дослідження необхідно підібрати відеопослідовності, які б містили сцени з нормальним освітленням, з недостатнім освітленням, з різкими змінами освітлення, хмарну погоду, туманну погоду, вітряну погоду, появу великих та малих рухомих об'єктів. Також кожна із вказаних сцен повинна досліджуватись при різних типах інтенсивності рухомих об'єктів.

На основі досліджень [1;6;7;9] проведемо порівняльний аналіз найбільш поширених алгоритмів виділення фону. В якості оціночних критеріїв роботи алгоритму використаємо наступні метрики рішень класифікатора: істинно позитивно (TP – true positive), істинно негативно (TN – true negative), хибно позитивно (FP – false positive), хибно негативно (FN – false negative).

Припустимо, що A – це рішення алгоритму, яка вказує на приналежність пікселя чи групи пікселів до фону (A = 1 – рухомий об'єкт, A = 0 – фон), T – це справжня приналежність пікселя чи групи пікселів до фону (T = 1 – рухомий об'єкт, T = 0 – фон). Таким чином, матрицю рішень класифікатора можна відобразити у вигляді таблиці (табл. 1).

Таблиця 1

Матриця рішень класифікатора

Справжнє значення / Відповідь алгоритму	T = 1	T = 0
A = 1	TP – вірно визначено приналежність до рухомого об'єкта	FP – помилково визначено приналежність до рухомого об'єкта
A = 0	FN – помилково визначено приналежність до фону	TN – вірно визначено приналежність до фону

Для оцінки якості роботи алгоритмів використаємо такі метрики як точність, повнота, F-міра, відсоток помилкових класифікацій (ВПК), відношення пікового сигналу до шуму (PSNR), індекс структурної подібності (SSIM) та D-score:

$$\text{Точність} = \frac{TP}{TP + FP},$$

$$\text{Повнота} = \frac{TP}{TP + FN}.$$

Показник точності характеризує долю об'єктів (пікселів чи груп пікселів), які вірно класифіковані як фонові, а показник повноти – яку долю об'єктів істинного класу із усіх об'єктів позитивного класу знайшов алгоритм. повнота демонструє здатність алгоритму знаходити даний клас, а точність – здатність відрізнити цей клас від інших класів.

Використаємо метрику F-міра, яка представляє собою спільну оцінку точності та повноти.

$$F\text{-міра} = \frac{\text{Повнота} \times \text{Точність}}{(\beta^2 \cdot \text{Точність}) + \text{Повнота}},$$

де  $\beta$  – вага точності в метриці.

Відсоток помилкових класифікацій:

$$\text{ВПК} = \frac{\text{Повнота} \times \text{Точність}}{(\beta^2 \cdot \text{точність}) + \text{повнота}}.$$

Відношення пікового сигналу до шуму (PSNR – peak signal-to-noise ratio):

$$\text{PSNR} = \frac{1}{n} \sum_{i=1}^n 10 \lg \frac{m}{\sum_{j=1}^m \|S_i(j) - G_i(j)\|^2},$$

де:  $S_i(j)$  – j-й піксель i-го зображення в послідовності S, яка має довжину n.

Індекс структурної подібності (SSIM):

$$\text{SSIM}(S, G) = \frac{1}{n} \sum_{i=1}^n \frac{(2\mu_{S_i} \mu_{G_i} + c_1)(2 \text{cov}_{S_i G_i} + c_2)}{(\mu_{S_i}^2 + \mu_{G_i}^2 + c_1)(\sigma_{S_i}^2 + \sigma_{G_i}^2 + c_1)}$$

де:  $\mu_{S_i}, \mu_{G_i}$  – середні,  $\sigma_{S_i}^2, \sigma_{G_i}^2$  – дисперсії,  $\text{cov}_{S_i G_i}$  – коваріація  $S_i$  та  $G_i$ ,  $c_1 = (k_1 L)^2$ ,  $c_2 = (k_2 L)^2$ , L – динамічний діапазон пікселів,  $k_1 = 0,01$ ,  $k_2 = 0,03$  – константи.

Метрика D-score характеризує локалізацію помилок відповідно до розміщення об'єкта:

$$D\text{-score}(S_i(j)) = \exp(-\ln(2DT(S_i(j)) - \alpha)^2),$$

де:  $\alpha$  – піковий параметр рівний 2,5,  $DT(S_i(j))$  – дистанція між пікселями ( $S_i(j)$ ) та навколишніми опорними пікселями [4].

В роботі [12], з метою комбінування показників усіх метрик запропоновано увести параметр узагальненої FSD-оцінки:

$$FSD(a) = \frac{\overline{F\text{-міра}(a)} + \overline{SSIM(a)} + (1 - \overline{D\text{-score}(a)})}{3}$$

де: a – окремий метод виділення фону,  $\overline{F\text{-міра}}, \overline{SSIM}, \overline{D\text{-score}}$  – середні значення метрик F-міра, SSIM, D-score по всьому датасету.

Але FSD метрика не враховує TN, та може дати зміщену оцінку внаслідок появи істинно невірних (TN) відповідей алгоритму.

Для врахування всіх значень матриці рішень класифікатора (див. табл. 1), запропоновано замість метрики F-міра використати коефіцієнт кореляції Метьюса (MCC – Matthews correlation coefficient) [11]:

$$MCC = \frac{TP/N - S \cdot P}{\sqrt{P \cdot S(1-S) \cdot (1-P)}},$$

де:  $N = TN + TP + FN + FP$ ;

$$S = \frac{TP + FN}{N};$$

$$P = \frac{TP + FP}{N}$$

У випадку, коли  $MCC = 1$  – модель алгоритму є ідеальною.

Отже, загальний показник ефективності роботи алгоритму виділення фону можна виразити формулою:

$$W(a) = \frac{(\overline{SSIM}(a) + (1 - \overline{D-score}(a)) + \overline{MCC}(a))}{3}$$

За результатами розрахунків експериментальних даних з результатів

дослідження [12] сформовано таблицю результатів (табл. 2) для дев'яти алгоритмів з покращеними параметрами. Проаналізувавши отримані результати (табл. 2 та рис. 2), можна зробити висновок, що запропонований загальний показник ефективності роботи алгоритму виділення фону  $W(a)$  відрізняється від показника FSD [12] тим, що  $W(a)$  враховує усі варіанти матриці рішень класифікатора, а відтак він є точнішим ніж FSD.

Таблиця 2

Результати дослідження роботи алгоритмів

№ з/п	Назва алгоритму	TP	FP	FN	TN	повнота	точність	ВПК	F – міра
1	2	3	4	5	6	7	8	9	10
1	PBAS	3541	717	76	72466	0,97899	0,83161	1,03255	0,8993
2	MultiLayerBGS	2916	369	701	72814	0,80619	0,88767	1,39323	0,8449
3	LBAdaptiveSOM	3173	438	444	72745	0,87725	0,8787	1,14844	0,8779
4	DPWrenGABGS	3488	639	129	72544	0,96434	0,84517	1	0,9008
5	MixtureOfGaussianV1BGS	2791	369	826	72814	0,77163	0,88323	1,55599	0,8236
6	AdaptiveBackground Learning	2851	396	766	72787	0,78822	0,87804	1,51302	0,8307
7	FuzzyChoquetIntegral	2234	368	1383	72815	0,61764	0,85857	2,27995	0,7184
8	T2FGMM_UM	3436	544	181	72639	0,94996	0,86332	0,94401	0,9045
9	DPEigenbackground BGS	2788	359	829	72824	0,7708	0,88592	1,54688	0,8243

Продовження таблиці 2

№ з/п	Назва алгоритму	PSNR	D – score	SSIM	FSD	MCC	W
1	2	11	12	13	14	15	16
1	PBAS	49,412	0,002	0,994	0,96377	0,97004	0,98735
2	MultiLayerBGS	49,398	0,001	0,993	0,94566	0,85287	0,94829
3	LBAdaptiveSOM	50,553	0,001	0,992	0,95632	0,89115	0,96072
4	DPWrenGABGS	51,394	0,001	0,993	0,96428	0,95672	0,98291
5	MixtureOfGaussianV1BGS	51,107	0,001	0,993	0,93856	0,83805	0,94335
6	AdaptiveBackground Learning	50,684	0,002	0,993	0,94057	0,84596	0,94565
7	FuzzyChoquetIntegral	50,366	0,001	0,992	0,90315	0,78303	0,92468
8	T2FGMM_UM	51,792	0,002	0,992	0,96486	0,94321	0,97774
9	DPEigenbackgroundBGS	32,843	0,011	0,891	0,90145	0,83737	0,90579

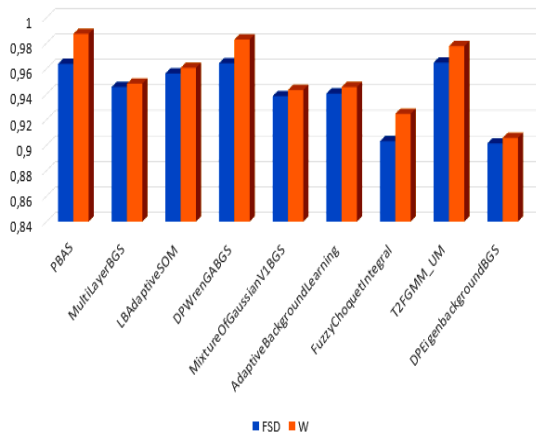


Рис. 2. Порівняльна характеристика алгоритмів за параметрами FSD та W

Структурно-логічну схему проведення дослідження зображено на рисунку 3.



Рис. 3. Структурно-логічна схема проведення дослідження з використанням запропонованого показника W

### Висновки і перспективи подальших досліджень

В роботі проведено дослідження найпоширеніших алгоритмів виділення фону у відеопослідовностях, методів порівняльного

аналізу та кількісних характеристик для вибору оптимальних алгоритмів виділення фону. В результаті проведеного дослідження запропоновано загальний показник ефективності роботи алгоритму виділення фону на відеопослідовностях, що отримані зі стаціонарних камер відеоспостереження в системах відеоспостереження. Вказаний показник є удосконаленим показником, запропонованим в

роботі [12] за рахунок введення метрик, які характеризують усі варіанти відповідей класифікатора. Адекватність показника підтверджено шляхом перевірки експериментального дослідження. Напрямоком подальших досліджень є програмна реалізація результатів дослідження у системах відеоспостереження Держприкордонслужби України.

### Література

**1. A. Benchmark.** Dataset for Outdoor Foreground/Background Extraction. *Computer Vision - ACCV 2012 Workshops: ACCV 2012 International Workshops. Part I.* / Antoine Vacavant, Thierry Chateau, Alexis Wilhelm, Laurent Lequière. Daejeon, Korea, 2012. С. 291–300. **2. Babae M.,** Dinh D.T., Rigoll G. A deep convolutional neural network for video sequence background subtraction. *Pattern Recognition.* Elsevier, 2018. Вип. 76. С. 635–649. URL : <https://doi.org/10.1016/j.patcog.2017.09.040>. (дата звернення : 16.01.2019). **3.** Background Subtraction Website. веб-сайт. URL : <https://sites.google.com/site/backgroundsubtraction/test-sequences/human-activities> (дата звернення: 25.12.2018). **4.** Borgefors G. Distance Transformations in digital images. *Computer Vision, Graphics, and Image Processing.* 1986. Вип. 34. С. 344–371. URL : <https://www.sciencedirect.com/science/article/pii/S0734189X86800470?via%3Dihub>. (дата звернення : 22.01.2019). **5. Bouwmans T.** Traditional and recent approaches in background modeling for foreground detection: An overview. *Computer Science Review.* Elsevier, 2014. № 11. С. 31–66. URL: <https://doi.org/10.1016/j.cosrev.2014.04.001>. (дата звернення : 20.01.2019). **6. Brutzer S., Hoferlin B., Heidemann G.** Evaluation of Background Subtraction Techniques for VideoSurveillance. In *Proceedings of the 24th IEEE Conference on Computer Vision and Pattern Recognition.* Colorado Springs, CO, USA, 2011. С. 1937–1944. **7.** CDnet 2014: An Expanded Change Detection Benchmark Dataset. *2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops.* / Wang Yi та ін. Columbus, OH, 2014. С. 393–400. **8.** ChangeDetection.NET (CDNET). веб-сайт. URL : <http://www.changedetection.net> (дата звернення: 25.12.2018). **9.** Comparative study of background subtraction algorithms. *Journal of Electronic Imaging.* / Yannick Benezeth, Pierre-Marc Jodoin, Bruno Emile, Hélène Laurent, Christophe Rosenberger. 2010. № 19 (3). URL : <https://doi.org/10.1117/1.3456695>. (дата звернення :

20.01.2019). **10.** Hayman Eric, Eklundh Jan-Olof. Statistical background subtraction for a mobile observer. *Proceedings Ninth IEEE International Conference on Computer Vision.* Nice, France : IEEE, 2003. С. 67–74. URL : <https://ieeexplore.ieee.org/document/1238315>. (дата звернення : 01.11.2019). **11. Matthews B.W.** Comparison of the predicted and observed secondary structure of T4 phage lysozyme. *Biochimica et Biophysica Acta (BBA)-Protein Structure.* Elsevier, 1975. № 405 (2). С. 442–451. **12.** Sobral Andrews, Vacavant Antoine. A comprehensive review of background subtraction algorithms evaluated with synthetic and real videos. *Computer Vision and Image Understanding.* 2014. Вип. 122. С. 4–21. URL : <https://doi.org/10.1016/j.cviu.2013.12.005>. (дата звернення: 22.01.2019). **13. Stauffer C.,** Grimson W. E. L. Adaptive background mixture models for real-time tracking. *Computer Society Conference on Computer Vision and Pattern Recognition* : 1999 Conference on Computer Vision and Pattern Recognition (CVPR '99). Ft. Collins, CO, USA : IEEE Computer Society, 1999. С. 2246–2252. URL : <https://dblp.uni-trier.de/db/conf/cvpr/cvpr1999.html>. (дата звернення : 16.01.2019). **14.** Stuttgart Artificial Background Subtraction Dataset. *Institute for Visualisation and Interactive Systems (VIS)* : веб-сайт. URL : [https://www.vis.uni-stuttgart.de/forschung/visual\\_analytics/visuelle\\_analyse\\_vid\\_eostroeme/stuttgart\\_artificial\\_background\\_subtraction\\_datas\\_et/index.en.html](https://www.vis.uni-stuttgart.de/forschung/visual_analytics/visuelle_analyse_vid_eostroeme/stuttgart_artificial_background_subtraction_datas_et/index.en.html) (дата звернення: 25.12.2018). **15. Zivkovic Z.,** F. van der Heijden. Efficient adaptive density estimation per image pixel for the task of background subtraction. *Pattern Recognition Letters.* 2006. № 27. С. 773–780. URL : <https://doi.org/10.1016/j.patrec.2005.11.005>. (дата звернення : 30.12.2018). **16. Zivkovic Z.** Improved Adaptive Gaussian Mixture Model for Background Subtraction. *Proceedings of the 17th International Conference on Pattern Recognition.* Cambridge, UK : IEEE, 2004. Вип. 2. С. 28–31.

## ОБОСНОВАНИЕ ПОКАЗАТЕЛЯ ВЫБОРА ОПТИМАЛЬНОГО АЛГОРИТМА ВЫДЕЛЕНИЯ ФОНА НА ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЯХ С КАМЕР ВИДЕОНАБЛЮДЕНИЯ ВЕДОМСТВЕННЫХ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

Бабарика Анатолий Александрович

Национальная академия Государственной пограничной службы, Хмельницкий, Украина

Выделение фона на видеопоследовательностях, полученных со стационарных (неподвижных) камер видеонаблюдения является важным этапом в процессе обнаружения движущихся объектов на этих видеопоследовательностях. Разнообразие подходов к решению задачи выделения фона в видеопоследовательностях со стационарных (неподвижных) камер видеонаблюдения обусловило необходимость проведения исследований по выбору оптимальных алгоритмов. Такие исследования проводятся путем сравнительного анализа известных методов и их оценки по определенным метрикам. На основе работ "A Benchmark Dataset for Outdoor Foreground / Background Extraction", "CDnet 2014: An Expanded Change Detection Benchmark Dataset", "Evaluation of Background Subtraction Techniques for VideoSurveillance" и "Comparative study of background subtraction algorithms" нами проведен сравнительный анализ наиболее распространенных алгоритмов выделения фона. Также по результатам

анализа размещения камер видеонаблюдения развернутых в составе ИИТС «Гарт» на определенных объектах и секторов их осмотра, определено, что условия их применения существенно не отличаются от условий функционирования камер видеонаблюдения, которые разворачиваются в общественных местах, на улицах, дорогах и других объектах.

В данной работе предложен усовершенствованный показатель выбора оптимальных алгоритмов выделения фона в видеопоследовательности со стационарных (неподвижных) камер систем видеонаблюдения. В качестве оценочных критериев работы алгоритма использованы следующие метрики решений классификатора как истинноположительно (TP - true positive), истинноотрицательно (TN - true negative), ложноположительно (FP - false positive), ложноотрицательно (FN - false negative). Суть усовершенствования заключается в расчете общего показателя эффективности работы алгоритма выделения фона, который отличается от показателя, предложенного Sobral Andrews и Vacavant Antoine в работе "A comprehensive review of background subtraction algorithms evaluated with synthetic and real videos" использованием в качестве одной из метрик коэффициента корреляции Мэтьюса для учета всех возможных вариантов решений алгоритма. Адекватность усовершенствованного показателя подтверждена путем проведения экспериментального исследования. Направлением дальнейших исследований является программная реализация метода в системах видеонаблюдения Госпогранслужбы Украины.

**Ключевые слова:** видеонаблюдение, VSS, фон, передний план, подвижные объекты, разница кадров, датасет, алгоритм, коэффициент корреляции Мэтьюса, Sobral Andrews, Vacavant Antoine.

### THE JUSTIFICATION OF OPTIMAL ALGORITHMS INDEX CHOICE FOR THE BACKGROUND SUBTRACTION IN VIDEO SEQUENCES DERIVED FROM STATIONARY CAMERAS OF VIDEO SURVEILLANCE SYSTEMS

*Anatolii Babaryka*

*The National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine*

*The background subtraction is an important stage in the process of detecting moving objects in video sequences derived from stationary cameras of video surveillance systems (VSS cameras). A variety of approaches to addressing the background selection problem in video sequences from stationary cameras of video surveillance systems has created the need for research on the choice of optimal algorithms.*

*In this paper, we described the problem factors that complicate the background allocation process and described the basic background subtraction algorithms classifications.*

*After analyzing the location of VSS cameras for certain objects within the Information and Telecommunication Systems of the State Border Guard Service and their inspection sectors, we have identified the features of the use of cameras from these systems.*

*We researched the most common algorithms of background subtraction in video sequences, methods of comparative analysis and methods for selecting optimal background subtraction algorithms in video sequences from stationary VSS cameras.*

*We developed an improved efficiency index for the choice optimal algorithms for the background subtraction in video sequences derived from stationary cameras of video surveillance systems on the basis method proposed Sobral Andrews and Vacavant Antoine in the "Comprehensive review of subtraction algorithms evaluated using synthetic and real video".*

*The essence of the improved method is that we propose to calculate the overall performance of the background subtraction algorithm using Matthews correlation coefficient, because this coefficient takes into account all possible variants of the matrix of algorithm responses (TP, TN, FP, FN).*

*The proposed method was tested by calculating the results of the experimental study in the "A comprehensive review of the subtraction algorithms evaluated using synthetic and real videos".*

*As a result, we have developed the index of efficiency of an algorithm of background subtraction, that differs from that offered gathered Sobral Andrews and Vacavant Antoine (FSD), because it takes into account all options matrix classifier responses, and therefore is more accurate than the FSD.*

**Keywords:** video surveillance, VSS, background, foreground, moving objects, frame difference, MOG, dataset, algorithm, Matthews correlation coefficient, Sobral Andrews, Vacavant Antoine.

*Ігор Борисович Кузнецов (кандидат технічних наук, доцент)*

*Андрій Олександрович Дядечко*

*Вадим Тадеушович Марценківський (кандидат технічних наук, доцент)*

*Національний університет оборони України імені Івана Черняхівського, Київ, Україна*

## АЛГОРИТМ КОНТРОЛЮ ПАРАМЕТРІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ ДЛЯ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНОЇ СИСТЕМИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

*Здійснення контролю за технічним станом озброєння та військової техніки, попередження передчасного виходу її з ладу та запобігання виникненню прихованих відмов в роботі апаратури є запорукою підтримання зразків озброєння, бойової та іншої техніки в постійній готовності до застосування за призначенням.*

*Уніфікація засобів контролю параметрів озброєння та військової техніки дозволить вирішити ряд суттєвих проблем які пов'язані з виготовленням, модернізацією та експлуатацією зразків озброєння та військової техніки, забезпечить своєчасне прийняття правильних рішень щодо технічного стану та необхідності здійснення технічного чи метрологічного обслуговування озброєння та військової техніки.*

*В статті запропонована узагальнена структура уніфікованої інформаційно-виміральної системи для контролю параметрів озброєння та військової техніки, а також обґрунтовано алгоритм контролю параметрів для неї із апостеріорною оцінкою достовірності контролю, використання якого дозволить виключити помилки 1-го і 2-го роду в ході проведення контролю параметрів озброєння та військової техніки та під час прийняття рішення щодо технічного стану конкретного зразка озброєння.*

***Ключові слова:** інформаційно-виміральною системою, озброєння та військова техніка, контроль параметрів ОВТ, достовірність контролю.*

### Вступ

Практично визначити реальний технічний стан зразка озброєння та військової техніки (ОВТ), готовність його до застосування за призначенням дозволяє контроль його параметрів, які в процесі експлуатації під впливом різних факторів, часу і режимів експлуатації можуть змінювати свої значення.

Впровадження стандартів НАТО в сфері оборони вимагає від нас здійснення певних кроків щодо модернізації існуючих та виготовлення нових зразків ОВТ, а також засобів її технічного обслуговування до яких відносяться виміральної прилади, системи та комплекси за допомогою яких здійснюється контроль параметрів ОВТ. Поряд з тим удосконалення потребують й способи здійснення контролю параметрів ОВТ, які б відповідали сучасним вимогам. В [1] передбачено створення нових та модернізацію існуючих засобів контролю параметрів ОВТ. Для цього необхідно врахувати необхідність уніфікації засобів та способів контролю для забезпечення можливості використання їх для контролю параметрів різноманітних типів ОВТ.

**Постановка проблеми.** Сучасний стан засобів контролю параметрів ОВТ, зокрема, бортового обладнання літаків, вертольотів, наземних систем управління зенітних ракетних комплексів тощо, характеризується застосуванням великого різноманіття вузькоспеціалізованого обладнання, експлуатаційно-ремонтних пультів, які додаються практично до кожного конкретного виробу, використанням засобів виміральної техніки військового призначення (ЗВТВП). Існуючі автоматизовані засоби контролю параметрів ОВТ також створювались окремо для конкретного типу або зразка.

Тому актуальною задачею є забезпечення ОВТ сучасними ефективними засобами контролю та побудова уніфікованої інформаційно-виміральної системи військового призначення (ІВС ВП), яка відповідатиме вимогам якісного контролю параметрів ОВТ.

**Аналіз останніх досліджень і публікацій.** З розвитком інформаційних технологій досить великої актуальності набули питання автоматизованого контролю технічного стану

ОВТ.

Так, наприклад, в [5] розглядаються питання автоматизованого контролю технічного стану для можливості інтеграції зразків ОВТ, які знаходяться на озброєнні у Збройних Силах (ЗС) України, у середовище інтегрованої логістичної підтримки.

Разом з тим в [6, 7] автори досліджують показники точності засобів контролю в складі ІВС ВП та їх вплив на результати автоматизованого контролю параметрів ОВТ.

Питанням достовірності контролю параметрів приділяється увага лише в [3] де автор проводить аналіз алгоритмів контролю параметрів, проте не досліджується можливість застосування тих чи інших алгоритмів в ІВС ВП.

В проаналізованих джерелах не розглянуті структура та склад ІВС ВП.

**Метою статті є** окреслення складових частин ІВС ВП та обґрунтування алгоритму контролю параметрів ОВТ для неї.

### Виклад основного матеріалу дослідження

Інформаційно-вимірювальна система – це сукупність функціонально об'єднаних засобів вимірювань різних фізичних величин, обчислювальних та інших допоміжних технічних засобів, призначена для отримання вимірювальної та іншої інформації про досліджуваний об'єкт в умовах його функціонування або зберігання, її перетворення і обробки з метою представлення

споживачеві в необхідному вигляді [2]. ІВС ВП використовуються для оцінки технічного стану зразків ОВТ та прийняття відповідного рішення щодо необхідності проведення їх технічного (метрологічного) обслуговування чи ремонту. Сучасні зразки ОВТ представляють собою складні вироби, виробництво, а особливо експлуатація яких потребує великих матеріальних витрат та суттєво залежить від засобів контролю, які знаходяться у військових частинах, ремонтних органах та на заводах виробниках.

За оцінкою вітчизняних та зарубіжних фахівців трудомісткість контрольних операцій при виробництві складного радіоелектронного обладнання складає понад 30% [4]. Також й під час експлуатації ОВТ для підтримання його працездатності й боєготовності необхідно проводити великий обсяг робіт щодо контролю технічного стану. Відсутність одноманітності способів й засобів контролю параметрів на всіх стадіях життєвого циклу ОВТ створює серйозні труднощі при його експлуатації та ремонті. Застосування ІВС ВП може дозволити значно знизити вартість експлуатації, в декілька разів зменшити трудомісткість контрольних-вимірювальних операцій при виробництві ОВТ.

Загальна структура ІВС ВП, що пропонується показана на рис. 1

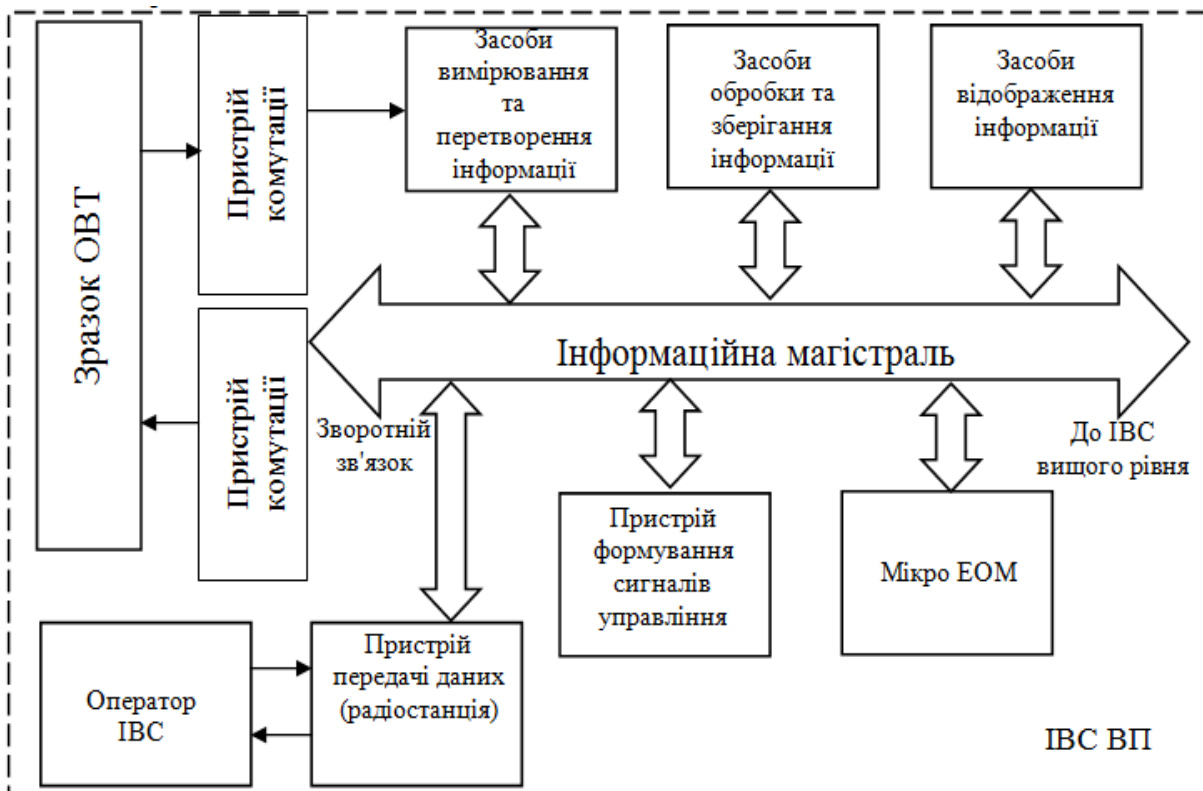


Рис. 1. Узагальнена структура ІВС ВП, що пропонується



Для зразків ОВТ вибір необхідної точності вимірювання параметрів є одним з найважливіших завдань. Це обумовлено тим, що від його вирішення залежать показники ефективності контролю – інформативність, оперативність і економічність. Однією з вимог побудови ІВС ВП є задана точність вимірювання параметрів ОВТ із визначеною достовірністю контролю.

Для ІВС ВП доцільно використовувати алгоритм контролю параметрів ОВТ з апостеріорною оцінкою достовірності контролю [3]. Це в свою чергу забезпечить прийняття правильного рішення щодо придатності зразка ОВТ до застосування за призначенням з високою імовірністю, тобто якщо всі параметри знаходяться в межах допуску і ймовірність невиявленої відмови  $R_{пв}$  не більше допустимої, то зразок ОВТ є придатним до застосування за призначенням; якщо хоча б один параметр зразка ОВТ вийшов за межі свого допуску і ймовірність помилкової відмови  $R_{пв}$  не більше допустимої, то зразок ОВТ є непридатним до застосування за призначенням.

Залежності апостеріорної ймовірності помилкової (1-го роду)  $\alpha$  і невиявленої (2-го роду)  $\beta$  відмов від імовірності помилок контролю першого  $\alpha_i$  і другого  $\beta_i$  роду за  $i$ -м параметром визначаються зі співвідношень

$$\alpha = 1 - \prod_{i=1}^N (1 - \alpha_i) \quad (1)$$

$$\beta = \frac{\prod_{i=1}^N [P_{ci}(1 - \alpha_i - \beta_i) + \beta_i] - \prod_{i=1}^N (1 - \bar{P}_{ci})(1 - \alpha_i)}{1 - \prod_{i=1}^N (1 - \bar{P}_{ci})} \quad (2)$$

де:  $\alpha_i = R_{пв} / P_c$  ;

$\beta_i = R_{пв} / (1 - P_c)$  ;

$\bar{P}_{ci}$  – ймовірність того, що виміряне значення  $i$ -го параметру ОВТ знаходиться поза межами допуску;

$P_c = \prod_{i=1}^N P_{ci}$  – ймовірність того, що виміряні

значення всіх контрольованих параметрів знаходяться в межах допуску;

$\bar{P}_c = \prod_{i=1}^N \bar{P}_{ci} = 1 - P_c$  – ймовірність того, що

виміряне значення хоча б одного контрольованого параметру знаходиться поза межами допуску.

Аналіз співвідношення (2) показує, що другий доданок чисельника є рівним нулю, якщо хоча б один контрольований параметр знаходиться за межами свого допуску, тобто  $\bar{P}_{ci} = 1$ . Знаменник у цьому випадку дорівнює одиниці. Якщо всі виміряні контрольовані параметри знаходяться в

межах допусків, то при контролі можлива тільки помилка контролю першого роду, і її визначають за формулою (1). Якщо виміряне значення хоча б одного контрольованого параметру знаходиться за межами допуску, то при контролі можлива помилка контролю другого роду, і її визначають за співвідношенням (2).

За допустимими значеннями апостеріорної ймовірності помилок контролю першого  $\alpha^\partial = R_{пв}^\partial / P_c$  і другого  $\beta^\partial = R_{пв}^\partial / \bar{P}_c$  роду визначимо вимоги до показників достовірності контролю кожного параметру ОВТ

$$1 - \prod_{i=1}^N (1 - \alpha_i) \leq \alpha^\partial$$

$$\frac{\prod_{i=1}^N [P_{ci}(1 - \alpha_i - \beta_i) + \beta_i] - \prod_{i=1}^N (1 - \bar{P}_{ci})(1 - \alpha_i)}{1 - \prod_{i=1}^N (1 - \bar{P}_{ci})} \leq \beta^\partial$$

При використанні апостеріорної оцінки достовірності результату контролю граничні значення помилок контролю за кожним параметром ОВТ є рівними допустимій ймовірності помилкової та невиявленої відмов зразка ОВТ в цілому:  $\alpha_i^\partial = \alpha^\partial$ ;  $\beta_i^\partial = \beta^\partial$ .

Це можна пояснити наступним чином: відповідно до формули (1) ймовірність помилки контролю першого роду не може перевищувати ймовірність помилкової відмови за кожним параметром, оцінка ймовірності невиявленої відмови (2) у процесі контролю дозволяє не вводити жорсткіші обмеження на ймовірність невиявленої відмови за кожним параметром, ніж на ймовірність такої відмови зразка ОВТ в цілому. Граничні значення похибки вимірювання кожного параметру, допуску на ці параметри, а отже, і необхідна точність вимірювального контролю, визначається за допомогою розв'язання системи рівнянь

$$\begin{cases} \alpha^\partial = \int_{-d_i}^{d_i} \phi(x_i) \left[ \int_{-\infty}^{-d_i-x_i} \phi(\Delta_i) d\Delta_i + \int_{d_i-x_i}^{\infty} \phi(\Delta_i) d\Delta_i \right] dx_i \\ \beta^\partial = \int_{-\infty}^{-d_i} \phi(x_i) \int_{d_i-x_i}^{-d_i-x_i} \phi(\Delta_i) d\Delta_i dx_i + \\ + \int_{d_i}^{\infty} \phi(y_i) \int_{-d_i-x_i}^{d_i-x_i} \phi(\Delta_i) d\Delta_i dx_i \end{cases} \quad (3)$$

де:  $\phi(x_i)$  – функція розподілу щільності ймовірності контрольованих параметрів ОВТ;

$\phi(\Delta_i)$  – функція розподілу похибки вимірювань контрольованих параметрів ОВТ;

$d_i$  – значення симетричного допуску на  $i$ -й

параметр,  $i = 1, N$ ;

$x_i, y_i$  – виміряні значення параметрів ОВТ.

Із системи рівнянь (3) можна визначити значення контрольного допуску  $i$  середнє квадратичне відхилення похибки вимірювання кожного контрольованого параметра зразка ОВТ. Математичне очікування похибки вимірювання приймається рівним нулю, тобто передбачається введення поправки на систематичну складову похибки.

Таким чином, алгоритм контролю параметрів ОВТ з апостеріорною оцінкою достовірності контролю має наступні переваги:

необхідна точність вимірювання параметрів контролю не залежить від їх загальної кількості;

забезпечується необхідна достовірність контролю кожного параметра;

відсутність інформації про закони розподілу контрольованих параметрів практично не впливає на необхідну точність вимірювань.

Блок-схема запропонованого алгоритму контролю параметрів зразка ОВТ представлена на рис.2.



Рис. 2. Блок-схема алгоритму контролю параметрів ОВТ, що пропонується.

Алгоритм контролю параметрів ОВТ визначає множину контрольованих параметрів, послідовність їх вимірювання й обробки результатів вимірювань. При здійсненні контролю параметрів зразка ОВТ для досягнення високої достовірності контролю передбачається багаторазове вимірювання контрольованих параметрів або зміна методу виконання вимірювання.

Оцінка стану параметрів ОВТ, значення яких

вимірюється, виконується шляхом порівняння їх можливих значень з допустимими межами відхилень, які встановлені для цих параметрів. Інформація про стан параметрів обробляється в ІВС ВП для прийняття рішення про технічний стан зразка ОВТ та про необхідність здійснення його технічного та метрологічного обслуговування.

Технічний стан ОВТ визначається за великою кількістю параметрів контролю, еталонні значення і допустимі межі відхилення яких вносяться в базу

даних про параметри зразка ОВТ яка в свою чергу інтегрується в ІВС ВП. Якщо хоча б один з параметрів зразка ОВТ не відповідає еталонному значенню в базі даних (тобто знаходиться за межами допустимих значень), то зразок ОВТ визнається непридатним до застосування. процесі аналізу параметрів контролю ОВТ може бути отримана інформація про очікуваний розвиток існуючих або майбутніх відмов. Уся отримана вимірювальна інформація фіксується, аналізується для прийняття рішення щодо необхідності проведення технічного та метрологічного обслуговування та накопичується для отримання статистичних даних про несправності та дрейфу параметрів конкретного зразка або групи зразків ОВТ.

### Література

1. Державна програма розвитку Збройних Сил України на період до 2020 року. 2. ДСТУ 2681-94 Державний стандарт України. Метрологія. Терміни та визначення. 3. Стаднік В.В. Аналіз алгоритмів вимірювального контролю параметрів складної технічної системи: Науковий журнал "Автомобильный транспорт". 2012. № 30. С. 83–86. 4. Васильков В.Г. Організація і управління процесами виробництва. / В.Г.Васильков, Н.В.Василькова. // Навчальний посібник. – Київ: КНЕУ, 2011. – 503 с. 5. Воїнов В.В. Автоматизований контроль технічного стану зразка ОВТ, як одна з умов інтеграції до середовища CALS. / В.В.Воїнов, М.Б.Бровко,

### Висновки й перспективи подальших досліджень

Таким чином, використання ІВС ВП та запропонованого алгоритму контролю параметрів ОВТ в ній дасть змогу усунути недоліки пов'язані зі складностями прийняття рішення про стан зразка ОВТ за великих імовірностей помилок та необхідністю виконання обчислень в процесі контролю, здійснювати контроль параметрів ОВТ з високою точністю вимірювань та високою достовірністю контролю, дозволить виконувати управління вимірюваннями параметрів, що контролюються (визначення розвитку можливих несправностей), контроль, відображення результатів контролю, тестування та управління технічним та метрологічним обслуговуванням.

Д.М.Запара. // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – № 1 (18). – С. 178-181. 6. Прибілєв Ю.Б. Метрологічна надійність інформаційно-вимірювальних систем військового призначення: Сучасні інформаційні технології у сфері безпеки та оборони. 2014. № 3 (21). С. 27-30. 7. Скопінцев О.О. Вплив контролю технічного стану озброєння та військової техніки на їх бойову готовність. / О.О.Скопінцев, Г.В.Рибалка, С.М. Швидков. // Збірник наукових праць Харківського університету Повітряних Сил. – 2016. - № 3 (48). – с. 30-33.

## АЛГОРИТМ КОНТРОЛЯ ПАРАМЕТРОВ ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ ДЛЯ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ ВОЕННОГО НАЗНАЧЕНИЯ

*Игорь Борисович Кузнецов (кандидат технических наук, доцент)*

*Андрей Александрович Дядечко*

*Вадим Тадеушевич Марценкиевский (кандидат технических наук, доцент)*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*Осуществление контроля за техническим состоянием ВВТ, предупреждения преждевременного выхода ее из строя и предотвращения возникновения скрытых отказов в работе аппаратуры является залогом поддержания образцов ВВТ в постоянной готовности к применению по назначению.*

*Унификация средств контроля параметров ВВТ позволит решить ряд существенных проблем, которые связаны с изготовлением, модернизацией и эксплуатацией образцов ВВТ, обеспечит своевременное принятие правильных решений относительно технического состояния и необходимости осуществления технического или метрологического обслуживания ВВТ.*

*В статье предложена обобщенная структура унифицированной информационно-измерительной системы для контроля параметров ВВТ, а также обоснованно алгоритм контроля параметров для нее с апостериорной оценкой достоверности контроля, использование которого позволит исключить ошибки 1-го и 2-го рода в ходе проведения контроля параметров ВВТ и при принятии решения относительно технического состояния конкретного образца вооружения.*

*Ключевые слова: информационно-измерительная система, вооружение и военная техника, контроль параметров ВВТ, достоверность контроля.*

## ALGORITHM FOR CONTROLLING THE PARAMETERS OF ARMS AND ARMAMENT FOR THE MILITARY INFORMATION-MEASURING SYSTEM

*Igor Kuznetsov (Candidate of Technical Sciences, Associate Professor)*

*Andrii Diadechko*

*Vadym Martsenkivskii (Candidate of Technical Sciences, Associate Professor)*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*Controlling the technical condition of weapons and military equipment, preventing its early failure and preventing the occurrence of hidden failures in the equipment is a key to maintaining samples of weapons, military and other equipment in constant readiness for its intended use.*

*The unification of the control parameters of weapons and military equipment will solve a number of significant problems related to the manufacture, modernization and operation of samples of weapons and military equipment, ensure timely decision-making about the technical condition and the need for technical or metrological maintenance of weapons and military equipment.*

*The article presents a generalized structure of a unified information-measuring system for controlling the parameters of weapons and military equipment, as well as the algorithm of parameter control for it with a posteriori estimation of the reliability of control, which will allow to eliminate errors of the 1st and 2nd kind during the control of parameters weapons and military equipment and when deciding on the technical condition of a specific weapon model.*

**Keywords:** *information-measuring system, armament and military equipment, control of parameters, reliability of control.*

### **References**

1. Derzhavna programa rozvytku Zbrojnyh Syl Ukrainy na period do 2020 roku. **2. DSTU 2681-94** Derzhavnyi Standart Ukrainy. Metrologija. Terminy ta vyznachennia.
3. **Stadnik V.V.** Analysis of algorithms for measuring control parameters of complex technical system. [Naukovii zhurnal "Avtomobilnyi transport"]. 2012. № 30. p. 83-86.
4. **Vasytkov V.G.** Organization and management of production processes. / V.G.Vasytkov, N.V.Vasytkova. // [Navchalnyi posibnyk.] – Kyiv: KNEU, 2011. – 503 p.
5. **Vojinov V.V.** Automated control of the technical condition of the sample of weapons and military equipment as one of the conditions for integration into the CALS environment. / V.V.Vojinov, M.B.Brovko, D.M. Zapara. // [Nauka i tehnika Povitrianyh Syl Zbrojnyh Syl Ukrainy.] – 2015. - №1 (18). – p. 178-181.
6. **Pribylev Yu.B.** Metrological reliability of military information and measurement systems: [Suchasni informatsijni tehnologiji u sferi bezpeky ta oborony.] 2014. №3 (21). p. 27-30.
7. **Skopintsev O.O.** The influence of control of the technical condition of weapons and military equipment on their combat readiness. / O.O. Skopintsev, G.V.Rybalka, S.M.Shvydkov. // [Zbirnyk naukovyh prats Harkivskogo universytetu Povitrianyh Syl.] – 2016. - №3 (48). – p. 30-33.

*Григорій Митрофанович Тіхонов (кандидат військових наук, с.н.с.)*

*Володимир Іванович Баталюк*

*Віталій Миколайович Безуглий*

*Національний університет оборони України імені Івана Черняхівського, Київ, Україна*

## ПІДГОТОВКА АПАРАТУ КЕРІВНИЦТВА ДО КОМАНДНО-ШТАБНОГО НАВЧАННЯ З ВИКОРИСТАННЯМ ЗАСОБІВ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

*В статті розглядаються сучасний процес організації роботи апарату керівництва та посередників в ході підготовки та проведення командно-штабних навчань з застосуванням сучасних засобів автоматизації та імітаційного моделювання бойових дій, надано повний перелік документів, що відпрацьовуються апаратом керівництва відмінності в роботі штабу керівництва на етапі планування навчання. Визначено особливості роботи штабу керівництва в період планування навчань та особливості у структурі апарату керівництва і посередників для проведення саме такого навчання. Розглядаються теоретичні положень та практичних рекомендацій щодо впровадження та удосконалення підготовки органів військового управління Збройних Силах України. Окреслено основні завдання групи застосування засобів автоматизації управління військами та групи імітаційного моделювання бойових дій. Визначено необхідність залучення до них представників інших військових формувань, що входять до складу сил оборони з метою відпрацювання заходи спрямованих на досягнення взаємодії спрямованих на набуття індивідуальних спроможностей щодо спільного виконувати завдання.*

*Запропоновано рекомендації з практичних питань підготовки апарату керівництва до командно-штабних навчань з використанням засобів автоматизації та імітаційного моделювання бойових дій JCATS, а також автоматизованої системи управління військами "Славутич".*

**Ключові слова:** *командно-штабне навчання, апарат керівництва, засоби автоматизації та імітаційного моделювання.*

### Вступ

Великої уваги керівництвом Збройних Сил України (далі – ЗС) приділяється підготовці органів військового управління (далі – ОВУ), військовим частинам та спільній підготовці ЗС і інших військових формувань (далі – ІВФ) під час проведення командно - штабних навчань (далі – КШН), особливостям роботи апарату керівництва під час підготовки та проведення КШН з використанням засобів автоматизації та імітаційного моделювання бойових дій.

На перший погляд це просте навчання, однак підготовка його потребує тривалого часу та залучення висококваліфікованих фахівців автоматизованих систем управління та засобів імітаційного моделювання бойових дій.

При плануванні саме таких КШН, у керівника та офіцерів штабу керівництва можуть виникнути певні труднощі пов'язані з відсутністю необхідної начально-методичної літератури.

**Постановка проблеми.** Аналіз сучасного стану виконання бойових завдань яскраво показує, що покращення якості виконання завдань військовими організаційними структурами спирається на рівень їх підготовки та його спроможність швидко та достатньо обґрунтовано здійснювати планування бойових дій. Своєчасне

та якісне вирішення проблеми вимагає мати навчений персонал ОВУ в необхідному місці і в необхідний час, що саме і буде сприяти підвищенню ефективній роботі військової організаційної структури.

**Аналіз останніх досліджень і публікацій.** В останній період проведення АТО та ООС постала гостро проблема підготовки кваліфікованих військових кадрів ОВУ, які забезпечать якісне планування бойових дій та управління військами (силами) вході їх ведення. Разом з тим в початковий період проведення бойових дій, а також і у подальшому вказує на низький рівень взаємодії сил сектору безпеки і оборони при спільному виконанні завдань, внаслідок попередніх помилок виправлення яких можливо за рахунок колективної підготовки ОВУ направлених на буття спроможностей щодо планування бойових дій міжвідомчих угруповань [6].

Внаслідок цього шляхи підвищення якості управлінської діяльності залежить від рівня навченості ОВУ.

**Метою статі** є розгляд теоретичних положень та надання практичних рекомендацій щодо впровадження та удосконалення підготовки ОВУ Збройних Силах України.

**Виклад основного матеріалу дослідження**

Методика роботи керівника та штабу керівництва при підготовці та проведенні КШН всіх видів мало чим відрізняються. Однак, в підготовці кожного виду КШН є свої особливості.

Для допомоги апарату керівництва в підготовці до таких навчань необхідними і важливими

документами будуть два посібники.

Планування навчання з використанням засобів автоматизації та імітаційного моделювання, на наш погляд, повинно починатися на пізніше, ніж за 60 діб до його початку. Для його проведення повинні бути відпрацьовані навчально-методичні, організаційні, бойові та документи із забезпечення КШН, які викладені на рис. 1.



Рис. 1 Основні документи для підготовки і проведення КШН.

Відмінністю в роботі штабу керівництва на етапі планування навчання є те, що він, додатково розробляє базу даних сил і засобів та місцевості для введення в засіб імітаційного моделювання бойових дій та формує базу даних автоматизованої системи управління військами та змінні вихідні дані для інформаційно-розрахункових задач.

Особливістю у структурі апарату керівництва та посередників для проведення такого навчання є те, що окрім основних посадових осіб – керівника, начальника штабу керівництва, заступників та помічників керівника і начальника штабу керівництва КШН, до його складу включені помічники керівника навчання з використання засобів автоматизації управління військами та з використання засобів імітаційного моделювання бойових дій.

Посередниками призначаються особи (офіцери, службовці, працівники ЗС України), що мають відповідну освіту, досвід роботи в органах військового управління (далі – ОВУ) (військах) і необхідні навички в роботі на засобах автоматизації та імітаційного моделювання.

Безумовно, посередників, які б могли працювати на об'єднаному імітаторі конфліктних і тактичних ситуацій, сьогодні, в ОВУ дуже мало,

або їх взагалі немає, їх необхідно готувати. При проведенні навчання на базі університету їх роль виконують викладачі та фахівці центру імітаційного моделювання (далі – ЦІМ).

В той самий час проведення таких навчань з залученням до них представників інших військових формувань, що входять до складу сил оборони, дозволять відпрацьовувати заходи щодо досягнення їх взаємодії, що в подальшому забезпечить набуття спроможностей спільно виконувати завдання

На бригадне КШН посередники призначаються при заступниках командира бригади, начальниках родів військ та служб, командирах батальйонів (дивізіонів). Посередник при командирі батальйону (дивізіону) є одночасно посередником при командирах підпорядкованих рот (батареї), якщо вони залучаються до навчання. Якщо командири рот до навчання не залучаються, то при нештатних командирах рот (батареї), можуть працювати оператори робочих станцій.

Для зручності та більш ефективної роботи апарату керівництва, за рішенням керівника навчання, до його складу можуть призначатися представники вищого штабу, так звані, «сили старшого начальника» (штабу оперативно-

тактичного угруповання військ, оперативного угруповання військ).

Відмінністю у структурі штабу керівництва навчання є введення до його складу: групи застосування засобів автоматизації управління військами та групи імітаційного моделювання бойових дій.

Функції і завдання даним структурам визначає особисто начальник штабу керівництва. До створених груп, ми вважаємо, повинні входити офіцери (службовці, працівники ЗС України) – фахівці автоматизованих систем управління та імітаційного моделювання бойових дій (далі – ІМБД) у тому числі від Національний університет оборони України імені Івана Черняхівського (далі – НУОУ).

Завданнями групи застосування засобів автоматизації управління військами та групи імітаційного моделювання бойових дій можуть бути:

для групи застосування засобів автоматизації управління військами: формування бази даних автоматизованої системи управління військами та змінних вихідних даних для інформаційно-розрахункових задач (моделей);

забезпечення безперебійного та надійного функціонування автоматизованої системи управління військами (далі – АСУВ) “Славутич” під час виконання тими, хто навчається, заходів планування та безпосереднього управління підрозділами під час ведення бойових дій;

адміністрування та налаштування АСУВ “Славутич”;

підтримка розіграшу дій противника та своїх військ;

забезпечення проведення аналізу проведених дій (далі - АПД).

для групи імітаційного моделювання бойових дій:

підготовка апаратно-програмного комплексу до навчання;

створення бази даних бригади (організаційно-штатна структура та бойовий і чисельний склад, положення і стан підрозділів бригади, вибір електронної карти місцевості, метеорологічних умов, пори року та часу доби) відповідно до замислу навчання;

забезпечення у взаємодії з відділенням планування розіграшу дій противника, відображення дії сил і засобів старшого начальника, сусідів, приданих і підтримуючих підрозділів;

супроводження та правильна експлуатація засобів імітаційного моделювання бойових дій;

забезпечення групи аналізу проведених дій необхідним матеріалом щодо втрат, миттєвими знітками реальної обстановки в ході бою, відеофайлами розіграшу бойових дій.

В період підготовки до навчання дещо змінюється алгоритм роботи самого керівника

навчання.

Особливістю в його роботі в цей період є те, що після визначення вихідних даних, при віддачі вказівок начальнику штабу керівництва, він додатково вказує на планування і терміни проведення низки заходів щодо підготовки апарату керівництва і посередників, пов'язаних із застосуванням засобів автоматизації та імітаційного моделювання на базі НУОУ.

Керівник навчання повинен особисто провести: рекогносцировку місць проведення навчання в НУОУ для вивчення особливостей роботи штабу керівництва і посередників, конфігурації КШН, порядку і особливостей розгортання пунктів управління (далі – ПУ) та організації роботи на них. В подальшому, протягом етапу теоретичної підготовки на базі університету, він приймає участь у проведенні занять з офіцерами апарату керівництва спільно з фахівцями університету по вивченню характеристик та можливостей засобів автоматизації управління та імітаційного моделювання в ході нарощування обстановки та розіграшу бойових дій;

визначає завдання офіцерам групи імітаційного моделювання на розробку бази даних сил і засобів та місцевості для введення в засіб імітаційного моделювання JCATS;

розглядає і затверджує базу даних для АСУВ “Славутич” та змінних вихідних даних для інформаційно-розрахункових задач [1].

Особливістю роботи штабу керівництва в період планування КШН є те, що за рішенням керівника, окрім групи планування навчання, до відпрацювання замислу навчання, можуть залучатись представники військової частини та центру інформаційного моделювання, які, в подальшому, будуть безпосередньо займатись підготовкою навчання і створенням бази даних військ та місцевості відповідно до сценарію навчання. При цьому, основоположний документ (Замисел КШН) повинен бути відпрацьований значно раніше і затверджений не пізніше місяця до його початку, з метою надання більше часу для проведення якісного планування навчання, підготовки офіцерів апарату керівництва, посередників в тому числі для проведення тренування в роботі на засобах автоматизації та імітаційного моделювання.

Досвід проведення бригадних КШН на базі університету показує, що підготовку офіцерів апарату керівництва та посередників доцільно проводити в 3 етапи. При цьому, підготовку необхідно проводити в навчальних центрах, де є відповідна навчально-матеріальна технічна база (далі – НМТБ) із залученням до проведення занять фахівців від НУОУ та інших вищих військових навчальних закладів (далі – ВВНЗ), або її проводити на базі НУОУ.

Основні заходи, що проводяться в ході поетапної підготовки апарату керівництва та

посередників:

етап перший – централізоване проведення теоретичної фази підготовки апарату керівництва та посередників на базі НУОУ (протягом 5 діб) та уточнення керівником навчання Замислу КШН (виходячи із можливостей НМТБ);

етап другий – завершення планування навчання (в штабах ОВУ, відпрацювання планів нарощування обстановки та розіграшу бойових дій, організації і проведення досліджень, підведення підсумків, а також бази даних сил і засобів та місцевості) та відпрацювання часткових планів роботи апарату керівництва і посередників;

етап третій – проведення практичних та інструктивних занять на ПУ та центрі імітаційного моделювання НУОУ.

Основна частина теоретичних занять повинна проводитись під керівництвом висококваліфікованих фахівців АСУВ “Славутич” та ІМБД.

В ході проведення 2-х денних практичних занять в НУОУ, офіцери апарату керівництва та посередники, під керівництвом керівника навчання та фахівців НУОУ тренуються у відпрацюванні порядку нарощування обстановки та розіграшу бойових дій. Керівник навчання проводить інструктивне заняття, в ході якого, уточняє порядок проведення кожного етапу (по днях) навчання, дії апарату керівництва навчанням та посередників, заслуховує їх про готовність та затверджує часткові плани роботи.

Тренування тих, хто навчається в роботі на тактичне завдання вручалось тим, хто навчається не пізніше ніж за 10-15 діб до його початку. Одночасно, вихідна обстановка в електронному вигляді вводилася в базу даних тих, хто навчається, з таким розрахунком, щоб її можна було використовувати під час попередніх тренувань апарату керівництва та тих, хто навчається, а база даних про бригаду (сил і засобів та місцевості) завчасно заносились в базу даних АСУВ “Славутич”. Контроль готовності бази даних здійснював особисто начальник штабу керівництва.

За 7 діб до початку навчання під контролем штабу керівництва, здійснювалось: розгортання ПУ, підготовка до роботи засобів енергопостачання і зв'язку та підготовка операторів робочих станцій.

На завершальному етапі підготовки, керівник навчання особисто та через штаб керівництва і посередників перевіряв готовність до навчання засобів автоматизації, імітаційного моделювання та обладнання автоматизованих робочих місць.

Алгоритм роботи керівника та штабу керівництва в ході проведення навчання:

доведення тим, хто навчається бойових наказів і розпоряджень у ролі старшого начальника та вихідної обстановки на електронній карті;

аналіз прийнятих рішень, тих хто навчаються,

за результатами проведених оперативно-тактичних розрахунків та відображення на електронних картах.

контроль за практичними діями тих, хто навчається, вивчення їх методів роботи по плануванню бою та управлінню підрозділами в ході ведення бойових дій [4].

Засоби автоматизації забезпечують ведення і відображення положення, стану та дій військ в реальному масштабі часу на електронній карті, яку постійно і в повному обсязі бачить керівник навчання.

Керівник може впливати на перебіг навчання, якщо ті, хто навчається, не впоралися з виконанням завдань, що поставлені перед ними, а також при необхідності внести зміни в загальний порядок нарощування обстановки та розіграшу тактичних епізодів. Для цього, він повинен зупинити навчання, провести аналіз дій тих, хто навчається та уточнити завдання штабу керівництва щодо подальшого нарощування обстановки.

Керівник та офіцери штабу керівництва і посередники здійснюють постійний контроль за практичними діями тих, хто навчається.

Основним способом нарощування обстановки в ході проведення навчання є - нарощування обстановки через “сили противника” (так звану “червону групу”).

Обстановка, що створена на навчання групую нарощування обстановки, через “сили противника”, в режимі реального часу, доводиться до командирів рот (батарей) які, її оцінюють та, по засобах зв'язку, доповідають командирам батальйонів (дивізіонів). Командири батальйонів (дивізіонів), наносять обстановку, на робочу карту (використовуючи “оверлей”) та на електронну карту АСУВ “Славутич”, приймають рішення та, доповідають командирю бригади. Тобто, все відбувається як в реальному бою.

В той же час, нарощування обстановки може здійснюватись і безпосередньо керівником навчання через “сили старшого командира та сусідів”, (так звану, “синю групу”). При цьому, в ході розіграшу бойових епізодів, на основі вказівок керівника навчання, обстановка у вигляді ввідних чи розпоряджень, доводиться в режимі реального часу, тим, хто навчається, через помічника керівника навчання з використання засобів автоматизованого управління військами “Славутич”.

В ході розіграшу бойових дій керівник навчання на екрані робочої станції спостерігає повне відображення обстановки у реальному масштабі часу та має можливість фіксувати недоліки прийнятих рішень тими, хто навчаються (невиконання бойових завдань, затримки у часі виходу на зазначені рубежі, понесені втрати тощо).



## Висновки й перспективи подальших досліджень

Таким чином, особливістю в роботі керівника КШН з використанням засобів автоматизації управління та імітаційного моделювання бойових дій є те, що він може не тільки контролювати дії підлеглих, але і показувати як позитивні, так і негативні аспекти прийнятих рішень та їх результати, а також особисто проводити розбір тактичних епізодів.

Оцінюючи позитивні і негативні аспекти в проведенні КШН з використанням засобів автоматизації та імітаційного моделювання, можна зробити висновок, що такі навчання мають низку переваг на відміну від традиційних командно-штабних навчань на місцевості, чи на картах і тому, в майбутньому, їх необхідно впроваджувати

## Література

1. Використання засобу імітаційного моделювання бойових дій "Об'єднаний імітатор конфліктних і тактичних ситуацій": навч. посіб./ колектив авторів; за заг. ред. С.М.Салкуцана.. – 2-ге вид., доповн. – К. : НУОУ ім. Івана Черняхівського, 2017. – 188 с.
2. Імітаційне моделювання у практиці підготовки військ: навч. посіб. / колектив авторів; за заг. ред. О. Ю. Пермякова. – К. : НУОУ ім. Івана Черняхівського, 2015. – 120 с.
3. Концепція підготовки Збройних Сил України : за станом на 22 лют. 2016 р. – К. : Мін-во оборони України та ГШ ЗСУ, 2016. – 14 с.
4. Методика підготовки і проведення командно-штабних

в практику підготовки ОВУ та військ враховуючи особливості об'єднаної підготовки.

Отже для підвищення рівня підготовки ОВУ пропонуються наступні рекомендації:

визначати на цикл навчання проведення КШН з використанням засобів автоматизації та імітаційного моделювання бойових дій;

на базі НУОУ створити групи застосування засобів автоматизації управління військами та групи імітаційного моделювання бойових дій;

залучити до проведення КШН з використанням засобів автоматизації та імітаційного моделювання бойових дій персонал інших складових сил оборони.

навчань за допомогою комп'ютерів з використанням технологій імітаційного моделювання: навч. посіб./ колектив авторів; за заг. ред. О. Ю. Пермякова. – К. : НУОУ ім. Івана Черняхівського, 2011. – 60 с.

5. Основи імітаційного моделювання: навч. посіб./ колектив авторів; за заг. ред. О. Ю. Пермякова. – К. : НУОУ ім. Івана Черняхівського, 2006. – 39 с.

6. Указ Президента України №92/2016 "Про рішення Ради національної безпеки і оборони України від 04 березня 2016 року "Про Концепція розвитку України" [Електронний ресурс]. – Режим доступу [www.president.gov.ua](http://www.president.gov.ua).

## ПОДГОТОВКА АППАРАТА УПРАВЛЕНИЯ К КОМАНДНО-ШТАБНЫМ УЧЕНИЯМ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

*Григорий Митрофанович Тихонов (кандидат военных наук, с.н.с.)*

*Владимир Иванович Баталюк*

*Виталий Николаевич Безуглий*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*В статье рассматриваются современный процесс организации работа аппарата руководства и посредников в ходе подготовки и проведения командно-штабных учений с применением современных средств автоматизации и имитационного моделирования боевых действий, предоставлен полный перечень документов, отрабатываются аппаратом руководства различия в работе штаба руководства на этапе планирования обучения. Определены особенностью работы штаба руководства в период планирования учений и особенности в структуре аппарата руководства и посредников для проведения именно такого обучения. Рассматриваются теоретические положений и практических рекомендаций по внедрению и совершенствованию подготовки органов военного управления Вооруженных Силах Украины. Определены основные задачи группы применения средств автоматизации управления войсками и группы имитационного моделирования боевых действий. Определена необходимость привлечения к ним представителей других военных формирований, входящих в состав сил обороны с целью отработки меры направленных на достижение взаимодействия направленных на приобретение индивидуальных возможностей по совместному выполнять задания.*

*Предложены рекомендации по практическим вопросам подготовки аппарата руководства к командно-штабных учений с использованием средств автоматизации и имитационного моделирования боевых действий JCATS, а также автоматизированной системы управления войсками "Славутич".*

**Ключевые слова:** командно-штабное учения, аппарат управления, средства автоматизации и имитационного моделирования

PREPARING THE MANAGEMENT APPARATUS FOR COMMAND POST EXERCISES USING SIMULATION TOOLS

*Hrygorii Tikhonov (Candidate of Military Sciences, Senior Researcher)*

*Vladimir Bataluk*

*Vitaly Bezuhlyi*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*The article examines the modern process of organizing the work of the leadership apparatus and intermediaries in the preparation and conduct of command and staff exercises using modern tools for automation and simulation of combat operations, provides a complete list of documents that are worked out by the leadership staff differences in the planning staff. The peculiarity of the work of the headquarters of the management during the planning of the exercises and the peculiarities in the structure of the management apparatus and intermediaries for carrying out such training are determined. Theoretical provisions and practical recommendations on the implementation and improvement of training of the military management bodies of the Armed Forces of Ukraine are considered. The main tasks of the group of application of tools of automation of control of troops and group of imitation modeling of fighting are outlined. The necessity to involve representatives of other military formations that are part of the defense forces in order to work out measures aimed at achieving cooperation aimed at acquiring individual capabilities to perform joint tasks was determined.*

*Recommendations on practical issues of preparation of the leadership apparatus for command and staff training using the JCATS automation and simulation of combat operations, as well as the Slavutich military automated control system are offered.*

**Keywords:** *command and staff training, leadership apparatus, automation and simulation tools.*

### **References**

1. Using the simulation tool of combat action "Joint simulator of conflict and tactical situations": Tutorial. guide / team of authors; for the total. ed. S.M. Salkutsana . - 2nd ed., Suppl. - K.: NGO them. Ivan Chernyakhovsky, 2017. - 188 p. 2. Simulation Modeling in the Practice of Troops Training. tool. / team of authors; for the total. ed. O.Y. Permyakova. - K.: NGO them. Ivan Chernyakhovsky, 2015. - 120 p. 3. The concept of training of the Armed Forces of Ukraine: as of February 22. 2016 - K.: Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine, 2016. - 14 p. 4. Methods of preparation and conduct of command-staff exercises using computers using simulation technologies: teach. guide / team of authors; for the total. ed. O.Y. Permyakova. - K.: NGO them. Ivan Chernyakhovsky, 2011. - 60 p. 5. Fundamentals of simulation modeling: teach. guide / team of authors; for the total. ed. O.Y. Permyakova. - K.: NGO them. Ivan Chernyakhovsky, 2006. - 39 p. 6. Presidential Decree No. 92/2016 "On the Decision of the National Security and Defense Council of Ukraine of March 04, 2016" "On the Concept of Development of Ukraine"[Electronic resource]. - Access mode [www.president.gov.ua](http://www.president.gov.ua).

Юрій Олександрович Ганненко  
Микола Анатолійович Закалад

Національний університет оборони України імені Івана Черняхівського, Київ, Україна

## АНАЛІЗ ФУНКЦІОНУВАННЯ СИСТЕМИ ЛОГІСТИКИ У ПРОВІДНИХ КРАЇНАХ СВІТУ

У статті на основі проведеного аналізу функціонування системи логістики Збройних Сил провідних країн світу пропонується її удосконалення шляхом створення автоматизованої системи управління логістики.

Для ефективного управління логістичними процесами Збройних Сил України необхідне використання системного рішення стосовно формування автоматизованої системи управління логістики, вибору інформаційно-програмної платформи відповідної функціональності та масштабу для автоматизації процесів управління логістики, побудови інформаційної інфраструктури системи логістики, та, зрештою, – створення автоматизованої системи управління логістики Збройних Сил України.

Інформатизація має бути одним з пріоритетних напрямків роботи з підвищення ефективності діяльності логістики Збройних Сил України. Створення нових і модернізація існуючих автоматизованих систем управління логістики на основі передових інформаційних технологій, дозволить підвищити ефективність управління логістикою ЗС України, скоротити час на одержання і всебічну оцінку відомостей про матеріальні засоби на всіх етапах їх руху, підвищити ефективність логістичного, медичного і фінансового забезпечення, а також покращити взаємодію з аналогічними системами країн-партнерів НАТО.

**Ключові слова:** логістика, автоматизована система управління логістики, інформаційні технології.

### Вступ

Створення сучасної ефективної системи логістики Збройних Сил (далі – ЗС) України набуває в сучасних умовах особливої актуальності. Динаміка бойових дій на Сході України значно підвищує вимоги до оперативності забезпечення військ (сил) матеріальними засобами і передбачає безумовну відповідність можливостей системи логістики потребам угруповань (підрозділів) військ (сил).

**Постановка проблеми.** Аналіз поточного стану логістики ЗС України, досвіду ведення операції об'єднаних сил (антитерористичної операції), оцінка стану сектору безпеки і оборони, виявили низку проблем, внаслідок яких неможливо належним чином впроваджувати систему логістики ЗС України, а саме:

відсутність єдиної системи логістики, недосконалість системи управління логістики Збройних Сил України (внаслідок перманентного реформування існуючих та створення нових органів військового управління логістики) не дозволяють на високому рівні здійснювати заходи організації та виконання необхідних завдань логістики (матеріального, технічного та медичного забезпечення) ЗС України;

неоптимальний розподіл відповідальності та необхідних повноважень за організацію та

здійснення завдань і заходів логістики у структурах органів військового управління Міністерства оборони та Генерального штабу ЗС України знижує ефективність системи логістики та системи управління ЗС у цілому;

недостатній рівень постачання ресурсів для забезпечення заходів розвитку, підготовки та застосування військ (сил), надмірність обсягів та неактуальність нормативно-правової бази призводять до зниження боєздатності та ефективності застосування військ (сил);

відсутність інтегрованої автоматизованої системи управління логістики ЗС не дозволяє у повній мірі використовувати інтелектуальний потенціал органів військового управління, можливості сил та засобів логістики, раціонально управляти матеріально-технічними та іншими необхідними ресурсами і, як наслідок, не дозволяє у повній мірі використовувати бойові спроможності військ (сил);

низький рівень застосування сучасних інформаційних технологій в ЗС України.

Для ефективного управління логістичними процесами ЗС України необхідне використання системного рішення стосовно формування автоматизованої системи управління логістики (далі – АСУЛ), вибору інформаційно-програмної

платформи відповідної функціональності та масштабу для автоматизації процесів управління логістики, побудови інформаційної інфраструктури системи логістики, та зрештою – створення автоматизованої системи управління логістики ЗС України.

Ефективність зусиль “об’єднаної логістики” визначається оптимальним розподілом функцій між командуваннями, видами ЗС, органами військового управління, матеріально-технічним забезпеченням, оптимальним функціонуванням виконавців заходів логістики, які у цілому утворюють єдину об’єднану систему логістики.

Інформаційно-аналітичне забезпечення процесів управління логістики – це основа своєчасного, якісного та ґрунтовного рішення, ефективних процесів управління та контролю. Зрозуміло, що управління всіма підсистемами логістики, виконавцями, ресурсами та забезпечення ЗС усім необхідним для їх надійного функціонування в умовах ведення бойових дій вимагають використання найсучасніших методів і засобів військової логістики, інформаційних технологій, постійного пошуку нетривіальних рішень у ході бою, коли ситуація змінюється безперервно і непередбачувано.

**Аналіз останніх досліджень і публікацій.** Аналіз останніх наукових досліджень і публікацій свідчить про те, що підвищенню ефективності системи логістики присвячена низка робіт попередників, які в свій час зробили вагомий внесок у розвиток теорії військової науки. Однак, аналіз запропонованих ними методик свідчить про те, що вони розглядали окремо тилове, технічне та медичне забезпечення і не були враховані чинники, які суттєво впливають на своєчасність та ефективність єдиної системи логістики, а саме використання автоматизованої системи управління логістики. Саме тому, дані методики у наявному вигляді не можуть бути використані у повному обсязі для дослідження автоматизованої системи управління логістики, але можуть бути обрані за основу для подальшого удосконалення.

**Метою статті** є дослідження автоматизованих систем управління логістики збройних сил провідних країн світу, удосконалення системи логістики, визначення проблем та шляхів їх вирішення.

### **Виклад основного матеріалу дослідження**

Проаналізувавши автоматизовані системи управління логістики збройних сил провідних країн світу можна виділити такі основні напрями підвищення ефективності системи логістики:

1. Для обробки гігантських потоків інформації у військових системах логістики широко впроваджуються та використовуються системи планування ресурсів підприємства Enterprise Resource Planning (ERP), системи електронних закупівель (e-procurement EP).

2. У підрозділах логістики активно використовуються інформаційні системи контролю за матеріальними потоками, відомі під назвою “систем повної видимості активів” total asset visibility.

3. Усі військові вантажі, контейнери та пакувальні матеріали оснащені пасивними радіочастотними мікрочіпами-ідентифікаторами RFID для безконтактної радіочастотної ідентифікації.

4. Використовуються стандарти планування потреб в матеріалах і концепції корпоративного планування, створюються системи управління матеріальними потоками – відбувається перехід від окремих закупівель до управління інтегрованими ланцюгами поставок (integrated supply chain management).

5. Відбуваються зміни концептуальних принципів в організації та здійсненні діяльності ЗС, зміщення акцентів від управління окремими структурами до організації наскрізних динамічних функціональних процесів [5,12,13].

Основні принципи та поняття, які покладені до основи автоматизованої системи управління ресурсами підприємства (Enterprise Resource Planing – ERP-System), повною мірою збігаються із понятійним апаратом таких автоматизованих систем управління матеріальними ресурсами військового призначення, як системи командування і управління (Command & (and) Control – C2), прийняті в арміях провідних країн світу (далі – ПКС), зокрема НАТО.

Ознаки ідентичності таких систем очевидні. Так, наприклад, система ERP позиціонується як система програмно реалізованих, автоматизованих засобів управління ресурсами підприємства, що включає управління матеріальними, фінансовими та людськими ресурсами (кадри).

$$Z_n(i, j) = \sqrt[N]{\prod_{m=1}^N H_{n,m}(i, j)},$$

де:  $H_{n,m}(i, j)$  – значення  $i$ -ої характеристики, виставленої  $j$ -ми експертами при порівнянні  $n$ -ої ERP-системи з іншими системами, підраховується по кожному рядку;

$Z_n(i, j)$  – середнє геометричне значень  $H_{n,m}(i, j)$  (обчислюється корінь  $N$ -го ступеня з добутку всіх значень) і проводиться нормування, тобто приведення значень до інтервалу  $[0,1]$  – кожне середнє геометричне ділиться на суму всіх середніх геометричних:

$$X_n(i, j) = \frac{Z_n(i, j)}{\sum_{m=1}^N Z_m(i, j)},$$

де:  $X_n(i, j)$  – нормоване значення  $i$ -ої характеристики, виставленої  $j$ -ою кількістю експертів при порівнянні  $n$ -ої ERP-системи з іншими системами.

Для кожної ERP-системи обчислюється значення  $X_n(i)$  – порівняльної оцінки n-ї ERP-системи з іншими системами за характеристикою і по всім M підгрупам експертів з урахуванням їх вагових коефіцієнтів:

$$X_n(i) = \frac{1}{M} \sum_{j=1}^M X_n(i, j) R(j),$$

де:  $R(j)$  – нормований ваговий коефіцієнт (вага) j-ї кількості експертів [5].

Стосовно ЗС України, в яких облік особового складу, матеріально-технічних засобів, озброєння і військової техніки та фінансових засобів досі ведеться окремо, впровадження як концепцій, так і програмних рішень ERP-систем є нагальною та актуальною необхідністю. Очевидно, що облік вищезазначених ресурсів військових частин по всім службам забезпечення є взаємопов'язаним і потребує своєї інтеграції в межах єдиної ERP-системи [4].

У ЗС провідних країн світу для розвитку інформаційної інфраструктури логістики проводяться комплексні заходи, спрямовані на модернізацію існуючих та розробку нових компонентів АСУЛ, ведуться роботи зі створення адаптивної інтегрованої інформаційної інфраструктури логістики з єдиним операційним середовищем і стандартизованими формами подачі інформації. За цим досвідом зроблено висновок, що цілеспрямовану логістику можна реалізувати тільки на основі сучасної автоматизованої системи на базі оборонного ІТ-рішення ERP-класу.

За оцінкою фахівців [5,12,13], широке застосування передових інформаційних технологій в процесі створення нових і модернізації існуючих систем логістики забезпечить більш ефективне управління логістикою ЗС, скоротить час на отримання інформації та всебічну оцінку відомостей щодо матеріальних та технічних ресурсів на всіх етапах руху, зменшить ризики несвоєчасного або недостатнього за силами і засобами реагування на загрози, підвищить ефективність та взаємодію логістичних підрозділів військових формувань ЗС України.

Світова тенденція по створенню великомасштабних автоматизованих систем для збройних сил з управління оборонними ресурсами у більшості провідних країн світу (членів НАТО) бере свій початок з другої половини 90-х років і полягає у поетапній модульній автоматизації управлінських процесів та інтеграції модулів в загальну функціональну інформаційну систему на одній програмній платформі ERP-класу. Така система об'єднує в єдиному програмному середовищі та інформаційному просторі найбільш важливі процеси забезпечення життєдіяльності, розвитку та застосування збройних сил (логістичне забезпечення, фінансова діяльність, менеджмент особового складу, ведення

організаційної структури, оборонне планування, управління інфраструктурою тощо).

Автоматизовані логістичні системи (далі – АЛС) ЗС провідних країн світу створюються у відповідності до вимог стосовно функціональності, архітектури, процесів, процедур та стандартів НАТО та враховують основні вимоги до військових логістичних концепцій таких як:

“Мережецентричне логістичне забезпечення” (Network Centric Logistics – NCL);

“Об'єднана логістика” (Joint Concept for Logistics - JCL);

“Загальна видимість ресурсів логістичного забезпечення” (Joint Total Asset Visibility - JTAВ);

“Цілеспрямоване логістичне забезпечення” (Focused Logistics);

“Чутливе і швидко-реагуюче логістичне забезпечення” (Sense and Respond Logistics)”

“Всеохоплююча логістична готовність” (360 Logistic Readiness) та інші.

Розвиток інформаційних технологій, а також вищезазначені концепції сформувало погляди командування збройних сил США щодо створення і впровадження автоматизованої системи управління логістики.

До числа основних завдань АСУЛ, на погляд експертів [1,2,18], входять:

взаємодія і інтеграція інформації об'єднаних і видових систем забезпечення збройних сил, включаючи систему постачання зброї і матеріальних засобів, фінансового, медичного, технічного забезпечення і перевезення;

взаємодія інформаційних систем логістики країн-членів НАТО, а також союзників США, під час спільного врегулювання конфліктів і криз;

взаємодія процесів забезпечення угруповань сил і оперативного управління ними, а також надання можливості командуючим оперативними формуваннями вибору з більшого числа тактичних варіантів дій;

планування логістики; забезпечення доступу до постійно оновлюваної інформації від різних джерел централізованої бази даних логістики (відстеження запасів, стану і місця розташування боєприпасів, ПММ та іншого майна);

централізація інформації про потреби бойових підрозділів у матеріальних засобах (далі – МтЗ);

взаємодія з постачальниками МтЗ і підрядниками з доступом посадових осіб до постійно підтримуваної загальної бази забезпечення і системам електронної комерції [7].

У межах досягнення намічених цілей за останні роки значних змін зазнала організаційна структура логістики збройних сил США і, перш за все, сухопутних військ.

На даний час у збройних силах США реалізується ініціатива “Логістика майбутнього”, активно впроваджується система автоматичної ідентифікації всієї номенклатури предметів постачання на основі штрих-кодів, активних і

пасивних радіочастотних міток, а також систем супутникової навігації транспортних засобів. З метою поліпшення показників своєчасності і якості регламентного обслуговування і ремонтних робіт впроваджують програми повного автоматизованого забезпечення життєвого циклу озброєння і військової техніки і їхнього забезпечення CALS (Continuous Acquisition and Life-cycle Support). Докладено значних зусиль для досягнення уніфікації технічного забезпечення і функціонально-технічної сумісності основних вузлів, агрегатів і механізмів. На цій основі створюються модульні ремонтно-відбудовчі комплекти запчастин, інструмента і приладдя.

Організаційно-технологічна структура перспективної системи логістичного забезпечення на тактичному рівні потребує створення підрозділів автоматизації, відповідальних за технічне обслуговування і ремонт комп'ютерних систем, усунення неполадок і коректування програмного забезпечення інформаційних систем озброєння та військової техніки.

Прогрес у розвитку систем автоматизації управління логістики особливо очевидний на прикладі повітряних сил, де подібна система базується на системі бойового управління експедиційними силами ECSS (Expeditionary Combat Support System), підсистемою якої є система відстеження потоків матеріальних запасів АМТ (Asset Marking and Tracking).

Також відмічається, що ECSS – це, по суті, АСУ логістичного забезпечення, що дозволяє управляти матеріальними ресурсами в режимі часу, близькому до реального, зводячи у єдиний процес усі заходи логістичного забезпечення з відображенням єдиної повної картини логістичної обстановки. Вона є основою експедиційного і “мережецентричного” логістичного забезпечення XXI століття. За досвідом експлуатації ECSS час вирішення завдань логістики, на які раніше було потрібно близько 1 год., скоротився до 15 хв.

“Загальна видимість ресурсів” забезпечується системою АМТ, що включає автоматичну ідентифікацію і радіочастотне маркування більш ніж 12,4 млн. предметів постачання. На сьогодні у межах цієї системи обслуговуються понад 700 тис. предметів постачання.

Зазначені системи дозволяють здійснювати забезпечення всіх існуючих у світі угруповань повітряних сил США на основі єдиного планування, оптимізації ресурсів (ERP) та на основі єдиних пріоритетів. Раніше даний процес відбувався на декількох підпорядкованих рівнях зі своїми пріоритетами на кожному з них [3,8,15,16,19].

Одне з технологічних нововведень демонструє з 2010 року програма TEMP (Tactically Expandable Maritime Platform) з розробки модулів на основі стандартних морських контейнерів для реалізації функцій логістичного забезпечення. На їхній базі планується створити модулі різного призначення:

організації зв'язку і управління; збору і обробки інформації; забезпечення енергією (паливом); реалізації систем захисту (самооборони); ремонту і обслуговування ОВТ; медичного забезпечення та ін.

Особливий інтерес представляють дві концепції: “модульний морський склад” (Modular Sea Depot) і “модульна морська база” (Modular Sea Base). Головна ідея цих концепцій у можливості створення великої автономної плавучої логістичної інфраструктури морського базування із модульних контейнерів-модулів. Наприклад, структура з десяти модулів може утворити злітно-посадочний майданчик для вертольотів або виконувати функції паливозаправників для десантних катерів, катерів сил спецоперацій, а також для інших малорозмірних кораблів у прибережній зоні.

Планується, що за допомогою контейнерних модулів можна буде зібрати велику базу для забезпечення дій об'єднаних американських експедиційних сил. Подібна морська рухома база забезпечить розміщення і дії всіх платформ і носіїв зброї, включаючи літаки палубного і наземного базування. При цьому вона буде мати необхідні морехідні якості, вантажопідйомність, стійкість і плавучість. Доставку контейнерів-модулів бази до будь-якої точки Світового океану передбачається здійснювати звичайними комерційними кораблями-контейнеровозами.

Військові експерти провідних країн світу [1,2,7] вважають основними критеріями оцінки ефективності функціонування системи логістичного забезпечення наступні:

час очікування поставки (виконання заявки) – з моменту реєстрації замовлення в системі постачання до підтвердження про одержання замовлених ресурсів;

точність за часом поставки (виконання заявки) – в межах установленого інтервалу.

Крім того, важливими критеріями є такі:

здатність забезпечити розгортання угруповань сил (в еквівалентних формуваннях, тис. чоловік);

швидкість розгортання (забезпечення мобільності) угруповань військ (сил);

здатність забезпечити автономність дій сил (тривалість бойових дій);

інтенсивність бойового забезпечення (доставки МтЗ) у ході бойових дій та ін.

Характерними рисами діючих і перспективних АСУЛ стануть: найвищий рівень автоматизації всіх основних функцій; здатність виконувати безперебійне постачання і будь-які вимоги угруповань сил у надзвичайних умовах; гнучкість і адаптивність системи забезпечення.

Система логістичного забезпечення збройних сил США спрямована на повне задоволення потреб угруповань сил у всіх фазах:

розгортання в районах бойового призначення; підготовки до перших операцій, початку бойових дій;

забезпечення сил у ході бойових дій (постачання, перегрупування і евакуація, відновлення боєздатності);

згортання бойових дій і передислокація до місць постійного базування.

Інформатизація і роботизація збройної боротьби висувають на перший план низку питань щодо: перевезення; технічного обслуговування і ремонту; відновлення боєздатності ОБТ поряд зі збереженням актуальності медичного і іншого видів забезпечення.

Логічним напрямком у розвитку АСУЛ збройних сил США та інших країн-членів НАТО є, без сумнівів, впровадження і застосування принципів і методів реалізованих у системах ERP-класу. Запропонована програма створення повністю інтегрованої ERP-системи логістичного забезпечення припускає будівництво єдиного віртуального органу логістики (Joint Logistics Enterprise) на базі корпоративного сховища даних (EDW – Enterprise Data Warehouse), а також інтеграцію різномірних інформаційних систем на основі WEB-технологій.

Процеси закупівель і розподілу ресурсів у сухопутних військ США до 2000-х років були роз'єднані. Даний недолік було усунуто лише з прийняттям до експлуатації системи GCSS-A. З 1999 року АСУЛ розвивалися на основі архітектури і з урахуванням досягнень відомої комерційної ERP-системи планування ресурсів фірми SAP (Systems, Applications and Products) версії R/3 (триланцюгова клієнт-серверна архітектура, що функціонує в реальному масштабі часу). Так, у військово-морських силах США розгорнуті три великі програми автоматизації логістичного забезпечення на основі ERP-системи SAP. На базі SAP будуються також системи прийняття рішень, аналізу і оцінки інформації (версія SAP NetWeaver BI – Business Intelligence) [10].

Глобальна АСУЛ сухопутних військ Сполучених штатів Америки GCSS-A (Global Combat Support System-Army) дозволяє мати точну, одержувану в реальному масштабі часу інформацію про ресурси, що є необхідною передумовою здійснення постачання сил без часу очікування. При цьому інтегруються до єдиного комплексу системи, які традиційно базувалися на трьох різних конфігураціях апаратних засобів, використовували сім операційних систем і розроблялися на восьми мовах програмування з використанням п'яти мережних протоколів обміну даними. GCSS-A увібрала в себе функції колишньої системи – STAMIS (Standard Army Management Information System), об'єднала понад десяти її підсистем у межах єдиної БД і операційної системи на платформі Windows NT, і ряду інших систем.

GCSS-A забезпечує доставку до передових бойових підрозділів ПММ і боеприпасів протягом доби. Інтеграція GCSS-A з автоматизованою

системою управління тилом вищого рівня CSSCS (Combat Service Support Command System) надає командирам повну логістичну інформацію, необхідну для прийняття ефективних рішень на полі бою. Маючи ситуаційну поінформованість, командир логістичного підрозділу здатний самостійно прогнозувати потреби забезпечуваного ним бойового підрозділу в постачанні, а також вчасно організовувати доставку і розподіл відповідних ресурсів. При цьому командир бойового підрозділу може зосередитися безпосередньо на веденні бойових дій, не відволікаючись на вирішення логістичних завдань [5,20].

Отже, на думку експертів АСУЛ провідних країн світу [2,15], стратегія і тактика є основою планування бойових дій, а служба логістики забезпечує засоби для їх ведення. Результат бойової операції залежить від стійкого і безперебійного функціонування логістики. Сьогодні логістика зазнає змін і розвивається під безпосереднім впливом військової стратегії, досягнення цілей якої вона покликано забезпечити.

Аналіз показує, що задовольнити наведеним вимогам можливо проведенням заходів, комплекс яких американські аналітики визначили як революцію в логістичному забезпеченні. Створення системи логістики з розподіленим базуванням планується шляхом:

заміни масових запасів матеріальних засобів і майна на створення умов їхньої швидкої доставки від виробників і постачальників у точній відповідності потребам замовників;

будови єдиної системи логістики на основі інформаційних технологій і ситуаційної поінформованості;

проведення організаційної реструктуризації;

створення гнучкої системи придбання;

впровадження нових технологій.

Основні заходи щодо вдосконалення системи логістики в найближчому майбутньому полягають у наступному. Скорочення надлишкових запасів матеріально-технічних засобів за рахунок переходу від принципу накопичення всього, що може знадобитися для потреб ЗС (“just-in-case”), до принципу постачання “з коліс” (“just-in-time”), що передбачає крім зазначених концепцій також:

1) розробку і впровадження концепцій “Прискореної доставки матеріальних засобів” для СВ, “Точної логістики” для морської піхоти (МП) і ініціативи управління логістики Міністерства оборони США “Пряма доставка від постачальників” (DVD – Direct Vendor Delivery) з метою поставок 50% усього майна, що виробляється, без складування, безпосередньо від виробника, а також проведення програм електронної комерції електронного взаємного обміну даними для укладення довгострокових контрактів, доставки майна “з коліс”, вибору

найвигідніших контрактів та вибору головного підрядника;

2) перехід ЗС до системи постачання за індивідуальними замовленнями;

3) реорганізацію існуючої системи логістики і створення модульних структур сил і засобів логістики, які легко адаптуються і спеціалізуються для виконання конкретних завдань;

4) передачу багатьох видів діяльності логістики з Міністерства оборони до приватного сектору за умови зниження витрат і виключення додаткового ризику для ЗС (програма Міністерства оборони США залучення цивільних організацій для логістики збройних сил США ( LOG-CAP – Logistic Civil Augmentation Program)).

5) модернізацію інформаційної інфраструктури логістики збройних сил США.

6) виявлення шляхів зменшення надлишкових запасів логістичного забезпечення в оперативнотактичній ланці, що знижують мобільність військ і їхню живучість, а також зниження вартості життєвого циклу об'єктів ОБТ, особливо їх експлуатації [1,2,5].

Слід зазначити, що для більшості перелічених вище заходів уже розроблені відповідні інформаційні технології у провідних країнах світу[6,9,11,14,17]. Інформаційними технологіями в логістиці, які використовуються з 2003 року, є ті з них, які застосовуються під час перевезень (штриховий код, радіочастотні маркери), у системах реляційних баз даних, мініатюрних приймачах сигналів глобальної системи визначення місця розташування GPS і передавачах повідомлень про місце розташування їх носіїв, космічному і волоконно-оптичному зв'язку, ефективних засобах планування військових кампаній і операцій.

Як вважають військові фахівці збройних сил США, революція в логістиці опирається, головним чином, на вдосконалення інформаційних систем і створення більш швидких транспортних систем меншої вартості, тому що однією з ключових складових у автоматизації поля бою і сил XXI століття є концепція досягнення панування в ситуаційній поінформованості, тобто знання всього того, що відбувається на полі бою, місця розташування, статусу, стану ресурсів своїх сил і сил противника, пересування і прогнозу поповнення запасів кожного елемента сил. Крім того, для повноти картини логістики повинна забезпечуватися загальна видимість ресурсів об'єднаних сил (JTAV), тобто їхнє місце розташування, стан, кількість, склад та інше.

В результаті впровадження концепції збройні сили США зможуть надійно випереджати противника в циклі бойового управління і прийняття рішень і, таким чином, різко підвищити ефективність дій своїх сил.

Процес впровадження ERP-систем є складним та вимагає серйозної підготовчої роботи, великого обсягу знань і навичок персоналу. Для

впровадження проектів доводиться вирішувати проблеми організаційного, технологічного характеру та, на жаль, долати протидію з боку співробітників організації-замовника ERP-системи, що характерно для консервативних, бюрократичних установ, у яких персонал не зацікавлений у нововведеннях, боїться втрати свого положення або розкриття нелегальних фінансових схем, не готовий відповідати за прийняті рішення, банально не бажає навчатися та опановувати нові знання, навички тощо. Для зменшення дії вказаних негативних факторів необхідно змінити мотивацію персоналу – заохочувати не за відсутність формальних помилок, а за зростання показників діяльності, також слід формувати у персоналу тверду впевненість у невідворотності новацій, підтримці проекту з боку вищого керівництва.

ERP системи дозволяють використовувати одну інтегровану програму замість декількох розрізнених. Єдина система комплексно управляє всіма сферами діяльності установи. Після впровадження ERP-системи в установі істотно знижується об'єм паперового документообігу, підвищується прозорість всіх процесів, інформація стає більш доступною і зручною для роботи. Крім автоматизації процесів установи, впровадження ERP-системи підвищує взаємну відповідальність всіх її підрозділів, сприяє підвищенню дисциплінованості співробітників.

Для керівництва ERP-система надає інструментарій для роботи з взаємозв'язаними показниками і стратегічного управління організацією в цілому. Зрілі ERP-системи сумісні з міжнародними стандартами якості, націлені на максимальне задоволення потреб організації в засобах управління. Нижче наведені середні значення показників підвищення ефективності діяльності установи за різними показниками при впровадженні ERP-систем [5,12].

### **Висновки і перспективи подальших досліджень**

Створення АСУЛ дозволить досягти виконання цілей стосовно:

підвищення боєготовності військ (сил) та ресурсного забезпечення їх бойової діяльності протягом тривалого часу;

збільшення ефективності функціонування ланцюгів забезпечення, надійності постачання та його адаптивності до потреб бойових підрозділів;

скорочення часу ремонту, обслуговування/модернізації озброєння, військової техніки та матеріальних засобів, зменшення обсягів потрібних запасних частин та майна.

Для досягнення цілей оборонної реформи щодо високої ефективності систем управління та відповідності і сумісності перспективних Збройних Сил України стандартам НАТО у період до 2020 року, необхідно для побудови АСУ "Логістика" обрати IT-рішення, яке пройшло випробування в експлуатації збройними силами



країн-членів НАТО. Доцільним рішенням є обрання готового промислового IT-рішення ERP-масштабу для оборонних відомств, адаптація якого дозволяє значно скоротити строки введення у продуктивну експлуатацію та звести до мінімуму ризику впровадження та подальшого використання системи внаслідок попередньої багатократної перевірки працездатності і надійної системи супроводу.

Таким чином, інформатизація має бути одним з пріоритетних напрямків роботи з підвищення

ефективності діяльності логістики ЗС України. Створення нових і модернізація існуючих АСУЛ на основі передових інформаційних технологій, дозволить підвищити ефективність управління тиловим та технічним забезпеченням ЗС України, скоротити час на одержання і всебічну оцінку відомостей про матеріальні засоби на всіх етапах їх руху, підвищити ефективність кадрового, медичного і фінансового забезпечення, а також покращити взаємодію з аналогічними системами країн-партнерів НАТО.

### Література

1. Автоматизированные информационные системы, базы и банки данных. Вводный курс. Учебное пособие. - М.: Гелиос АРВ, 2002, - 368 с. 2. Ващинин И.А. Война XXI века / Зарубежное военное обозрение №5/. - М.: Воениздат, 1998. - с.2-97. 3. Ващинин И.В. Взгляды США на развитие ВВС в начале XXI века / Зарубежное военное обозрение №1. - М.: Воениздат, 1998. - с. 17- 78. 4. Гаврилов А.Б., Красинський С.В., Носик О.М., Спренне В.С. Розробка автоматизованої системи отримання, зберігання та обробки інформації про наявність, стан та рух матеріальних засобів у Збройних Силах України Харків.- Честь і закон.-№2.-2007. 5. Дэннел О'лири ERP-системы: выбор, внедрение, эксплуатация. Современное управление ресурсами предприятия / - М.: Вершина, 2008. 6. Емельянова И.З., Партыка Т.Л., Попов И.И. Основы построения автоматизированных информационных систем: учебное пособие. / М.: ФОРУМ: ИНФРА- М, 2005. 7. Зацаринный А.А., Ионенков Ю.С. Тенденции развития современных информационных технологий с учетом концепции сетевых войн // Системы и средства информатики. 2007. Вып. 17. С. 47-64. 8. Заяц В.И. Роль и место воздушного транспорта в обеспечении стратегической мобильности вооруженных сил США / Зарубежное военное обозрение - М.: Воениздат, 1999,- № 4. -с.24-89. 9. Исследование операций и АСУ. - Республиканский межведомственный научный сборник. Выпуск № 18 - К.: Вища школа, 1981. - 88 с. 10. Кравченко Ю.А. PLM-технологии в SAP:

Учебное пособие. 2009, 170 с. 11. Курбаков К.И. Автоматизированные информационные системы в производстве, маркетинге и финансах: учеб. пособие / М.: КОС ИНФ, Рос. экон. акад., 2003. 12. Кульга К.С. Особенности внедрения на предприятиях и методы интеграции CAD/CAM/PDM/FRP/MRP/MES/PLM и ERP-систем / САПР и графика. 2008. №3. С. 91-94. 13. Мартынов Д. Проблемы быстрого действия систем ERP - системный кризис / Автоматизация управления компаниями. 2007. №10. С. 10-15. 14. Петров В.Н. Информационные системы. / СПб.: Питер, 2002, - с.688. 15. Резяпов Н. Основные аспекты развития системы тылового обеспечения ВС США: Зарубежное военное обозрение №3, 2012, С.24-29. 16. Резяпов Н. Развитие информационной инфраструктуры тылового обеспечения ВС США 2000 - настоящий момент: Зарубежное военное обозрение №9 2012 С.22- 31. 17. Титоренко Г.А. Автоматизированные информационные технологии в экономике: учебник // М.: ЮНИТИ, 2005. 18. Шмаков И.Г. Тыловое обеспечение сухопутных войск США / Зарубежное военное обозрение.- М.: Воениздат, 1995.- № 10. - с. 17-86. 19. Щербинин Р.В. Перспективы развития парка военно-транспортных и транспортно-заправочных самолетов США / Зарубежное военное обозрение - М.: Воениздат, 2000,- № 2. - с. 33-59. 20. Battle Command and Sustainment Support System (BCS3) [Электронный ресурс]Режим доступа до журн.: <https://www.globalsecurity.org/military/systems/ground/bcs3.htm>.

## АНАЛИЗ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЛОГИСТИКИ ВЕДУЩИХ СТРАН МИРА

*Юрий Александрович Ганненко  
Николай Анатолиевич Закалад*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*В статье на основе проведенного анализа функционирования системы логистики Вооруженных Сил ведущих стран мира предлагается ее усовершенствования путем создания автоматизированной системы управления логистики.*

*Для эффективного управления логистическими процессами Вооруженных Сил Украины необходимо использование системного решения по формированию автоматизированной системы управления логистики, выбора информационно-программной платформы соответствующей функциональности и масштаба для автоматизации процессов управления логистики, построения информационной инфраструктуры системы логистики, и наконец - создание автоматизированной системы управления логистики Вооруженных Сил Украины.*

*Информатизация должна быть одним из приоритетных направлений работы по повышению эффективности деятельности логистики Вооруженных Сил Украины. Создание новых и модернизация существующих автоматизированных систем управления логистики на основе передовых информационных технологий, позволит повысить эффективность управления логистикой ВС Украины, сократить время на получение и всестороннюю оценку сведений о материальных средствах на всех*

етапах їх движенья, підвищить ефективність логістического, медичнеского и фінансового обеспечення, а также уллучить взаємодєєствие с аналогічними системами стран-партнеров НАТО.

**Ключевые слова:** логістика, автоматизированная система управління логістики, інформаційні технології.

## ANALYSIS OF THE LOGISTICS SYSTEM IN THE LEADING COUNTRIES OF THE WORLD

*Iurii Hannenk  
Mikola Zakalad*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*In the article, based on the analysis of the functioning of the logistics system of the Armed Forces of leading countries of the world, it is proposed to improve it by creating an automated logistics management system.*

*The efficient management of logistics processes of the Armed Forces of Ukraine is necessary to use a system solution for the formation of an automated logistic management system, the selection of information and software platform of the appropriate functionality and scale for automation of logistics management processes, construction of the information infrastructure of the logistics system, and, ultimately, the creation of an automated logistic management system The Armed Forces of Ukraine.*

*Informatization should be one of the priority directions of work on improving the efficiency of logistics activities of the Armed Forces of Ukraine. Creation of new and modernization of existing automated logistic management systems based on advanced information technologies will allow to improve the efficiency of logistics management of the Armed Forces of Ukraine, reduce the time to receive and comprehensively evaluate information about material means at all stages of its movement, improve the efficiency of logistics, medical and financial provision, and also improve interaction with similar systems of NATO partner countries.*

**Key words:** logistics, automated logistics management system, information technology.

### References

1. Avtomatizirovannyye informatsionnyye sistemy, bazy i banki dannykh. Vvodnyy kurs. Uchebnoye posobiye. -M.: Gelios ARV, 2002, - 368 s. 2. **Vashchinin I.A.** Voyna XXI veka / Zarubezhnoye voyennoye obozreniye №5/. - M.: Voenizdat, 1998. - s.2-97. 3. **Vashchinin I.V.** Vzglyady SSA na razvitiye VVS v nachale XXI veka / Zarubezhnoye voyennoye obozreniye №1. - M.: Voenizdat, 1998. - s. 17-78. 4. **Gavrilov A.B., Krasins'kiy C.B., Nosik O.M., Sprenne B.C.** Rozrobka Avtomatizovanoi sistemi otrimannya, zberigannya ta obrobki informatsii pro nayavnist', stan ta rukh material'nikh zasobiv u Zbroynikh Silakh Ukraїni / Kharkiv.- Chest' i zakon.-№2.-2007. 5. **Deniyel O'iri.** ERP-sistemy: vybor, vnedreniye, espluatatsiya. Sovremennoye upravleniye resursami predpriyatiya / - M.: Vershina, 2008. 6. **Yemel'yanova I.Z., Partyka T.L., Popov I.I.** Osnovy postroyeniya avtomatizirovannykh informatsionnykh sistem: uchebnoye posobiye. / M.: FORUM: INFRA- M, 2005. 7. **Zatsarinnyy A.A., Ionenkov Y.S.** Tendentsii razvitiya sovremennykh informatsionnykh tekhnologiy s uchetom kontseptsii setetsentricheskikh voyn / Sistemy i sredstva informatiki. 2007. Vyp. 17. S. 47-64. 8. **Zayats V.I.** Rol' i mesto vozdušnogo transporta v obespechenii strategicheskoy mobil'nosti vooruzhennykh sil SSHA / Zarubezhnoye voyennoye obozreniye - M.: Voenizdat, 1999,- № 4. -s.24-89. 9. Issledovaniye operatsiy i ASU. - Respublikanskiy mezhdodomstvennyy nauchnyy sbornik. Vypusk № 18 - K.: Vishcha shkola, 1981. - 88 s. 10. **Kravchenko Y.A.** PLM-tekhnologii v SAP: Uchebnoye posobiye. 2009, 170s. 11. **Kurbakov K.I.** Avtomatizirovannyye informatsionnyye sistemy v proizvodstve, marketinge i finansakh: ucheb. posobiye / M.: KOS INF, Ros. ekon. akad., 2003. 12. **Kul'ga K.S.** Osobennosti vnedreniya na predpriyatiyakh i metody integratsii CAD/CAM/PDM/FRP/MRP/MES/PLM i ERP-sistem / SAPR i grafika. 2008. №3. S. 91-94. 13. **Martynov D.** Problemy bystrodeystviya sistem ERP - sistemnyy krizis / Avtomatizatsiya upravleniya kompaniyami. 2007. №10. S. 10-15. 14. **Petrov V.N.** Informatsionnyye sistemy. / SPb.: Piter, 2002, - s.688. 15. **Rezyapov N.** Osnovnyye aspekty razvitiya sistemy tyloвого obespecheniya VS SSHA: Zarubezhnoye voyennoye obozreniye №3, 2012, S.24-29. 16. **Rezyapov N.** Razvitiye informatsionnoy infrastruktury tyloвого obespecheniya VS SSHA 2000 - nastoyashchiy moment: Zarubezhnoye voyennoye obozreniye №9 2012 S.22- 31. 17. **Titorenko G.A.** Avtomatizirovannyye informatsionnyye tekhnologii v ekonomike: uchebnyk / M.: YUNITI, 2005. 18. **Shmakov I.G.** Tylovoye obespecheniye sukhoputnykh voysk SSHA / Zarubezhnoye voyennoye obozreniye.- M.: Voenizdat, 1995.- № 10. - s. 17-86. 19. **Shcherbinin R.V.** Perspektivy razvitiya parka voyenno-transportnykh i transportno-zapravochnykh samoletov SSHA / Zarubezhnoye voyennoye obozreniye - M.: Voenizdat, 2000,- № 2. - s. 33-59. 20. Battle Command and Sustainment Support System (BCS3) [Yelektronniyresurs] /Rezhim dostupu do zhurn.: <https://www.globalsecurity.org/military/systems/ground/bcs3.html>.

Олександр Юрійович Пермяков (доктор технічних наук, професор)<sup>1</sup>

Наталія Олександрівна Королюк (кандидат технічних наук)<sup>2</sup>

Софія Олександрівна Маслійова<sup>2</sup>

<sup>1</sup> Національний університет оборони України імені Івана Черняхівського, Київ, Україна

<sup>2</sup> Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків, Україна

## ПІДХІД ЩОДО АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ОЦІНКИ ПОВІТРЯНОГО ПРОТИВНИКА НА ПУНКТАХ УПРАВЛІННЯ ПОВІТРЯНИХ СИЛ ЗСУ

У статті запропонований підхід щодо вдосконалення спеціального математичного і програмного забезпечення АСУ для вирішення задачі розпізнавання замислу повітряного противника на основі нових інформаційних технологій створення та використання баз знань. Розглядається процес розпізнавання замислу дій повітряного противника в якості слабо структурованої задачі, яка стоїть перед особою, що приймає рішення, в ході підготовки та веденні бойових дій. Обґрунтовано для рішення слабо структурованої задачі використання теорії нечітких множин, що дозволяє розв'язати задачу розпізнавання замислу дій повітряного противника у складі системи підтримки прийняття рішення. В якості базової моделі представлення знань процесів розпізнавання варіантів дій повітряного противника в умовах невизначеності обґрунтована нечітка множина типу 2 і заснована на ній нечітка логічна система, що дозволяє формалізувати завдання, які не піддаються суворій формалізації і мають логіко-аналітичний характер. Використання когнітивних методів при створенні баз знань забезпечує можливість засобам автоматизації щодо рішення задачі оцінки повітряного противника в цілому, і зокрема задачі розпізнавання варіантів його дій, яка обмежується в основному технічними характеристиками обчислювальних засобів.

**Ключові слова:** розпізнавання замислу повітряного противника, нечітка множина типу 2, нечітка логічна система, система підтримки прийняття рішення.

### Вступ

**Постановка проблеми.** Аналіз локальних військових конфліктів останнього десятиліття двадцятого і початку двадцять першого століть дозволяє зробити висновок, що вдосконалення системи протиповітряної оборони (ППО) України є в даний час однією з важливих завдань військового будівництва. В ході ведення бойових дій однією з вирішальних умов організації та успішного проведення ППО об'єктів, своїх військ є обґрунтоване і своєчасне прийняття рішень на застосування сил і засобів за результатами оцінки повітряного противника (ПП). При цьому в ході ведення бойових дій основним змістом оцінки противника є аналіз даних про повітряну обстановку, що надходять з вищестоящого пункту управління (ПУ), від підлеглих і взаємодіючих військ, зіставлення цих даних з раніше зробленими прогнозами і передбачення змін в обстановці.

Процес оцінки і розпізнавання ПП в ході ведення бойових дій можна умовно розділити на оцінку противника на підступах до об'єктів, що обороняються, оцінку противника, діючого в межах відповідальності підпорядкованих сил і засобів авіації і ППО, і оцінку противника після відбиття ударів або в проміжках між ними. Основним питанням оцінки ПП на підступах до об'єктів, що обороняються, є розпізнавання варіанту дій противника. Важливість достовірного і оперативного розпізнавання варіантів дій ПП

визначається тим, що результат розпізнавання є основою для прийняття рішення особою, що приймає рішення (ОПР), на введення того чи іншого варіанту дій своїх військ.

У той же час, зростаюча динамічність і швидкоплинність бойових дій, високий ступінь невизначеності обстановки, жорсткі часові рамки розпізнавання варіантів дій ПП і необхідність аналізу і врахування великої кількості різномірних чинників свідчать про необхідність підвищення рівня автоматизації процесу вирішення задач розглянутого класу.

Аналіз спеціального математичного і програмного забезпечення як існуючих комплексів засобів автоматизації (КЗА) КП Повітряних Сил (ПС) дозволяє стверджувати, що процеси розпізнавання варіантів дій ПП автоматизовані недостатньо.

В ході нанесення удару з повітря, противник намагається досягнути певної мети. Метою може бути зміна політичного спрямування влади в країні-об'єкті удару, порушення її територіального суверенітету, реалізація економічних інтересів тощо. Мета визначається органами державного та військового управління противника на етапі формування замислу операції і, відповідно, являється визначеною для противника та невизначеною для сторони, по якій завдається удар. Оскільки мета операції (бойових дій) багато

в чому буде визначати форми і засоби застосування військ противника та об'єкти його удару, розпізнавання цієї мети якомога раніше є важливим завданням для органів управління ППО держави. Це дозволить зменшити рівень невизначеності відносно варіанта замислу дій ПП, та дасть можливість вибрати раціональний варіант дій своїх військ (сил) щодо прикриття від ударів з повітря тих об'єктів, по яким буде наноситись удар, й своєчасно визначити (уточнити) завдання підпорядкованим військам.

**Аналіз останніх досліджень і публікацій.** Розробці та використанню інтелектуальних інформаційних технологій для автоматизації процесів управління та створення відповідних БЗ присвячений цілий ряд робіт [1-4]. Однак питання розробки і використання методів формалізації, консолідації знань процесів розпізнавання варіантів дій ПП в умовах невизначеності є недостатньо дослідженими.

Таким чином, проблема полягає у пошуку методів розпізнавання замислу дій ПП, у знаходженні логічних закономірностей діяльності органів управління, які дозволять розпізнати об'єкти удару, а з них знайти можливі варіанти ієрархії цілей дій ПП, які розкривають його замисел.

**Метою статті є** удосконалення підходів щодо визначення закономірностей, що зв'язують сукупність розпізнаних об'єктів повітряного удару з ієрархічними цілями операції (бойових дій), які на підставі аналізу розвідувальних даних розкриють замисел дій ПП.

### **Виклад основного матеріалу дослідження**

Розпізнавання замислу дій ПП є найбільш складною та слабо структурованою задачею, яка стоїть перед ОПР в ході підготовки та веденні бойових дій. На теперішній час її рішення лежить в площині емпіричних знань людини, що на основі отриманої різномірної інформації і власного досвіду та інтелекту, викриває замисел його дій. Однак, розвиток методів штучного інтелекту для рішення слабо структурованих задач, а також використання теорії нечітких множин дозволило реалізувати задачу розпізнавання замислу дій ПП у складі системи підтримки прийняття рішення (СППР).

Побудова повітряного угруповання противника здійснюється у відповідності з відомими законами збройної боротьби, виходячи з обраної мети удару та порядку досягнення даної мети. Саме тому розпізнавання мети дій засобів повітряного нападу (ЗПН) противника зводиться до визначення порядку його дій, виходячи з відомої інформації, яка може бути отримана різними засобами з різних джерел. Для ОПР важливо, щоб ця інформація була заданого рівня достовірності, але це не завжди можливо забезпечити.

Прийняття рішення щодо розпізнавання замислу дій ПП відноситься до класу задач

прийняття рішення в умовах природної і поведінкової невизначеності. Природна невизначеність передбачає аналіз подій, які не носять масового характеру, тому не можуть бути описаними імовірнісними законами, а ситуації, що розглядаються при підготовці й прийнятті рішень, як правило, є унікальними. Такі ситуації, явища та події необхідно враховувати при прийнятті рішення, тому що застосування детермінованих методів теорії дослідження операцій може привести до значних помилок.

Таким чином, при організації процесу управління виникає протиріччя між необхідністю обробки інформації з нестохастичною (природною і поведінковою) невизначеністю та відсутністю ефективних методів її обробки для забезпечення прийняття рішень, що спрямовані на раціональне виконання поставлених бойових задач. Отже, в процесах підготовки й прийняття рішень виникає задача – розроблення методики розпізнавання замислу дій ПП з застосуванням СППР, яка дозволить приймати раціональні за ефективністю бойових дій рішення з врахуванням існуючих ресурсних обмежень на ведення бойових дій.

Це призводить до того, що розпізнавання здійснюється або тільки на основі суб'єктивних оцінок ОПР або з використанням результатів розв'язання окремих інформаційно-розрахункових завдань, що не дозволяють в повному обсязі врахувати складність динамічної повітряної обстановки. При цьому результати аналітичної роботи відповідних органів управління на етапі планування бойових дій в алгоритмах КЗА не враховуються. Забезпечення необхідного рівня автоматизації процесів розпізнавання варіантів дій ПП утруднено і тим, що в ході бойової роботи ОПР використовують в основному власні знання і досвід, які важко формалізуються. Одним з перспективних напрямків автоматизації процесів вироблення рішень є вдосконалення спеціального математичного і програмного забезпечення АСУ на основі нових інформаційних технологій. До таких технологій належать і інтелектуальні інформаційні технології створення та використання баз знань (БЗ) КЗА [5-7]. БЗ КЗА являють собою сукупність правил, фактів, механізмів виведення і програмних засобів, що описує деяку предметну область і призначені для подання накопичених в ній знань [7]. Одним з найбільш складних і основоположних етапів технології створення БЗ є етап формалізації і консолідації знань в заданій предметній області.

Використання когнітивних методів при створенні БЗ КЗА забезпечує такі можливості засобів автоматизації, завдяки яким рішення задач оцінки ПП в цілому, і зокрема задач розпізнавання варіантів його дій, обмежується в основному технічними характеристиками обчислювальних засобів. Спеціальне математичне і програмне забезпечення в КЗА з використанням БЗ відрізняється високим ступенем адаптивності до зовнішніх умов, здатністю до самонавчання,

реалізації функцій самоорганізації складних систем, що дозволяє розширити коло, автоматизовано розв'язуваних, завдань при оцінці ПП. Функції ОПР в таких системах полягають в формалізації і введенні в БЗ КЗА експертних знань на етапі підготовки КЗА до функціонування, а також у формулюванні директив і норм системи, що регламентують її поведінку.

Процес створення БЗ повністю визначається обраним методом представлення знань, тобто сукупністю методів і засобів опису, розміщення, зберігання і модифікації знань [7]. Метод представлення знань являє собою сукупність взаємозалежних способів формального опису знань і маніпулювання цими описами. Розрізняють дві групи методів представлення знань: декларативні і процедурні.

В основі когнітивних методів, використовуваних для автоматизації завдань управління, використовуються відповідні моделі подання знань. Модель представлення знань – це сукупність правил подання, опису та породження знань в БЗ. Моделі подання знань діляться на два типи: логічні та евристичні. Логічні моделі дозволяють уявити знання про завдання логіко-аналітичного, розрахункового і пошукового характеру. Однак ряд істотних недоліків (немає суворої процедури підбору аксіом для організації логічного висновку, не завжди є можливість отримання результату рішення; наявність невизначеності вихідної інформації не дозволяє організувати логічний висновок на формалізованих структурах знань) обмежують їх застосування для представлення процесу оцінки дій ПП. Евристичні моделі (мережеві, фреймові і продукційні) мають більш різноманітний набір засобів, що передають специфічні особливості предметної області, але також не дозволяють враховувати невизначеність (нечіткість) вихідних даних.

Останнім часом більшого практичного застосування знаходять моделі подання знань, засновані на нечітких множинах і нечіткої логіки [4,5]. Нечіткі множини і нечітка логіка використовуються для формалізації задач, які чинять спротив суворої формалізації, що мають логіко-аналітичний характер, а в якості вхідних

або вихідних даних мають невизначені (нечіткі) дані [5].

В даний час, в рамках дослідження математичного апарату нечітких множин та нечіткої логіки, одним з найбільш актуальних є питання, пов'язані з вивченням різних узагальнень нечітких множин, які забезпечували б формалізацію більшої кількості додаткових ступенів невизначеності в порівнянні з класичними нечіткими множинами (нечіткими множинами типу 1 (НМТ1)). За останнє десятиліття подальший розвиток в даній області отримали перш за все нечіткі множини типу 2 (НМТ2). Таким чином, в якості базової моделі представлення знань процесів розпізнавання варіантів дій ПП в умовах невизначеності визначимо НМТ2 і засновані на них нечіткі логічні системи (НЛС) інтервального типу 2 (НЛС ІТ2).

### Висновки й перспективи подальших досліджень

Таким чином, одним з основних етапів оцінки ПП в ході ведення бойових дій є розпізнавання варіантів його дій при відбитті ударів. Невизначеність і динамічність повітряної обстановки, тимчасові обмеження, значні обсяги інформації, що характеризують дії ПП, які не задані чітко і є суперечливими, зумовлюють зростання вимог до рівня обґрунтованості та оперативності розпізнавання варіантів дій ПП на ПУ Повітряних Сил. Одним з напрямків виконання вимог є автоматизація процесів розпізнавання. При цьому перспективним напрямком підвищення рівня автоматизації оперативності та достовірності розпізнавання є використання інтелектуальних інформаційних технологій. На даний момент відсутні методи формалізації знань в досліджуваній предметній області, що, в свою чергу, визначає необхідність вдосконалення технології, яка забезпечила б виконання вимог щодо засобів формалізації знань, засобів програмної реалізації БЗ.

В якості моделі представлення знань процесів розпізнавання варіантів дій ПП в умовах невизначеності визначені НМТ2 і засновані на них НЛС ІТ2, що дозволяють формалізувати завдання, що не піддаються суворої формалізації і мають логіко-аналітичний характер.

### Література

1. Alimpiev A. Selecting a model of unmanned aerial vehicle to accept it for military purposes with regard to expert data Eastern-European. *Journal of Enterprise Technologies*. 2017. Vol. 1, No. 9(85). P. 53-60.
2. Даник Ю.Г., Пермяков О.Ю. Сучасні інформаційні технології в забезпеченні національної безпеки і оборони. *Сучасні інформаційні технології у сфері безпеки і оборони*. 2018. С.159-174.
3. Command and Control of Joint Air Operations. Joint Publication/3-3010, February 2014.
4. Королюк Н.О., Першин О.В., Грідньова Т.О., Шевченко С.О. Обґрунтування сучасного підходу щодо автоматизації процесів прийняття рішень по управлінню авіацією. *Збірник наукових праць*. 2019. №1(59). С.32-39.
5. Королюк Н.О., Корольов Р.В., Коршець О.А. Процедура формалізації даних, які використовуються при описі процесу управління рухом повітряних об'єктів. *Збірник наукових праць ХНУПС*. 2017. № 4(53). С.103-106.
6. Камінський В.В., Тюрін В.В., Камінський В.В., Коршець О.А., Королюк Н.О. Аналіз застосування безпілотних літальних апаратів в сучасних збройних конфліктах та АТО на Сході України. *Наука і оборона*. 2017. № 3(4). С.4-8.
7. Субботин С.А., Олейник А.А., Гофман Е.А. Интеллектуальные информационные технологии проектирования автоматизированных систем диагностирования и распознавания образов: монография. Харьков: ООО «Компания Смит». 2016. 317 с.

ПОДХОД ПО АВТОМАТИЗАЦИИ ПРОЦЕССОВ ОЦЕНКИ ВОЗДУШНОГО ПРОТИВНИКА НА ПУНКТАХ УПРАВЛЕНИЯ ВОЗДУШНЫХ СИЛ ВСУ

Александр Юрьевич Пермяков (доктор технических наук, профессор)<sup>1</sup>  
Наталья Александровна Королюк (кандидат технических наук)<sup>2</sup>  
София Александровна Маслиева<sup>2</sup>

<sup>1</sup> *Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*  
<sup>2</sup> *Харьковский национальный университет Воздушных Сил имени И.Кожедуба, Харьков, Украина*

В статье предложенный подход по совершенствованию специального математического и программного обеспечения АСУ для решения задачи распознавания замысла воздушного противника на основе новых ин-формационных технологий создания и использования баз знаний. Рассматривается процесс распознавания замысла действий воздушного противника в качестве слабо структурированной задачи, которая стоит перед лицом, принимающим решение, в ходе подготовки и ведения боевых действий. Обоснованно для решения слабо структурированной задачи использование теории нечетких множеств, что позволяет решить задачу распознавания замысла действий воздушного противника в составе системы поддержки принятия решения. В качестве базовой модели представления знаний процессов распознавания вариантов действий воздушного противника в условиях неопределенности обосновано нечеткое множество типа 2 и основана на ней нечеткая логическая система, что позволяет формализовать задания, которые не поддаются формализации и имеют логико-аналитический характер. Использование когнитивных методов при создании баз знаний обеспечивает возможность средствам автоматизации помочь решению задачи распознавания вариантов действий противника, которая ограничивается в основном техническими характеристиками вычислительных средств.

**Ключевые слова:** распознавание замысла воздушного противника, нечеткое множество типа 2, нечеткая логическая система, система поддержки принятия решения.

APPROACH ON THE AUTOMATION OF AIRCRAFT OWNER'S EVALUATION PROCESSES AT THE POINTS OF MANAGEMENT OF THE AIR FORCE

Aleksandr Permakov (Doctor of technical sciences, Professor)<sup>1</sup>  
Natalia Korolyuk (Candidate of technical sciences, associate professor)<sup>2</sup>  
Sofia Masliova<sup>2</sup>

<sup>1</sup> *National defence University of Ukraine named after Ivan Chernyakhovsky, in Kiev, Ukraine*  
<sup>2</sup> *Kharkiv national Air Forces named after I. Kozhedub, Kharkiv, Ukraine*

In the article offered approach in relation to perfection of special mathematical and programmatic за-безпечення ASC for the decision of task of recognition of intention of air opponent on the basis of new informative technologies of creation and use of bases of knowledge. The process of recognition of to intention actions of air opponent is examined as the poorly structured task, that stands before a person that makes decision, during preparation and conduct of battle actions. Reasonably for a decision poorly of task of the use of theory of fuzzy sets, that allows the to untie task of recognition of intention of actions of air opponent in composition the system of support of decision-making. As a base model of representation of knowledge of processes of recognition of variants of actions of air opponent in the conditions of vaguenesses a fuzzy set is reasonable as 2 and the unclear logical system is based on her, that allows to formalize tasks that does not yield severe formalization and have analytical character. Using of logical methods for creation of bases of knowledge provides possibility to facilities of automations in relation to the decision of task of estimation of air opponent on the whole, and in particular tasks of recognition of his actions, that is limited to mainly technical descriptions of computing facilities.

**Keywords:** recognition of intention of air opponent, fuzzy set as 2, unclear logical system, system of support of decision-making.

References

1. Alimpiev A. Selecting a model of unmanned aerial vehicle to accept it for military purposes with regard to expert data Eastern-European. *Journal of Enterprise Technologies*. 2017. Vol. 1, 9(85). R. 53-60. 2. Danyk Ju.Gh., Permjakov O.Ju. Suchasni informacijni tekhnologhiji v zabezpechenni nacionaljnoji bezpeky i oborony. *Suchasni informacijni tekhnologhiji u sferi bezpeky i oborony*. 2018. S.159-174. 3. Command and Control of Joint Air Operations. Joint Publication/3-3010, February 2014. 4. Koroljuk N.O., Pershyn O.V., Ghridnjova T.O., Shevchenko S.O. Obghruntuvannja suchasnogho pidkholdu shhodo avtomatyzacijni procesiv pryjnattja rishenj po upravlinnju aviacijeju. *Zbirnyk naukovykh pracj*. 2019. №1(59). S.32-39.

5. Koroljuk N.O. Koroljov R.V., Korshej O.A. Procedura formalizacijni danykh, jaki vykorystovujutsja pry opysi procesu upravlinnja rukhom povitrtjanykh ob'ektiv. *Zbirnyk naukovykh pracj KhNUPS*. 2017. 4(53). S.103-106. 6. Kaminsjkij V.V., Tjurin V.V., Kaminsjkij V.V., Korshhej O.A., Koroljuk N.O. Analiz zastosuvannja bezpilotnykh litalnykh aparativ v suchasnykh zbrojnykh konfliktakh ta ATO na Skhodi Ukrajinjy. *Nauka i oborona*. 2017. 3(4). S.4-8. 7. Subbotyn S.A., Olejnyk A.A., Ghofman E.A. Yntellektualnye ynformacyonnye tekhnologhyy proektyrovannja avtomatyzirovannykh system dyaghnostyrovannja y raspoznavannja obrazov: monoghrafija. Kharjkov: OOO «Kompanija Smyt». 2016. 317 s.

*Дмитро Анатолійович Чопа* (кандидат технічних наук, с.н.с.)<sup>1</sup>  
*Анатолій Йосипович Дерев'янчук* (кандидат технічних наук, професор)<sup>2</sup>  
*Наталія Миколаївна Козир*<sup>3</sup>

<sup>1</sup>Національний університет оборони України імені Івана Черняхівського, Київ, Україна

<sup>2</sup>Сумський державний університет, Суми, Україна

<sup>3</sup>Науково-дослідний центр Ракетних військ і артилерії, Суми, Україна

## ОСНОВНІ ІННОВАЦІЙНІ НАПРЯМИ ЗАСТОСУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ ВІЙСЬКОВИХ ФАХІВЦІВ

Застосування Збройних Сил України в сучасних умовах обумовлює нові вимоги до організації навчання та підготовки військових фахівців. Існує нагальна потреба в розробленні нових технологій навчання, підвищенні рівня засвоєння навчального матеріалу та удосконаленні способів контролю його засвоєння. Тому в статті на основі досвіду кафедри військової підготовки Сумського державного університету наводяться основні інноваційні напрями застосування інформаційних технологій у підготовці військових фахівців (на прикладі фахівців РВ і А). А саме, ця стаття присвячена створенню мультимедійних віртуальних тренажерів (симуляторів), моделюванню навчальних ігор, розробленню системи автоматизованої оцінки знань та розробленню інформаційно-дистанційно-тренажерної системи навчання. Автори статті продовжують ділитися власним досвідом щодо концепції застосування сучасних методів викладання військово-технічних дисциплін з метою подальшого їх обговорення, розвитку та впровадження в освітній процес ВВНЗ.

**Ключові слова:** інформаційні технології, мультимедійні віртуальні тренажери (симулятори), навчальні ігри, система автоматизованої оцінки знань, інформаційно-дистанційно-тренажерна система навчання.

### Вступ

Дану статтю слід розглядати як подальший аналіз технічних основ розвитку сучасних методів викладання військово-технічних дисциплін (ВТД), які були сформульовані та висвітлені у роботах [1-2].

**Постановка проблеми.** Традиційні методи підготовки фахівців РВ і А вже не можуть певною мірою забезпечувати виконання ними бойових завдань, використання озброєння та військової техніки (ОВТ) за призначенням. Це змушує безперервно вести пошук нових технологій у вивченні ВТД на фоні зростаючого постачання нових зразків ОВТ у війська.

Як свідчить досвід локальних війн і збройних конфліктів минулого, проведення ООС (АТО) на сході України, підготовлені на високому технічному рівні підрозділи вели бойові дії з малими втратами особового складу і ОВТ.

Із наведеного вище випливає пріоритетне завдання, на основі визначених інноваційних напрямів застосування сучасних інформаційних технологій створити новітню систему вивчення ВТД, яка б забезпечувала комплексну підготовку фахівців з теоретичних знань і практичних навиків.

**Мета і актуальність** статті полягає у подальшому розвитку інноваційних напрямів застосування інформаційних технологій, що у підсумку створить комплексну систему якісної підготовки військових фахівців.

### Виклад основного матеріалу дослідження

У роботі [1] розглянуто перші три інноваційні напрями застосування сучасних інформаційних технологій у викладанні ВТД.

Пропонуються до розгляду і осмислення наступні чотири інноваційні напрями, саме: розроблення мультимедійних віртуальних тренажерів (симуляторів); моделювання навчальних ігор; розроблення системи автоматизованої оцінки знань; розроблення інформаційно-дистанційно-тренажерної системи навчання.

*Інноваційний напрям 4.* Розроблення мультимедійних віртуальних тренажерів (симуляторів).

Загальновідомо, що в особливий період в країні, коли йдуть бойові дії на сході, різко збільшилося ОВТ, яке потребує ремонту, відновлення. Відомо також, що військові фахівці і персонал ремонтних органів ще не мають потрібної кваліфікації для поводження з ОВТ та його ремонту і відновлення, що в свою чергу, висуває завдання розроблення та впровадження спеціалізованих комп'ютерних (віртуальних) тренажерів, застосування яких підвищить кваліфікацію як фахівців, так і персоналу, що обслуговує ОВТ, зменшить витрати на закупівлю дорогої техніки та ЗІП до неї, а обслуговуючий

персонал зможе отримувати навички поведінки у нештатних ситуаціях тощо. Практичні заняття допомагають відпрацьовувати отримані навички у безпечному віртуальному середовищі. Віртуальні тренажери надають можливість обрати не тільки індивідуальний підхід до навчання, але й зручний і гнучкий режим заняття. При розробці віртуальних тренажерів необхідно враховувати наступне [2]: інтерфейс повинен бути максимально наближений до реальних зразків озброєння (пульти, щитки управління, ключі, ЗІП, механізми тощо); динамічна модель (3D модель) повинна враховувати основні реальні процеси взаємодії вузлів і механізмів ОВТ; всі додатки повинні бути прості і гнучкі; інструктору (керівнику заняття) надана можливість змінювати сценарій шляхом введення нештатних ситуацій; тренажер повинен робити аналіз і оцінку дій фахівця.

Так, розроблений нами тренажер, може використовуватися у наступних режимах: читання і огляд матеріалу; пошук потрібних матеріалів;

друкування матеріалів (за бажанням замовника); перевірка знань; перегляд довідникового матеріалу.

У режимі читання користувач переглядає текстову частину обраного питання. Доступ до матеріалів стосовно іншого питання реалізується у вигляді гіперпосилання на графічні елементи або інші текстові розділи. Натиснувши на гіперпосилання, в окремому вікні відкривається відповідний текст, графічний або відео матеріал.

Процес навчання із використанням віртуального тренажера показано на схемі (рис. 1). Такий комп'ютерний тренажер містить в собі сукупність програмних і апаратних засобів, що дозволяє здійснювати процес навчання без посередньої взаємодії фахівця і реального зразка озброєння. Апаратні можливості тренажера – це сучасний персональний комп'ютер, оснащений якісними пристроями вводу (виводу) інформації.



Рис. 1. Спрощена схема принципу роботи віртуального тренажера

Програмний засіб – це математично обґрунтована віртуальна модель, що містить в собі систему графічної візуалізації, звуковий супровід і текстову інформацію.

Ми пропонуємо декілька різновидів тренажерів різних за своєю сутністю та складністю. На рис. 2,3 надані зразки віртуальних тренажерів (зі складання бойових зарядів та затвору 122-мм гаубиці Д-30 відповідно).



Рис. 2. Тренажер зі складання бойового заряду у робочому стані



Рис. 3. Приклад практичного модуля (затвор) 122-мм гаубиці Д-30

Зазначені віртуальні тренажери працюють за єдиним алгоритмом, що представлений на рис.4.

*Інноваційний напрям 5. Моделювання навчальних ігор.*

Навчальна гра – це гра, що призначена навчити студентів щодо певного предмету та набути ними майстерності, а також це інтерактивна гра, яка навчає їх цілям, правилам, адаптації, вирішенню проблем, взаємодії.



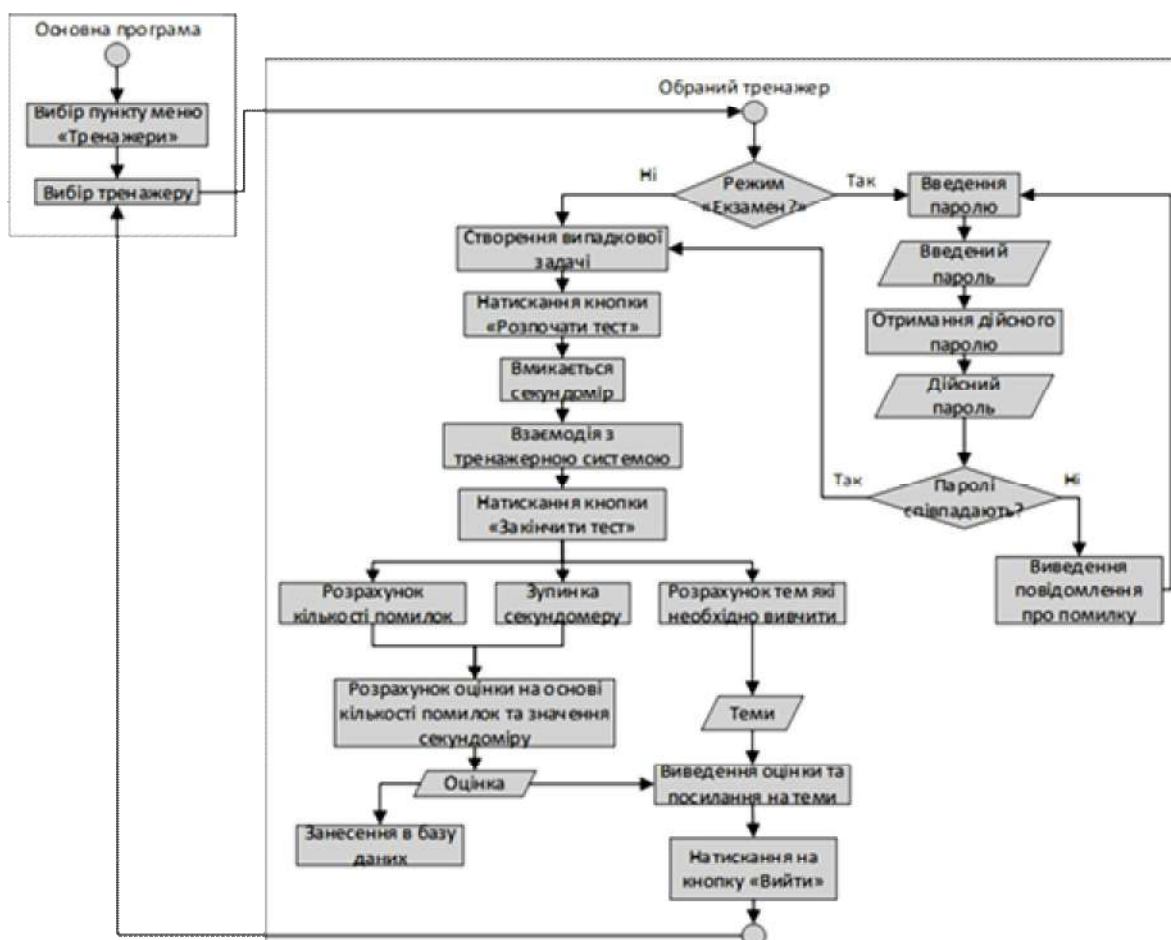


Рис. 4. Блок-схема алгоритму роботи віртуального тренажера

Такі ігри задовольняють основну потребу в навчанні, забезпечуючи зацікавленість, пристрасну участь, мотивацію, соціальну взаємодію та емоції в ході гри та, в той же час, навчання продовжується.

Військові завжди були користувачами або розробниками інноваційних технологій моделювання. Характер військових місій вимагає, щоб вони репетували їх дуже часто для того, щоб краще зрозуміти їх складні взаємодії та оцінити результати. Ця потреба призвела до застосування моделювання низки різних заходів, використання комп'ютерних технологій в сфері навчання та використання навчальних ігор.

Прикладом використання навчальних ігор є програма, що поєднує у собі інтелектуальну гру "філворд" з 3D моделюванням (використанням реалістичних 3D моделей ОБТ).

Завданням користувача програми є збирання на ігровому полі слова за правилами гри "філворд". Наступним кроком користувачу поруч з полем буде показана 3D модель слова, що було тільки-но зібране. Така послідовність дій пов'язує вербальну пам'ять із зоровою, що, в свою чергу, дозволяє покращити якість та швидкість навчання, запам'ятовування назв окремих деталей.

Дана комп'ютерна програма дозволяє непомітно для користувача продовжити навчання навіть під час відпочинку, зменшити час для отримання інформації, сформуванню термінологічну грамотність студентів, підвищити зацікавленість у

навчальному матеріалі, може візуалізувати об'єкт вивчення (за його фізичної відсутності).

В її основу покладено алгоритм, зображений на рис. 5.

Об'єднавши методику навчальних ігор з комп'ютерними технологіями, а саме, електронним додатком, отримуємо потужний механізм навчання з такими вагомими перевагами: уникнення шаблонності побудови "філворду"; швидкість навчання (зібравши слово користувач побачить реалістичну 3D модель), тим самим використовується як зорова, так і вербальна пам'ять; кросплатформеність – програма однаково добре працює як на ПЕОМ, так і на смартфоні.

В програмі наданий рівень-словник, тобто якщо користувач лише хоче згадати як виглядає або називається той чи інший об'єкт, дізнатися точну будову деталі (особливо за її відсутності або недоступності) йому не доведеться грати знову і знову для отримання потрібного слова. Достатньо лише знайти у "Бібліотеці" потрібний об'єкт (слово).

Результатом впровадження ігрових методів навчання є підвищення мотивації до вивчення дисципліни; підвищення якості запам'ятовування та утримання інформації.

Приклад ігрового поля зображено на рис. 6.

Авторська методика спирається на поєднанні зорової та вербальної пам'яті користувача. Ігрове поле має формальний поділ на 2 зони. Перша з яких присвячена "філворду", а друга є полем для

3D моделей. Спеціально створений алгоритм, що в основу своєї логіки дій бере випадкову генерацію чисел, буде поле “філворда” повністю унеможливлючи повторення положення слів відносно генерованих ігрових полів попередньої сесії. Користувач повинен зібрати, за правилами

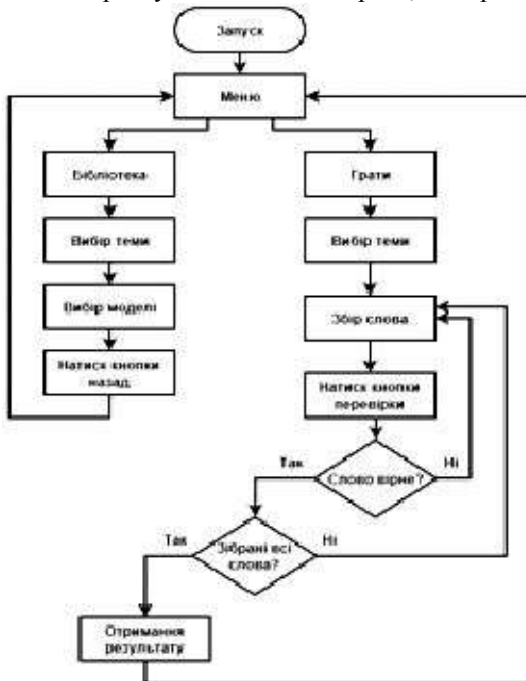


Рис. 5 Алгоритм програми



Рис. 6. Варіанти матриці ігрового поля: (обране слово-екстрактор)

Саме цей момент зв'язує в пам'яті студента слово з його предметом.

*Інноваційний напрям 6.* Розроблення системи автоматизованої оцінки знань.

Наступним кроком до подальшого вдосконалення програмних продуктів стало дослідження засвоєння рівня навчального матеріалу студентами, де використовувались власні розроблені мультимедійні засоби навчання (МЗН). Була розроблена система автоматизованої оцінки якості знань (далі – система оцінки). Створена система оцінки містить в собі увесь навчальний матеріал, який використовується у МЗН, таким чином, що робота з системою оцінки якості знань збільшує ще на певний відсоток кількість інформації, що запам'ятовується, через використання принципу “повторюваності”. Відповідаючи на запитання в системі оцінки, слухач візуально на екрані бачить той самий матеріал, що і у МЗН, відповідно до обраної теми.

“філворду”, слово та підтвердити свій вибір. Якщо слово, що повинно бути назвою предмета, деталі, котру потрібно запам'ятати, справді існує то поруч з ігровим полем “філворду” з'явиться реалістична 3D модель цього предмета (рис.7).



Рис. 7. Загальний вигляд 3D моделі екстрактора

Аналіз результатів дослідження показав не тільки підвищення рівня засвоєння навчального матеріалу, але й посилення мотивації студентів.

Саме це сприяло створенню системи оцінки, де поєднувалися програмні продукти навчально-методичних матеріалів, а саме: комп'ютерні презентації ілюстративного характеру і електронні посібники, словники – довідники, і електронні тренажери, тестові системи, самовчителі, а користування ними викликало інтерес у студентів.

Загальна схема системи оцінки і взаємодії між його складовими подана на рис. 8.

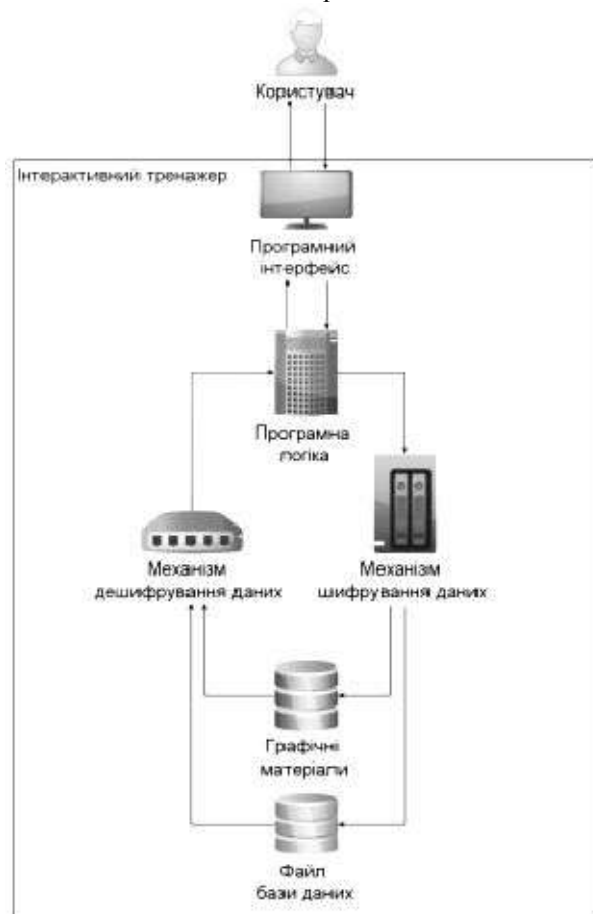


Рис. 8. Структура системи автоматизованої оцінки якості знань

На рисунку зображено процес проведення оцінювання з використанням системи оцінки. Це – студенти, які отримують певні знання та готуються до їх перевірки, комп'ютер із встановленою програмою, за допомогою якої система оцінки та слухачі обмінюються інформацією у діалоговому режимі, та, власне, сама система оцінки якості знань. За допомогою стрілок вказані напрями обміну інформацією між цими складовими. Розроблена система автоматизованої оцінки знань поєднує у собі можливості мультимедійного посібника та тренувального додатка. Її застосування дозволяє суттєво підвищити рівень засвоєності матеріалу слухачами та перевірити їх знання за пройденими розділами. Простота користування та функціональність роблять систему оцінки однією з найкращих на ринку подібних програмних засобів, а якісні ілюстрації та відеоролики до матеріалу забезпечують високий конкурентоздатний рівень. Серед основних можливостей відзначимо наступні: легкий і

зрозумілий інтерфейс; наявність “живих” ілюстрацій, анімацій та відеороликів до поставлених питань; влаштована система оцінювання знань; захищений файл-сховище даних, які використовує програма; наявність вбудованого редактора контрольних питань, що надає можливість додавати та змінювати існуючі питання; прозора система оцінювання знань студентів; наявність вбудованих підказок та посилань на навчальні матеріали курсу дисциплін; збереження детальної інформації про результати проходження тесту студентами; вбудована система аналізу помилок; для встановлення та роботи програми не потрібні жодні сторонні додатки; система оцінки поєднує в собі ретельно підібрані запитання, якісні і яскраві ілюстрації, відеоролики та сучасні технології роблять її справжньою знахідкою для будь-якого військового навчального закладу.

Блок-схема алгоритму роботи програми зображена на рис. 9.

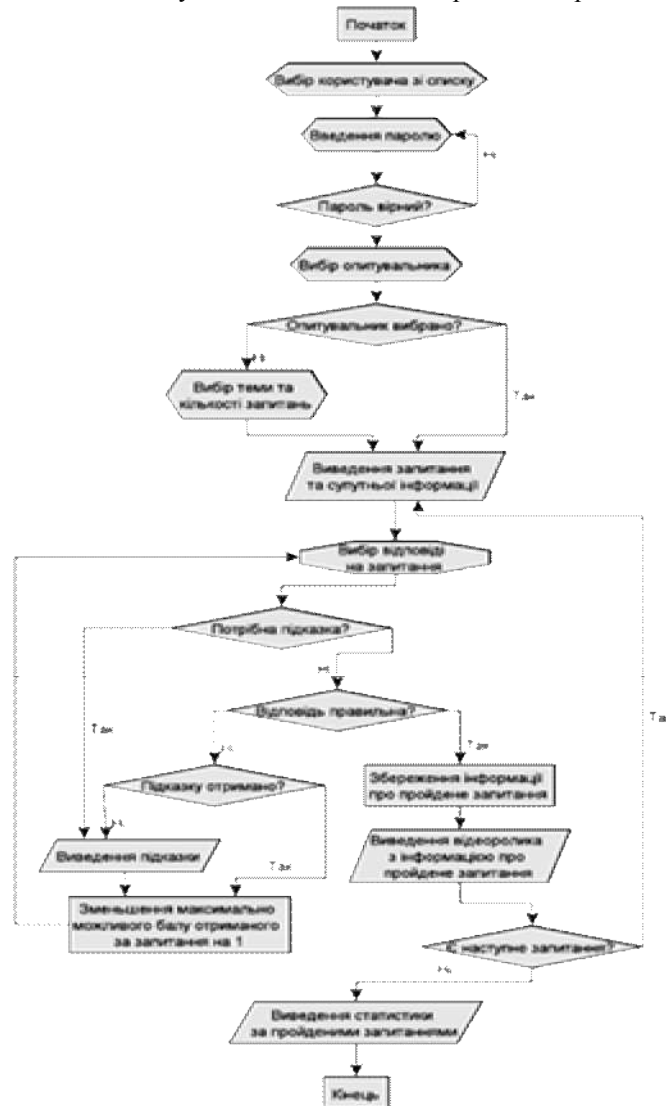


Рис. 9. Блок-схема алгоритму роботи системи оцінки знань

Аналіз успішності слухачів з різною загально-інженерною підготовкою наведені на рис. 10, з якого можна зробити висновок щодо доцільності використання розробленої системи автоматизованої оцінки якості знань.

При чому, аналіз проводить система оцінки, відповідно до співвідношення правильних відповідей на запитання наданих слухачам, та в автоматичному режимі будує діаграму успішності.

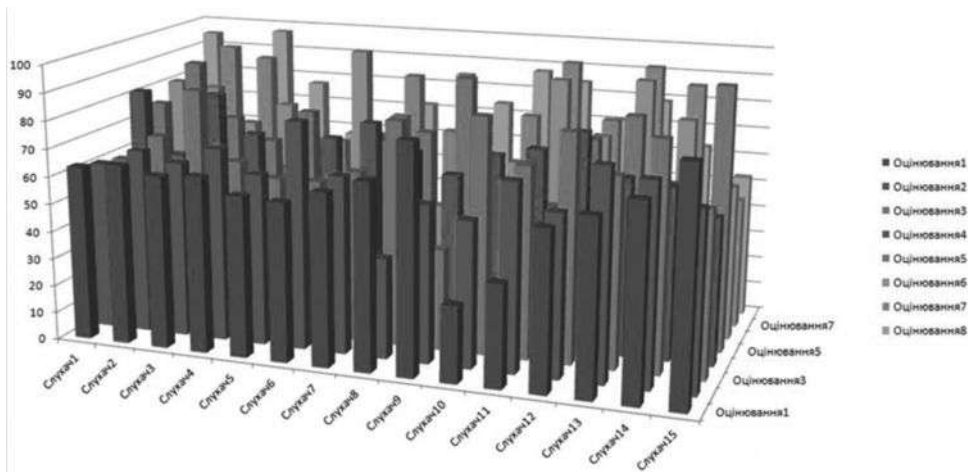


Рис. 10. Діаграма успішності рівня засвоєння теоретичних знань і практичних навиків

Таким чином, виходячи із викладеного і результатів дослідження, можна стверджувати, що впровадження системи оцінки у навчальний процес в системі підготовки військових фахівців має високу ефективність, а зменшення навантаження на викладача та можливість забезпечувати діалоговий режим у процесі вирішення конкретних питань роблять їх дуже корисними не тільки для ВВНЗ, а й для навчальних центрів, командирів військових частин і підрозділів.

*Інноваційний напрям 7.* Розроблення інформаційно-дистанційно-тренажерної системи навчання.

Немає сумніву в тому, що впровадження технологій дистанційного навчання у ВВНЗ на теперішній час займає пріоритетний напрямок. Ця теза підтверджується тим, що у листопаді 2018 року у Києві відбулася перша міжнародна

науково-практична конференція, присвячена проблемам впровадження дистанційного навчання під егідою Інституту Джефферсона (США) [3]. Це стосується також військових кафедр і факультетів, що готують офіцерів запасу. Таке пояснюється тим, що матеріально-фінансові можливості студентів, що мешкають за межами навчальних закладів, обмежені як за часом, так і відсутністю навчальних зразків ОВТ. Основною проблемою у підготовці фахівців є неможливість відпрацювання практичних питань (здобуття практичних навиків).

Для усунення таких недоліків автори розробили класичну систему, що дозволяє отримувати знання самостійно користувачами, використовуючи мережу Internet, базу даних, що зберігає на сервері навчальний контент. Така схема отримала назву інформаційно-дистанційно-тренажерна система (ІДТС) (рис. 11).

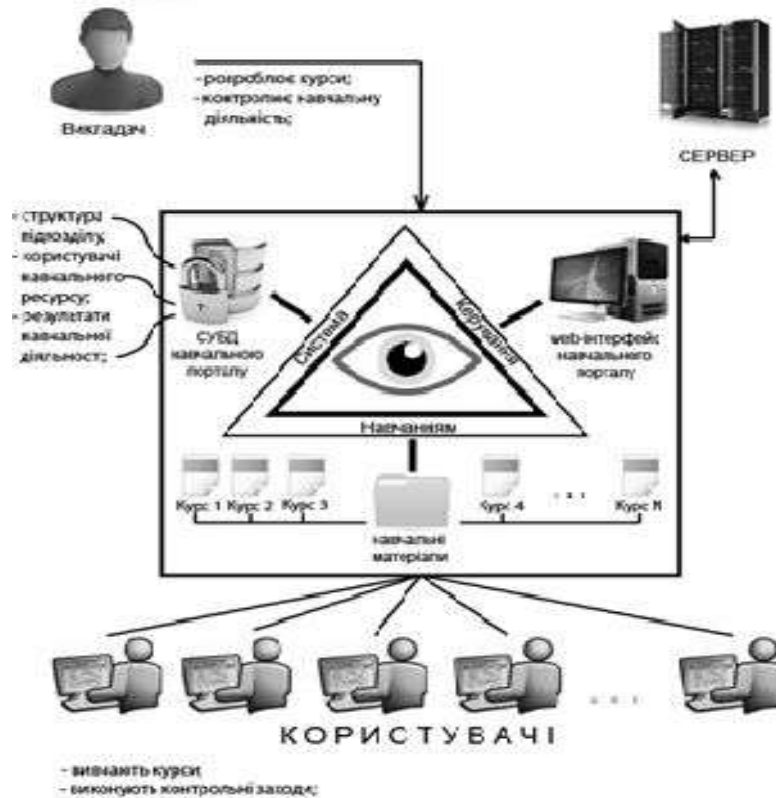


Рис. 11. Інформаційно-дистанційно-тренажерна система

У більшості випадків навчальний контент таких систем – це набір навчальних матеріалів розроблених засобами Microsoft Office у текстовому або презентаційному вигляді та набір контрольних тестів, питань для перевірки вивченого матеріалу. З метою заохочення та мотивації засвоєння навчального контенту автори ввели кросворди, філворди та інші матеріали, що знімають загальні напруження, в той же час, спонукають до подальшого вивчення, викликаючи інтерес.

Основою ІДТС є розроблені відеофільми та відеоролики на основі 3D моделювання, анімації дії вузлів ОВТ, боеприпасів тощо.

Із викладеного вище випливає нагальна необхідність мотиваційних зусиль щодо підготовки фахівців з бажання прискорити процес навчання, удосконалити набуті навички, довести виконання операцій до автоматизму. Меню навчального контенту представлено на рис.12.



Рис. 12. Меню навчальної контенту

Порівнювальна характеристика рівня знань в залежності від тривалості застосування 3D моделювання на заняттях представлена на рис. 13.

З рисунку видно, що для застосування 3D-моделей на планових заняттях оптимальним часом є 30-60 хвилин і 15-45 хвилин на самостійній підготовці. Подальше зниження рівня засвоєння на планових заняттях і самостійній підготовці пояснюється стомленістю студентів за причини отримання великого обсягу інформації.

Отже, основним завданням ІДТС є подальше

### Література

1. Дерев'янчук А.Й., Чопа Д.А., Дегтярьов В.В., Семенов Ф.Д. Кейс - метод як форма інтерактивного навчання з військово - технічних дисциплін при підготовці фахівців ракетних військ і артилерії. Сучасні інформаційні технології в сфері безпеки та оборони. НУОУ. 2019. №1(34). 2. Дерев'янчук А.Й., Чопа Д.А., Дегтярьов В.В. Інформаційні технології як технічна основа розвитку сучасних методів викладання військово-технічних дисциплін. Сучасні інформаційні технології в сфері безпеки та оборони. НУОУ. 2019.

наповнення платформи новими матеріалами як власних розробок, так і інших ВВНЗ.

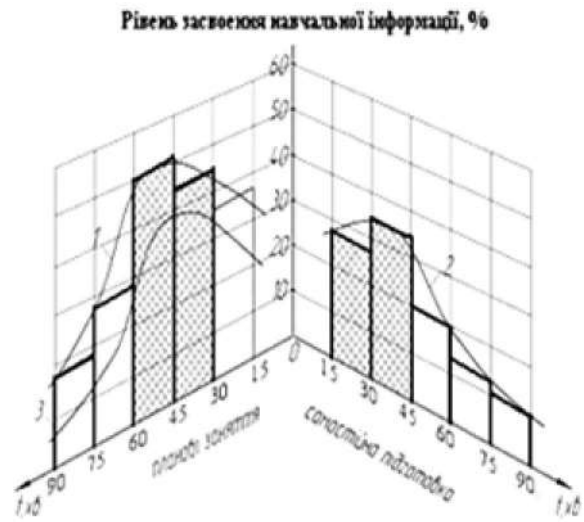


Рис. 13. Порівняльна характеристика рівня знань залежно від тривалості застосування 3D моделювання

На рис. 13 криві 1,2 відображають результати навчального процесу із використанням 3D моделювання на планових заняттях і самостійній підготовці відповідно, крива 3 – при відсутності у самостійній підготовці застосування 3D моделювання.

### Висновки і перспективи подальших досліджень

Таким чином, у статті завершено розгляд основних інноваційних напрямів застосування інформаційних технологій у викладенні ВТД. Результати досліджень дозволяють зробити висновок щодо доцільності створення комплексу новітніх методик. Впровадження інформаційних технологій як технічної основи подальшого розвитку сучасних методів викладання військово-технічних дисциплін дозволяє значно підвищити не тільки теоретичні знання, а й практичні навички.

Подальші дослідження вбачаємо у розширенні і наповненні вказаних методик сучасним контентом та їх удосконаленням, в розробленні тренажерів віртуальної реальності.

№2(35). 3. Образцов И.В., Белов В.В. Виртуальные тренажеры в практике технического образования URL:<http://cdokp.tstu.tver.ru/site.services/download.aspx?act1&did=89791&dbid>. 4. Перша міжнародна науково-практична конференція. Проблеми впровадження дистанційного навчання в освітньому процесі вищих військових навчальних закладів та можливі шляхи їх вирішення. Збірник матеріалів 1-ої міжнародної науково-практичної конференції. Київ, 2018.

### ОСНОВНЫЕ ИННОВАЦИОННЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПОДГОТОВКЕ ВОЕННЫХ СПЕЦИАЛИСТОВ

Дмитрий Анатольевич Чопа (кандидат технических наук, с.н.с.)<sup>1</sup>  
Анатолий Йосипович Деревьянчук (кандидат технических наук, профессор)<sup>2</sup>  
Наталья Николаевна Козырь<sup>3</sup>

<sup>1</sup>Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

<sup>2</sup>Сумської державний університет, Суми, Україна

<sup>3</sup>Научно-исследовательский центр Ракетных войск и артиллерии, Суммы, Украина

Применение Вооруженных Сил Украины в современных условиях обуславливает новые требования к организации обучения и подготовки военных специалистов. Существует настоятельная необходимость в разработке новых технологий обучения, повышении уровня усвоения учебного материала и совершенствовании способов контроля его усвоения. Поэтому в статье на основе опыта кафедры военной подготовки Сумского государственного университета приводятся основные инновационные направления применения информационных технологий в подготовке военных специалистов (на примере специалистов РВ и А). В частности, эта статья посвящена созданию мультимедийных виртуальных тренажеров (симуляторов), моделированию учебных игр, разработке системы автоматизированной оценки знаний и созданию информационно-дистанционно-тренажерной системы обучения. Авторы статьи продолжают делиться собственным опытом концепции применения современных методов преподавания военно-технических дисциплин с целью дальнейшего их обсуждения, развития и внедрения в образовательный процесс ВВУЗ.

**Ключевые слова** информационные технологии, мультимедийные виртуальные тренажеры (симуляторы) обучающие игры; системы автоматизированной оценки знаний; информационно-дистанционно-тренажерная система обучения.

## GENERAL INNOVATIVE DIRECTIONS OF THE USE OF MODERN INFORMATION TECHNOLOGIES IN THE TRAINING OF MILITARY SPECIALISTS

Dmitro Chopa (Candidate of technical sciences, Senior Research Fellow)<sup>1</sup>  
Anatolii Derevianchuk (Candidate of technical sciences, professor)<sup>2</sup>  
Natalya Kozyr<sup>3</sup>

<sup>1</sup>National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

<sup>2</sup>Sumy State University, Sumy, Ukraine

<sup>3</sup>Artillery Research Center, Sumy, Ukraine

The use of the Armed Forces of Ukraine in modern conditions stipulates new requirements for the organization of education and training of military specialists. There is an urgent need to develop new learning technologies, increase the level of learning material and improve ways to control its learning. Therefore, in the article, based on the experience of the department of military training of Sumy State University, the main innovative directions of the use of information technologies in the training of military specialists are given (for example, artillery specialists). In particular, this article is devoted to the creation of multimedia virtual simulators (simulators), the simulation of educational games, the development of an automated knowledge assessment system and the creation of information and distance learning equipment. The authors of the article continue to share their own experience of the concept of applying modern methods of teaching military-technical disciplines for the purpose of further discussing them, developing and introducing them into the educational process of the higher military educational establishment.

**Keywords:** information technology, multimedia virtual simulators (simulators) educational games; automated knowledge assessment systems; information and distance learning system of training.

## References

1. Derevyanchuk A., Chopa D., Dehtiarov V., Semenov F. (2019). Keis - metod yak forma interaktyvnoho navchannia z viiskovo - tekhnichnykh dystsyplyn pry pidhotovtsi fakhivtsiv raketnykh viisk i artylerii [Case-method as a form of interactive training on military-technical disciplines in preparation of artillery specialists]. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. NUOU. №1(34). 2. Derevyanchuk A., Chopa D., Dehtiarov V. (2019). Informatsiyni tehnologiyi yak tehnicna osnova rozvitku suchasnih metodiv vkladannya viyskovo-tehnicnih distsyplyn [Information technologies as a technical basis for the development of modern methods of teaching military-technical subjects]. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. NUOU. №2(35).

3. Obratsov I., Belov V. Virtualnye trenazheryi v praktike tehniceskogo obrazovaniya [Virtual simulators in the practice of technical education] URL:<http://cdokp.tstu.tver.ru/site.services/download.aspx?act=1&did=89791&dbid=marcmain>. 4. The first international scientific-practical conference (2018). Problemi vprovadzhennya distantsiynogo navchannya v osvltnomu protsesi vischih vlyskovih navchalnih zakladiv ta mozhlivl shlyahi Yih virlshennya. [Problems of introduction of distance learning in the educational process of higher military educational establishments and possible ways of solving them]. Collection of materials of the 1st international scientific-practical conference. Kyiv.

*Борис Леонідович Бутвін (доктор технічних наук, професор)*

*Олександр Олександрович Машкін (кандидат технічних наук, с.н.с.)*

*Олексій Іванович Соломицький (кандидат технічних наук, с.н.с.)*

*Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна*

## МЕТОД РОЗРАХУНКУ ІНТЕГРАЛЬНОГО ПОКАЗНИКА ЯКОСТІ МОДЕЛЕЙ ТА ПОЛІМОДЕЛЬНИХ КОМПЛЕКСІВ ОПЕРАЦІЙ (БОЙОВИХ ДІЙ)

У статті розглядаються особливості оцінювання якості моделей та полімодельних комплексів операцій (бойових дій). Такі моделі є дієвим та необхідним інструментом проведення оперативних розрахунків на заходах оперативної підготовки, а процедура оцінки їх якісних властивостей – важливим та відповідальним етапом життєвого циклу. В рамках теоретичної кваліметрії розрізняють прямі та зворотні задачі оцінювання якості, в основі першої лежить безпосереднє вимірювання якості, в основі другої задачі – управління якістю продукції з метою придання йому необхідних властивостей. Особливої актуальності зворотна задача набуває для полімодельних комплексів операцій (бойових дій), які визначально будуються з гнучкою структурою, що передбачає можливість включення до їх складу нових моделей або модифікації вже існуючих. Оскільки поняття якості включає як об'єктивні властивості, так і суб'єктивні оцінки корисності об'єкту, які кваліметричними методами оцінюються одним узагальненим показником, природним є залучення до таких оцінок експертів у предметній сфері. Розвиненість апарату оброблення експертної інформації поряд з сучасними програмними засобами аналізу та оброблення даних надає можливість упорядкування процесу оцінювання якості найважливіших властивостей моделей та полімодельних комплексів. Це можливо шляхом встановлення нелінійної аналітичної залежності, яка пов'язує незалежні змінні (оброблені оцінки експертів) з залежною змінною, в ролі якої виступає інтегральна оцінка якості моделей. Приклад побудови такої залежності з високим коефіцієнтом детермінації інтегральної оцінки якості, розглянутий у статті, підтвердив доцільність такого підходу. Наявність зазначеного інструменту оцінювання якості дозволить з достатньо високою точністю розраховувати інтегральний показник якості обраних властивостей моделей, а також може бути використана для кваліметричного аналізу можливих модифікацій та структурних змін у моделях та полімодельних комплексах операцій (бойових дій).

**Ключові слова:** кваліметрія моделей; полімодельний комплекс операцій; якісна оцінка властивостей.

### Вступ

Моделі та полімодельні комплекси (ПМК) операцій (бойових дій) є дієвим та необхідним інструментом роботи органів військового управління та оперативних штабів. Оцінка якісних характеристик моделей та ПМК – важливий та відповідальний етап їх життєвого циклу, який завершує, як правило, період дослідної експлуатації моделей. За результатами такої оцінки можна зробити висновок про ступінь придатності моделей до використання за призначенням, або виявити такі їх сторони, що потребують уваги та доопрацювання.

Взагалі, чисельна оцінка та управління якістю будь-якої продукції є основою кваліметрії – науки про вимірювання та кількісну оцінку якості об'єктів та процесів. Якість, як ключове поняття кваліметрії, по відношенню до моделей та ПМК може бути визначена як «властивість або сукупність властивостей моделей, що

обумовлюють їх придатність до використання за призначенням» [1]. Важливими для уваги є декілька аспектів теоретичної кваліметрії, які безпосередньо стосуються моделей та ПМК операцій (бойових дій). Першим таким аспектом слід вважати те, що в рамках кваліметрії розрізняють прямі та зворотні задачі, під якими розуміються відповідно задачі аналізу якості продукції та задачі синтезу заданих (потрібних) їх властивостей. В основі вирішення прямої задачі лежить безпосереднє вимірювання якості, в основі зворотної – управління якістю продукту з метою придання йому необхідних властивостей. Особливої актуальності зворотна задача набуває для ПМК операцій (бойових дій), які визначально будуються з гнучкою структурою, що передбачає можливість включення до їх складу нових моделей або модифікації вже існуючих. Так, досвід експлуатації діючого зразка ПМК операцій на

заходах оперативної підготовки останніх років вказує на те, що модифікація та удосконалення комплексу проводиться достатньо регулярно, це вимагає такої ж постійної уваги до аналізу та управління його якісними характеристиками. Другим важливим аспектом можна вважати включення в поняття якості як об'єктивних властивостей, так і суб'єктивних оцінок корисності об'єкту, які кваліметричними методами оцінюються одним узагальненим показником [2]. Це природним чином потребує участі експертів (фахівців у предметній області та безпосередніх користувачів моделей) для надання оцінок, насамперед, тим показникам якості, які проблематично описати однозначною чисельною мірою. Наприклад, оцінки таких важливих властивостей як адекватність або адаптивність моделей відображаються, як правило, у інтервальних шкалах, що потребує відповідного їх упорядкування та нормування для подальшої обробки. Методи обробки експертної інформації достатньо розвинені та представлені у тематичній літературі, крім цього, сучасні програмні засоби аналітичної обробки даних надають можливість створювати адекватні моделі з високим коефіцієнтом детермінації залежних змінних, в якості яких й можуть бути представлені інтегральні показники якості. Такий аналітичний інструмент здатен значно спростити оцінку якісних характеристик об'єктів, що постійно розвиваються, тобто отримують нові властивості, які і потребують аналізу. До таких об'єктів, безумовно, повною мірою відносяться і згадані вище моделі та ПмК операцій (бойових дій).

**Постановка проблеми.** Активний розвиток та постійне удосконалення моделей та ПмК операцій (бойових дій) обумовлюють необхідність розгляду питань, пов'язаних з автоматизацією всебічного аналізу та оцінювання нових властивостей, набутих моделями в результаті такого розвитку. Раціональним шляхом для цього представляється поєднання розвиненого апарату оброблення експертної інформації з можливостями сучасних засобів аналізу даних. Результатом такого поєднання може бути модель, що встановлює однозначний аналітичний зв'язок між незалежними змінними (оцінками експертів ключових властивостей моделей) та залежною змінною – інтегральною оцінкою якості моделі (ПмК). Крім цього, така модель повинна дозволити оцінювати внесок кожної з обраних для аналізу властивостей моделі в інтегральний показник якості, а програмний засіб як середовище побудови такої моделі - проводити всі необхідні для аналізу даних перевірки (перевірки залишків на гетероскедастичність, відсутність колінеарних незалежних змінних або кореляції між ними тощо). Власне, дослідження за побудованою таким чином моделлю будуть певним чином вирішувати дві типові задачі кваліметрії – проводити чисельну оцінку якості вже розроблених програмних продуктів, а також аналізувати зміни, які

відбудуться у інтегральній оцінці їх якості при модифікації або структурних змінах для прийняття обґрунтованого рішення про доцільність або корисність таких змін.

**Аналіз останніх досліджень і публікацій.** Серед робіт, присвячених розгляду питань за тематикою статті, можна виділити: у теоретичному плані – монографію [1] та публікації [3,4]; у прикладному – практичне керівництво [5]. В рамках робіт [1,3,4] їх авторами декларується думка про те, що розвиток теорії кваліметрії моделей неможливий без узагальнення результатів досліджень, що проводяться відносно якісних властивостей спеціалізованих моделей (ПмК) у суто прикладних сферах досліджень. Погоджуючись з цією думкою авторів, можна вважати, що реалізація ключових теоретичних положень кваліметрії у практичній площині відносно достатньо спеціалізованих моделей операцій (бойових дій) є актуальним прикладним завданням, розгляд питань розробки моделі оцінювання якості полімодельного комплексу операцій і становить мету статті.

### Виклад основного матеріалу дослідження

Постановочна частина задачі побудови моделі оцінювання якісних властивостей ПмК операцій (бойових дій) може бути сформульована наступним чином. Існує полімодельний комплекс (який являє собою сукупність аналітичних та імітаційних моделей операцій, а також ряду інформаційно-розрахункових задач, що використовують єдину базу даних та геоінформаційну систему), який активно застосовується на більшості заходів оперативної підготовки з органами військового управління оперативного та оперативно-стратегічного рівнів. Експертам, якими визначені фахівці з оперативної підготовки відповідного рівня та особи, безпосередньо відповідальні за експлуатацію комплексу в процесі навчань та тренувань, було запропоновано: по-перше, обрати п'ять найважливіших властивостей, що вирішальним чином впливають на узагальнену оцінку якості ПмК операцій; по-друге, оцінити якість обраних властивостей за інтервальною шкалою [0;1]. У відповідності до рекомендацій [6] щодо планування експерименту для п'яти параметрів в якості вихідних даних для подальших обчислень необхідно сформувати таблиці розмірності 5 (обраних властивостей) на 21 (експертних оцінок). Залишаючи поза розглядом методичні деталі процедур експертного оцінювання, зауважимо лише, що вибір результуючої таблиці здійснювався за типовим алгоритмом пошуку медіани Кемені.

У підсумку роботи експертів у такій постановці отримуємо набір упорядкованих та віднормованих значень, які можна обробляти з урахуванням основних положень аналізу даних, викладених, наприклад, у [5]. Серед достатньо повного



переліку типових властивостей моделей та полімодельних комплексів, розглянутих у [1,3,4], експертами визначені як найважливіші: адекватність; адаптивність; стійкість (у роботі); простота (з точки зору користувача); достовірність результатів. В якості програмного пакету для проведення аналізу та оброблення отриманих даних доцільно обрати такий, в якому реалізуються алгоритми нейронних мереж, а базова модель пов'язує залежну змінну у (інтегральну оцінку якості) з незалежними змінними x (оціночними судженнями експертів відносно якості властивостей ПМК) за допомогою поліному Колмогорова – Габора виду:

$$y = \omega_0 + \sum_{i=1}^m \omega_i x_i + \sum_{i=1}^m \sum_{j=1}^m \omega_{ij} x_i x_j + \sum_{i=1}^m \sum_{j=1}^m \sum_{k=1}^m \omega_{ijk} x_i x_j x_k + \dots \quad (1)$$

У такій моделі  $x = \{x_i | i = 1, \dots, m\}$  – множина незалежних змінних, а  $\omega$  – вектор параметрів – вагових коефіцієнтів:

$$\omega = \langle \omega_i, \omega_{ij}, \omega_{ijk}, \dots | i, j, k, \dots = 1, \dots, m \rangle. \quad (2)$$

Основні особливості побудованої таким чином моделі оцінювання якості властивостей ПМК можуть бути пояснені за допомогою матеріалу, який представлений на наступних рисунках.

На рис.1 – вихідні дані у вигляді нормованих оцінок експертів по кожній з обраних властивостей. На рис. 1 прийняті наступні позначення:  $\alpha 1$  – адекватність;  $\alpha 2$  – адаптивність;

$\alpha 3$  – стійкість у роботі;  $\alpha 4$  – простота користування;  $\alpha 5$  – достовірність результатів.

Експ.	a1	a2	a3	a4	a5	as/5
1	0,67	0,72	0,8	0,71	0,64	0,708
2	0,71	0,67	0,67	0,81	0,73	0,718
3	0,59	0,8	0,79	0,85	0,74	0,754
4	0,64	0,79	0,73	0,75	0,65	0,712
5	0,75	0,71	0,7	0,85	0,58	0,718
6	0,8	0,57	0,85	0,87	0,72	0,762
7	0,69	0,75	0,8	0,75	0,68	0,734
8	0,73	0,69	0,77	0,77	0,7	0,732
9	0,81	0,77	0,81	0,85	0,68	0,784
10	0,58	0,6	0,65	0,77	0,65	0,65
11	0,66	0,67	0,78	0,88	0,7	0,738
12	0,69	0,81	0,74	0,91	0,55	0,74
13	0,65	0,77	0,79	0,79	0,72	0,744
14	0,69	0,81	0,85	0,85	0,71	0,782
15	0,7	0,8	0,83	0,79	0,64	0,752
16	0,65	0,65	0,9	0,9	0,75	0,77
17	0,71	0,75	0,79	0,87	0,7	0,764
18	0,67	0,69	0,77	0,79	0,65	0,714
19	0,71	0,79	0,85	0,85	0,59	0,758
20	0,8	0,85	0,84	0,75	0,67	0,782
21	0,65	0,69	0,75	0,82	0,68	0,718

Рис. 1. Нормовані експертні оцінки обраних властивостей ПМК

На рис. 2 – результати аналізу гетероскедастичності залишків побудованої моделі. З рис. 2 можна зробити однозначний висновок про гомоскедастичність (однорідну варіативність випадкових відхилень) залишків, що свідчить на користь отриманої моделі.

На рис. 3 – результати аналізу автокореляції залишків моделі, які свідчать про те, що залишки некорельовані (висновок за графічним методом рядів, залишки мають асимптотично нормальний розподіл), специфікація моделі обрана правильно

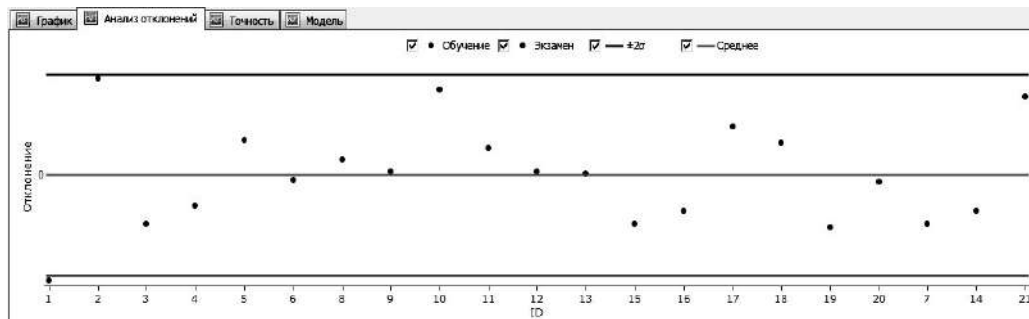


Рис. 2. Результати аналізу гетероскедастичності залишків моделі

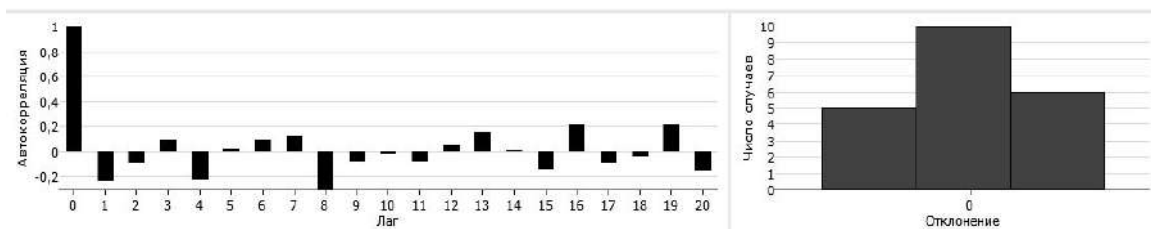


Рис. 3. Результати аналізу автокореляції залишків моделі

На рис. 4 – характеристики достовірності отриманої моделі. Ключовою характеристикою достовірності моделі можна вважати коефіцієнт детермінації (R2), як долю дисперсії залежної змінної (якою є інтегральна оцінка якості), що пояснюється отриманою моделлю. Близькість коефіцієнту детермінації до 1 є переконливим

аргументом на користь якості отриманої моделі, яка здатна «пояснити» 99, 8 % випадків варіацій залежної змінної.

На рис. 5 приведені оцінки значимості кожної з незалежних змінних, що входять до отриманої моделі. Така оцінка достатньо важлива з точки зору подальшого застосування моделі, а саме

аналізу змін властивостей ПмК, що можуть відбутися внаслідок структурної перебудови або модифікації існуючих моделей комплексу.

Макс. отрицательное отклонение	-0,0010127
Макс. положительное отклонение	0,000545693
Средний модуль ошибки (СМО)	0,000423177
Среднеквадратическое отклонение (СКО)	0,000543866
Сумма отклонений	-1,11022E-15
Стандартное отклонение остатков	0,000543866
Кoeffициент детерминации (R <sup>2</sup> )	0,998906
Корреляция	0,999453

Рис 4. Характеристики достовірності отриманої моделі

№	Если заместить средним значением	Влияние на СКО	Графически	СКО
1	a2	37,62%		0,0123457
2	a1	36,15%		0,0118608
3	a3	35,36%		0,0116036
4	a4	31,91%		0,0104699
5	a5	31,63%		0,0103796
	[Ничего не замещено]	0%		3,19485E-13
	[Замещено все]	100%		0,0328132

Рис 5. Результати оцінки значимості незалежних змінних

Приведені на рис. 5 значення свідчать про правильне ранжування «внеску» незалежних змінних (обраних експертами властивостей) у інтегральну оцінку якості ПмК.

На рис. 6 показана графічна візуалізація залежності інтегральної оцінки від двох найбільш значущих незалежних змінних моделі – адаптивності та адекватності полімодельного комплексу.

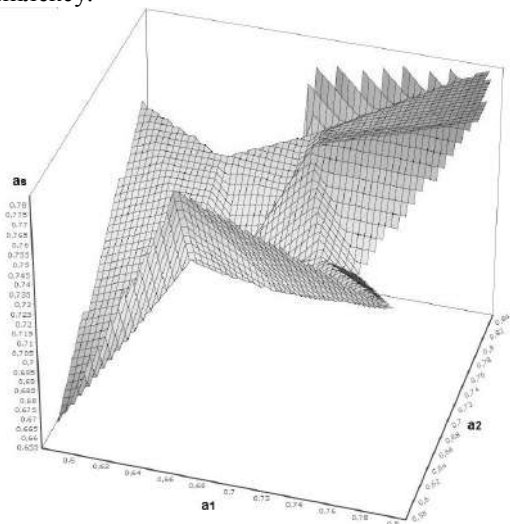


Рис. 6. Графічна залежність інтегральної оцінки від значущих змінних моделі оцінки якості

Отримана модель оцінки якості ПмК операцій (бойових дій) представляється у вигляді нелінійного поліному так, як показано на рис. 7.

За сукупністю проаналізованих характеристик отримана модель представляється цілком придатною для оцінювання якості полімодельного комплексу операцій (бойових дій) і може бути задіяна в якості інструменту вирішення двох загальних задач кваліметрії моделей – прямої (безпосереднє чисельне оцінювання якості), та

зворотної – управління якістю моделей та комплексів

$$\begin{aligned}
 &as = 1.07707e-16 + N3^*1 \\
 &N3 = -7.87e-12 + N43^*0.02274e-11 + N4^*1 \\
 &N4 = -3.28906e-12 + a5^*1.21975e-12 + N5^*1 \\
 &N5 = -8.90687e-12 + N42^*1.05942e-10 + N6^*1 \\
 &N6 = 1.44407e-11 + N348^*1.05942e-10 + N7^*1 \\
 &N7 = -1.06247e-10 + N378^*1.05239e-09 + N8^*1 \\
 &N8 = -1.4267e-10 + N159^*0.02713e-08 + N9^*1 \\
 &N9 = 3.66434e-09 + N435^*2.11082e-08 + N10^*1 \\
 &N10 = 5.88652e-09 + a5^*1.42338e-08 + N11^*1 \\
 &N11 = 1.73309e-08 + N285^*4.57281e-07 + N12^*1 \\
 &N12 = -4.9046e-09 + N106^*4.89389e-05 + N13^*0.898951 \\
 &N13 = 5.92019e-08 + N193^*4.16337e-09 + N14^*1.0004 \\
 &N15 = -2.49738e-06 + N373^*2.75261e-05 + N19^*0.999976 \\
 &N19 = 6.23938e-08 + N51^*1.0589179 + N21^*1.05892 \\
 &N21 = -2.23828e-05 + N289^*0.000651 + N20^*0.99958 \\
 &N28 = -2.50235e-06 + N44^*0.893275 + N32^*0.306728 \\
 &N32 = 0.00748148 + N272^*0.0839686 + N118^*1.07333 \\
 &..... \\
 &N118 = 0.06164653 + N40^*1.0122549 + N145^*1.01872 \\
 &N145 = 0.0220349 + N247^*2.38919 + N328^*1.41904 \\
 &N328 = -0.123568 + N388^*0.12578 + N403^*0.454858 \\
 &N403 = -0.120222 + a5^*0.167595 + N48^*0.120285 \\
 &N388 = -0.1239138 + a1^*0.171814 + N414^*0.869387 \\
 &N372 = -0.144338 + N39^*0.03205 + N207^*0.41857 \\
 &N427 = -0.108524 + a4^*0.20779 + N440^*0.920119 \\
 &N396 = -0.0589883 + N409^*0.465635 + N414^*0.614809 \\
 &N44 = 0.000584212 + N24^*1.0420441 + N7^*0.104128 \\
 &N76 = -0.0043326 + N342^*0.0796922 + N11^*0.926449 \\
 &N11 = 0.029414 + N249^*0.14197 + N349^*1.17776 \\
 &N288 = -0.234917 + N378^*0.840951 + N425^*0.477194 \\
 &N425 = 8.76083e-12 + N426^*1 \\
 &N51 = 0.000533106 + N19^*1.0412941 + N79^*1.04048 \\
 &N79 = -0.0043326 + N342^*0.0796922 + N11^*0.926449 \\
 &N110 = 0.029414 + N249^*0.14197 + N349^*1.17776 \\
 &N343 = -0.115089 + N393^*0.614518 + N417^*0.541402 \\
 &N417 = -0.0423555 + a1^*0.216533 + N436^*0.83307 \\
 &N393 = -0.759886 + N44^*1.0062 + N460^*1.02346 \\
 &N446 = -0.111277 + N350^*0.678025 + N379^*0.472757 \\
 &N379 = -0.430222 + N404^*0.942892 + N440^*0.640265 \\
 &N441 = -0.236004 + N404^*0.837474 + N426^*0.891117 \\
 &N195 = -0.121706 + N461^*0.328467 + N329^*0.959752 \\
 &N461 = 0.532073 + a4^*0.257576 \\
 &N373 = -0.141297 + N404^*0.569204 + N409^*0.822166 \\
 &N133 = 0.0548951 + N344^*1.041894 + N189^*1.34559 \\
 &N189 = 0.0529732 + N359^*1.040699 + N285^*1.3269 \\
 &N399 = 5.24858e-12 + N406^*1 \\
 &N434 = -0.130116 + N430^*0.87728 + N444^*0.888381 \\
 &N436 = 0.416083 + a2^*0.428551 \\
 &N106 = -0.00141709 + N116^*0.832219 + N159^*0.169701 \\
 &N116 = 0.029414 + N249^*0.14197 + N349^*1.17776 \\
 &N446 = -0.115089 + N394^*0.614518 + N416^*0.541402 \\
 &N416 = -0.0194249 + a2^*0.65943 + N440^*0.653944 \\
 &N449 = 0.503235 + a1^*0.351169 \\
 &N394 = -0.211717 + a4^*0.265818 + N444^*1.0062 \\
 &N247 = -0.111277 + N350^*0.678025 + N389^*0.472757 \\
 &N285 = -0.116453 + N394^*0.732689 + N395^*0.42106 \\
 &N395 = 5.47455e-12 + N404^*1 \\
 &N350 = -0.439118 + N420^*0.75189 + N444^*0.841822 \\
 &N453 = 0.114483 + a2^*0.251871 + N444^*0.383331 \\
 &N444 = 0.340405 + a2^*0.222265 + a5^*0.024523 \\
 &N159 = 0.0316287 + N274^*2.34615 + N316^*1.1389 \\
 &N316 = -0.164049 + N32^*0.728855 + N445^*0.493423 \\
 &N445 = -0.0411592 + a5^*0.024523 + N449^*0.382452 \\
 &N449 = 0.338992 + a1^*0.420164 \\
 &N82 = -0.0012448 + a2^*0.341346 + N42^*0.65449 \\
 &N274 = -0.164083 + N375^*0.616024 + N30^*0.608822 \\
 &N30 = -0.090707 + a4^*0.164917 + N404^*0.942692 \\
 &N375 = -0.148492 + N409^*0.222566 + N426^*0.378949 \\
 &N409 = 0.304569 + a1^*0.202264 + a3^*0.37812 \\
 &N378 = -0.107127 + N404^*0.497593 + N414^*0.647565 \\
 &N414 = 0.192618 + a3^*0.445342 + a4^*0.246892 \\
 &N404 = 0.293928 + a2^*0.437271 + a5^*0.167595 \\
 &N348 = -0.0550689 + a4^*1.10907 + N418^*0.94538 \\
 &N418 = 0.312941 + a1^*0.216533 + a2^*0.365943 \\
 &N462 = 2.5458e-11 + N460^*1 \\
 &N460 = 0.532073 + a1^*0.257576 \\
 &N426 = 0.339093 + a1^*0.304715 + a4^*0.20779
 \end{aligned}$$

Рис. 7. Модель оцінки якості властивостей ПмК операцій (бойових дій)

Відносно оберненої задачі є необхідними декілька зауважень. Управління якістю у даному випадку передбачає придання властивостей моделі (комплексу) із заданим рівнем якості і цілком залежатиме від мети, яку намагаються досягти розробники. Так, модифікація моделей (ПмК) має за мету, як правило, їх удосконалення за результатами дослідної експлуатації, і у більшості випадків призводить до підвищення однієї або декількох якісних оцінок певних властивостей (наприклад – простоти для користувача та адаптивності). У разі структурних змін ПмК (включення до їх складу нових моделей, задач, алгоритмів тощо) ситуація дещо складніша, оскільки підвищення якості одних властивостей може призвести до погіршення якості інших (наприклад – якщо включення нових моделей до складу ПмК спрямоване на підвищення достовірності отриманих результатів, це може призвести до ускладнення процесу користування комплексом моделей). В такому випадку доцільніше вести мову не стільки про підвищення якісних властивостей, скільки про збереження на необхідному рівні загальної (інтегральної) оцінки якості комплексу або моделі. Ще однією особливістю управління якістю моделей (ПмК) операцій можна вважати структурну реконфігурацію комплексів моделей, яка здійснюється з метою вибору такої моделі (задачі, алгоритму) з числа наявних, що у найбільшій мірі відповідає поточному завданню та умовам моделювання. Така реконфігурація здійснюється безпосередньо в процесі моделювання, її можливість визначається такою властивістю як адаптивність комплексу (моделі). Розгляд завдання управління якістю у такій постановці виходить за межі тематики статті і приводиться лише з метою окреслення напрямків вирішення зворотної задачі кваліметрії.

У будь-якому випадку наявність інструменту для оцінювання якості типових властивостей моделей та ПМК операцій (бойових дій) надасть можливість обґрунтовано (з точки зору кваліметрії) підходити до модифікації та структурних змін у моделях та комплексах моделей операцій.

### Висновки й перспективи подальших досліджень

Оцінка якісних характеристик моделей та ПМК операцій (бойових дій), як дієвого та необхідного інструменту роботи органів військового управління, є відповідальним етапом, за яким визначається ступінь придатності моделей до використання за призначенням. Кваліметрія моделей (чисельна оцінка якісних характеристик) передбачає необхідність урахування як об'єктивних властивостей, так і суб'єктивних оцінок корисності моделей (комплексів моделей), які кваліметричними методами оцінюються одним узагальненим показником (інтегральним

показником якості). Поєднання розвинутого методичного апарату оброблення експертної інформації з можливостями сучасних засобів аналізу даних дозволяє побудувати модель, яка спроможна з достатньо високою точністю розраховувати інтегральний показник якості обраних властивостей моделей, а також може бути використана для кваліметричного аналізу можливих модифікацій та структурних змін у моделях (ПМК). Розглянутий у статті практичний приклад (з використанням діючого полімодельного комплексу операцій та залученням експертів) побудови моделі оцінки якості ПМК підтвердив можливість та доцільність такого підходу.

Перспективою подальших досліджень вважається розгляд питань, пов'язаних з оцінкою кваліметричними методами структурної реконфігурації полімодельних комплексів операцій (бойових дій) в процесі їх застосування в умовах часових обмежень.

### Література

1. Микони С.В. Кваліметрія моделей і полімодельних комплексів: монографія / С.В. Микони, Б.В. Соколов, Р.М. Юсупов. – М.: РАН, 2018. – 314 с.  
2. Пятак И.А. Метрология, стандартизация, сертификация и аккредитация. – Д.: ДНУ, 2012. – 26 с.  
3. Соколов Б.В. Концептуальные и методические основы кваліметрии моделей и полімодельных комплексів / Б.В. Соколов, Р.М. Юсупов // Труды Санкт-Петербургского института информатики и автоматизации РАН. – Санкт-Петербург: СПИИРАН, 2004. – Вып. 2. Т. 1. – С.10–34.  
4. Охтилев М. Ю. Комплексное моделирование сложных объектов: основные особенности и примеры практической

реализации / М.Ю. Охтилев, А.Н. Павлов, А.М. Плотников, С.А. Потрясаев, Б.В. Соколов, Р.М. Юсупов // Имитационное моделирование: Теория и практика (ИММОД-2015): пленарные доклады 7-ой науч.-практ. конф. по имитац. моделир. и его применению в науке и промышленности. – М.: НОИМ, 2015. – С. 58–81.  
5. Кулаичев А.П. Методы и средства анализа данных в среде Windows. STADIA. – М.: Информатика и компьютеры, 2002. – 341 с.  
6. Загорка О.М. Элементы дослідження складних систем військового призначення: посібник / О.М. Загорка, С.П. Мосов, А.І. Сбитнев, П.І. Стужук. – К.: НАОУ, 2005. – 72 с.

## ПРИМЕНЕНИЕ МОДИФИЦИРОВАННЫХ УРАВНЕНИЙ ДИНАМИКИ СРЕДНИХ ДЛЯ ОПЕРАТИВНОГО ПРОГНОЗИРОВАНИЯ ХОДА И РЕЗУЛЬТАТОВ БОЕВЫХ ДЕЙСТВИЙ

*Борис Леонидович Бутвин (доктор технических наук, профессор)*  
*Александр Александрович Машкин (кандидат технических наук, с.н.с.)*  
*Алексей Иванович Соломицкий (кандидат военных наук, с.н.с.)*

*Центральный научно-исследовательский институт Вооруженных Сил Украины, Киев, Украина*

В статье рассматриваются особенности оценки качества моделей и полимодельных комплексов операций (боевых действий). Такие модели являются действенным и необходимым инструментом проведения оперативных расчетов на мероприятиях оперативной подготовки, а процедуры оценки их качественных свойств – важным и ответственным этапом жизненного цикла. В рамках теоретической кваліметрии различают прямые и обратные задачи оценки качества, в основе первой лежит непосредственное измерение качества, в основе второй задачи – управление качеством продукта с целью придания ему необходимых свойств. Особенную актуальность обратная задача приобретает для полимодельных комплексов операций (боевых действий), которые изначально строятся с гибкой структурой, что предусматривает возможность включения в их состав новых моделей или модификацию уже существующих. Поскольку понятие качества включает как объективные свойства, так и субъективные оценки полезности объекта, которые кваліметрическими методами оцениваются одним обобщенным показателем, естественным является привлечение к таким оценкам экспертов в предметной области. Разработанность аппарата обработки экспертной информации вкупе с современными программными средствами анализа и обработки данных предоставляет возможность упорядочивания процесса оценки качества наиболее важных свойств моделей и полимодельных комплексов. Это возможно путем установления нелинейной аналитической

зависимости, которая свяжет независимые переменные (обработанные оценки экспертов) с зависимой переменной, в роли которой выступает интегральная оценка качества моделей. Пример построения такой зависимости с высоким коэффициентом детерминации интегральной оценки качества, рассмотренный в статье, подтвердил целесообразность такого подхода. Наличие описанного инструмента оценки качества позволит с достаточно высокой точностью рассчитывать интегральный показатель качества выбранных свойств моделей, а также может быть использовано для квалиметрического анализа возможных модификаций и структурных изменений в моделях и полимодельных комплексах операций (боевых действий).

**Ключевые слова:** квалиметрия моделей; полимодельный комплекс операций; качественная оценка свойств.

## APPLICATION OF MODIFIED EQUATIONS OF DYNAMICS OF AVERAGE FOR OPERATIONAL FORECASTING OF THE TURN AND RESULTS OF BATTLE ACTION

*Borys Butvin (Doctor of Technical Sciences, Professor)*

*Olexander Mashkin (Candidate of Technical Sciences, Senior Researcher)*

*Olexii Solomitskii (Candidate of Military Sciences, Senior Researcher)*

*Central Scientific Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine*

The article discusses the peculiarities of evaluation of quality of models and multimodel complexes of operations (combat actions). Such models are an effective and necessary tool for operational calculations at operational training activities, and procedures for assessing their qualitative properties are an important and responsible phase of the life cycle. In theoretical qualifiers the direct and reverse tasks of quality assessment are distinguished, the first is based on the direct quality measurement, the second is the quality management of the product to give it the necessary properties. The reverse task becomes especially relevant for multimodel complexes of operations (combat actions), which are initially built with a flexible structure, which includes the possibility of adding new models or modifying existing ones. Since the concept of quality includes both objective properties and subjective assessments of the utility of an object, which are evaluated by a single generic indicator with a qualifying method, it is natural to involve experts in the subject area in such assessments. The development of an expert information processing unit, together with modern software tools for data analysis and processing, provides an opportunity to organize the process of quality assessment of the most important properties of models and multimodel complexes. This is possible by establishing a non-linear analytical dependency that links independent variables (processed expert estimates) to a dependent variable, which is an integral quality assessment of models. The example of such a dependency with a high determinative factor of integrated quality assessment, as discussed in the article, confirmed the usefulness of such an approach. Having the described quality assessment tool will allow to calculate the integral quality indicator of selected model properties with a high accuracy, as well as can be used for qualifying analysis of possible modifications and structural changes in models and multimodel complexes of operations (combat actions).

**Keywords:** model qualification; polymodel complex of operations; qualitative assessment of properties.

### References

1. Mikoni S.V., Sokolov B.V., Yusupov R.M. (2018), Qualimetry of the models and polymodel complexes: monograph. [Kvalimetriya modeley i polimodel'nykh kompleksov: monografiya], RAS, Moscow, 314 p.
2. Pyatak I.A. (2012), Metrology, standardization, certification and accreditation. [Metrologiya, standartizatsiya, sertifikatsiya i akkreditatsiya], DNU, Dnepropetrovsk, 26 p.
3. Sokolov B.V., Yusupov R.M. (2004), Conceptual and methodical bases of the model and polymodel complexes qualification metering. [Kontseptual'nyye i metodicheskiye osnovy kvalimetrii modeley i polimodel'nykh kompleksov], Proceedings of the Saint-Petersburg Institute of Informatics and Automation of the Russian Academy of Sciences, SPIIRAN, Saint-Petersburg, Issue 2. T. 1. pp. 10–34.
4. Okhtilev M.Yu., Pavlov A.N., Plotnikov A.M., Potryasaev S.A., Sokolov B.V., Yusupov R.M. (2015), Complex modeling of complex objects: main features and examples of practical implementation. [Kompleksnoye modelirovaniye slozhnykh ob'yektov: osnovnyye osobennosti i primery prakticheskoy realizatsii], Simulation modeling: Theory and practice (IMMOD-2015): plenary reports of the 7th scientific-practical conf. on imitation modeling and its application in science and industry, NOVIM, Moscow, pp. 58–81.
5. Kulayichev A.P. (2002), Data analysis methods and tools in Windows environment. STADIA. [Metody i sredstva analiza dannykh v srede Windows. STADIA], Informatics and Computers, Moscow, 341 p.
6. Zagorka O.M., Mosov S.P., Sbitnev A.I., Stizhuk P.I. (2005), Elementary research of the complex military systems: textbook. [Elementy doslidzhennya skladnykh system viys'kovoho pryznachennya: posibnyk], NADU, Kiev, 72 p.

*Володимир Іванович Коцюруба (доктор технічних наук, доцент)<sup>1</sup>*

*Анатолій Степанович Довгополий (доктор технічних наук, професор)<sup>2</sup>*

*Олег Михайлович Гусяков (кандидат технічних наук)<sup>2</sup>*

*Микола Павлович Лойко<sup>3</sup>*

<sup>1</sup> *Національний університет оборони України імені Івана Черняхівського, Київ, Україна*

<sup>2</sup> *Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил, Київ, Україна*

<sup>3</sup> *Товариство з обмеженою відповідальністю “Юг-нафтогазгеологія”, Київ, Україна*

## ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ НЕВИБУХОВОГО ІМПУЛЬСНОГО СЕЙСМІЧНОГО ДЖЕРЕЛА ДЛЯ ЗНИЩЕННЯ ВИБУХОВИХ ПРИСТРОЇВ

Досліджується проблема гуманітарного розмінування та можливість використання принципу дії, що покладено в основу невибухового імпульсного сейсмічного джерела для знищення (знешкодження) вибухових пристроїв з різними датчиками цілі, які встановлені на суші або у воді. Як невибухове імпульсне сейсмічне джерело застосовано дослідний зразок електродинамічного імпульсного джерела сейсмічних сигналів ІДД-27, що надано товариством з обмеженою відповідальністю “Юг-нафтогазгеологія”. На основі аналізу результатів проведеного комплексного натурного експерименту перевірені гіпотези щодо можливості використання пристрою даного типу для знищення (знешкодження) вибухових пристроїв шляхом впливу збуджених поверхневих і епіцентральных сейсмічних та електромагнітних хвиль на контактні або неконтактні датчики цілі вибухових пристроїв. Як контактні використовувались макети обривних (натяжних), натискних, штирьових, сейсмічних датчиків цілі протитанкових, протитраспортних, об’єктних, протипіхотних мін, мін-сюрпризів та саморобних вибухових пристроїв, а також штирьових датчиків цілі протидесантних мін.

Крім того вимірювання параметрів розповсюдження сейсмічних хвиль здійснювалось за допомогою цифрової сейсмічної станції TEXAN-125A з сейсмодатчиками GS-11D та сейсмографа Guralp CMD 40TD. З метою встановлення можливості знищення (знешкодження) вибухових пристроїв із неконтактними магнітними датчиками цілі проводилось дистанційне вимірювання параметрів розповсюдження електромагнітних хвиль від дії електродинамічного імпульсного джерела сейсмічних сигналів ІДД-27 за допомогою магнітотелуричної станції LEM1-423. Аналіз одержаних результатів показав неоднозначність в питаннях можливості використання розглянутого принципу дії невибухового імпульсного сейсмічного джерела для знищення (знешкодження) вибухових пристроїв з різними датчиками цілі на суші та у воді.

**Ключові слова:** гуманітарне розмінування; знищення (знешкодження); датчик цілі; вибуховий пристрій; вибухонебезпечний предмет; невибухове імпульсне сейсмічне джерело; сейсмічні хвилі; електромагнітне випромінювання.

### Вступ

**Постановка проблеми.** Внаслідок бойових дій на сході нашої країни значна територія Донецької та Луганської областей забруднена вибухонебезпечними предметами (ВНП). За попередніми оцінками площа звільненої території та території, яка тимчасово не підконтрольна нашій державі, що вважаються мінно-небезпечними, складає близько 23000 км<sup>2</sup>, на якій проживає більш ніж 5 млн. громадян [1]. За наявною інформацією ця територія замінована та забруднена ВНП, що буде потребуватиме гуманітарного розмінування після встановлення на цій території державного контролю. До того ж, постійні обстріли з боку незаконних збройних формувань, які проводяться у порушення Мінських домовленостей, призводять до нових руйнувань та забрудненню території ВНП.

Аналіз втрат особового складу, озброєння і

військової техніки у ході антитерористичної операції та операції Об’єднаних сил на території Донецької та Луганської областей показав, що від підризу на мінах отримані втрати в особовому складі та бойовій та спеціальній техніці є значним. Найбільш критичним виявився 2015 рік. У 2015 році за даними Стокгольмського інституту Миру за кількістю втрат Україна займає 5 місце випереджаючи Афганістан, Камбоджу, Малі та Пакистан [1].

За даними Управління екологічної безпеки та протимінної діяльності з початком бойових дій на території Донецької та Луганської областей в наслідок підризу на мінах постраждало близько 1900 цивільних осіб (близько 500 загинуло, з них більш 20 – діти) [2].

Досвід виконання завдань з розмінування у воєнних конфліктах сучасності та миротворчих операціях [3-7] показав, що темпи розвитку мінної зброї значно перевищують темпи розвитку

протимінних засобів. Цей факт, враховуючи зростаючу інтенсивність застосування мін та саморобних вибухових пристроїв, у провідних країнах світу давно вже сприймається як загальносвітова проблема, вирішення якої потребує комплексного підходу [8]. При цьому, особлива увага в операціях по розмінуванню приділяється якості очищення місцевості від ВВП, що визначається міжнародними стандартами з розмінування [9].

Взагалі, на даний час не існує ні одного технічного засобу, який би забезпечував виконання вимог [9], що і обумовлює подальше поширене застосування ручного способу розмінування, який є вкрай небезпечним. Отже, враховуючі все вищезазначене, в практиці розмінування існує потреба значного підвищення якості розмінування за рахунок застосування ефективних засобів пошуку (виявлення), знищення (знешкодження) вибухових пристроїв (ВП). Одним із перспективних напрямків розвитку протимінних засобів є впровадження новітніх принципів дії у процеси розмінування, до яких відноситься використання енергії сейсмічних хвиль, що виникають внаслідок штучного впливу невибухового імпульсного сейсмічного джерела (НСД) на укриваючі середовища.

**Аналіз останніх досліджень і публікацій** [10-16] показав, що в них піднято та розглянуто часткові наукові задачі. Так відомі праці [10, 11] присвячені висвітленню результатів наукових досліджень, спрямованих на моделювання процесів та обґрунтування вимог до засобів пошуку та виявлення ВВП різними методами. При цьому, в [10] розглядається можливість та наведені залежності щодо виявлення великих об'єктів та

перехідних шарів у ґрунтах сейсмоакустичним методом. Вказаний метод поки що не знайшов поширеного використання у практиці розмінування. У [12-16] наведені результати експериментальних та теоретичних досліджень способів знищення (знешкодження) ВП, до основних з яких належать вибуховий, механічний, лазерний тощо.

Проведений аналіз відомих доступних досліджень і публікацій дозволив дійти висновку, що задача проведення комплексних експериментальних досліджень можливості використання енергії НСД, як засобу знищення (знешкодження) ВП, не ставилась, а отже і не вирішувалась.

**Мета статті** полягає у висвітленні основних результатів проведеного натурного експерименту щодо дослідження можливості використання НСД для знищення (знешкодження) ВП під час гуманітарного розмінування.

### Виклад основного матеріалу дослідження

В якості робочої гіпотези було використано твердження щодо можливості використання штучного невибухового імпульсного методу збудження сейсмічним коливаль у ґрунтах та ударних хвиль у воді для знищення (знешкодження) ВП, датчики цілі яких засновані переважно на контактних принципах дії.

Як НСД під час експерименту на суші та на воді (рис. 1) було застосоване дослідний зразок електродинамічного імпульсного джерела сейсмічних сигналів ІДД-27 [17], що надане Товариством з обмеженою відповідальністю "Юг-нафтогазгеологія".



а.



б.

Рис. 1 Використання під час експериментальних досліджень електродинамічного імпульсного джерела сейсмічних сигналів ІДД-27: а – на суші; б – на воді.

У ході планування була сформульована додаткова гіпотеза щодо можливого впливу електромагнітного поля від дії НСД на електричні вибухові мережі та магнітні неконтактні датчики інженерних мін (ІМ) та саморобних вибухових пристроїв (СВП).

Отже, в якості об'єкту експериментальних досліджень обрано спосіб знищення або знешкодження ВП шляхом використання НСД, що викликає сейсмічні коливання, ударні хвилі і

електромагнітні поля в укриваючих середовищах. При цьому, задача досліджень полягала в проведенні натурного експерименту з метою визначення характеристик поширення сейсмічних коливаль у ґрунті, ударних хвиль у воді і електромагнітного поля та їх впливу на датчики цілі ВП різного типу.

Планування та проведення експериментальних досліджень здійснювалось на основі методики [18], блок-схема якої наведена на рис. 2.

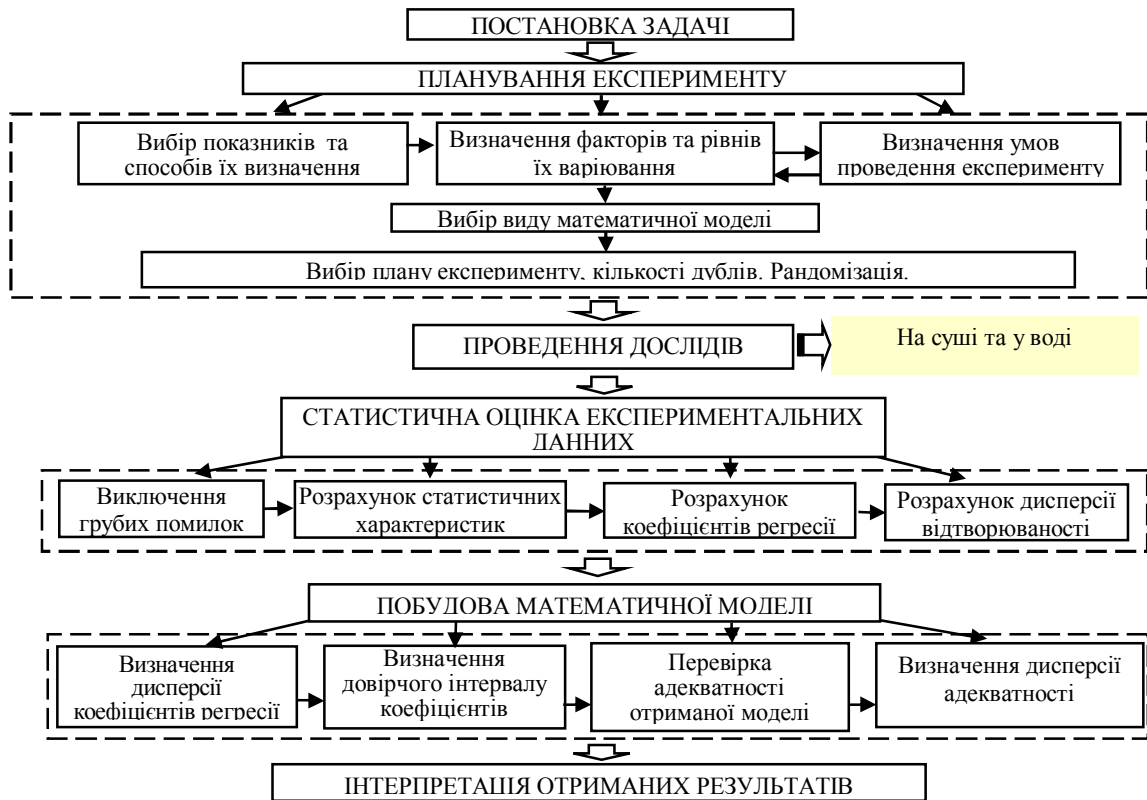


Рис. 2. Блок-схема методики планування та проведення експериментальних досліджень

Варіанти встановлення імітаційних засобів у просторі: на поверхні ґрунту; у ґрунті; на деревах; у воді. Для імітації контактних використовувались макети обривних (натяжних), натискних, штирьових, сейсмічних датчиків цілі

протитанкових (ПТМ), протитраспортних (ПТрМ), об'єктних, протипіхотних мін (ППМ), мін-сюрпризів та СВІП, а також штирьових датчиків цілі протицесантних мін (ПЦМ) (рис. 3).



а.



б.



в.



г.

Рис. 3. Варіанти використаних під час експериментальних досліджень макетів ІМ та СВІП: а – ПТМ натискної дії; б – ПТМ штиреві; в – ППМ, міні-ловушки та СВІП з натяжними (обривними), сейсмічними датчиками цілі; г – ПЦМ донної зі штиревим датчиком цілі

Для проведення досліджень було обрано 6 основних варіантів встановлення ВП у просторі відносно НІСД за типовими схемами (рис. 4), для яких обрано фактори, показники (табл. 1).

На рис. 4 представлені варіанти досліджуваних схем розташування датчиків цілі ВП відносно НІСД:

варіант № 1 – натяжні (обривні) датчики цілі ППМ та СВП, що встановлені на поверхні ґрунту;

варіант № 2 – натяжні (обривні) датчики цілі ППМ та СВП, що встановлені над поверхнею ґрунту (між деревами);

варіант № 3 – натискні датчики цілі ПТМ, що встановлені під поверхнею ґрунту;

варіант № 4 – штиреві датчики цілі ПТМ, що встановлені під поверхнею ґрунту;

варіант № 5 – вібраційні датчики цілі (датчики

руху) ПТрМ та СВП, що встановлені на поверхні ґрунту;

варіант № 6 – штиреві датчики цілі ПДМ, що встановлені у воді.

Показниками, значення яких визначались у ході експерименту (табл. 1), є:

$y_1$  – питомий імпульс ( $i_1$ , кгс/см<sup>2</sup>), визначається через відстань переміщення чеки зривника;

$y_2$  – питомий імпульс ( $i_2$ , кгс/см<sup>2</sup>), визначається через відстань переміщення чеки зривника;

$y_3$  – питомий імпульс ( $i_3$ , кгс/см<sup>2</sup>), визначається через тиск;

$y_4$  – питомий імпульс ( $i_4$ , кгс/см<sup>2</sup>), визначається через тиск;

$y_5$  – частота спрацювання зривника ( $P$ );

$y_6$  – питомий імпульс ( $i_5$ , кгс/см<sup>2</sup>), визначається через тиск.

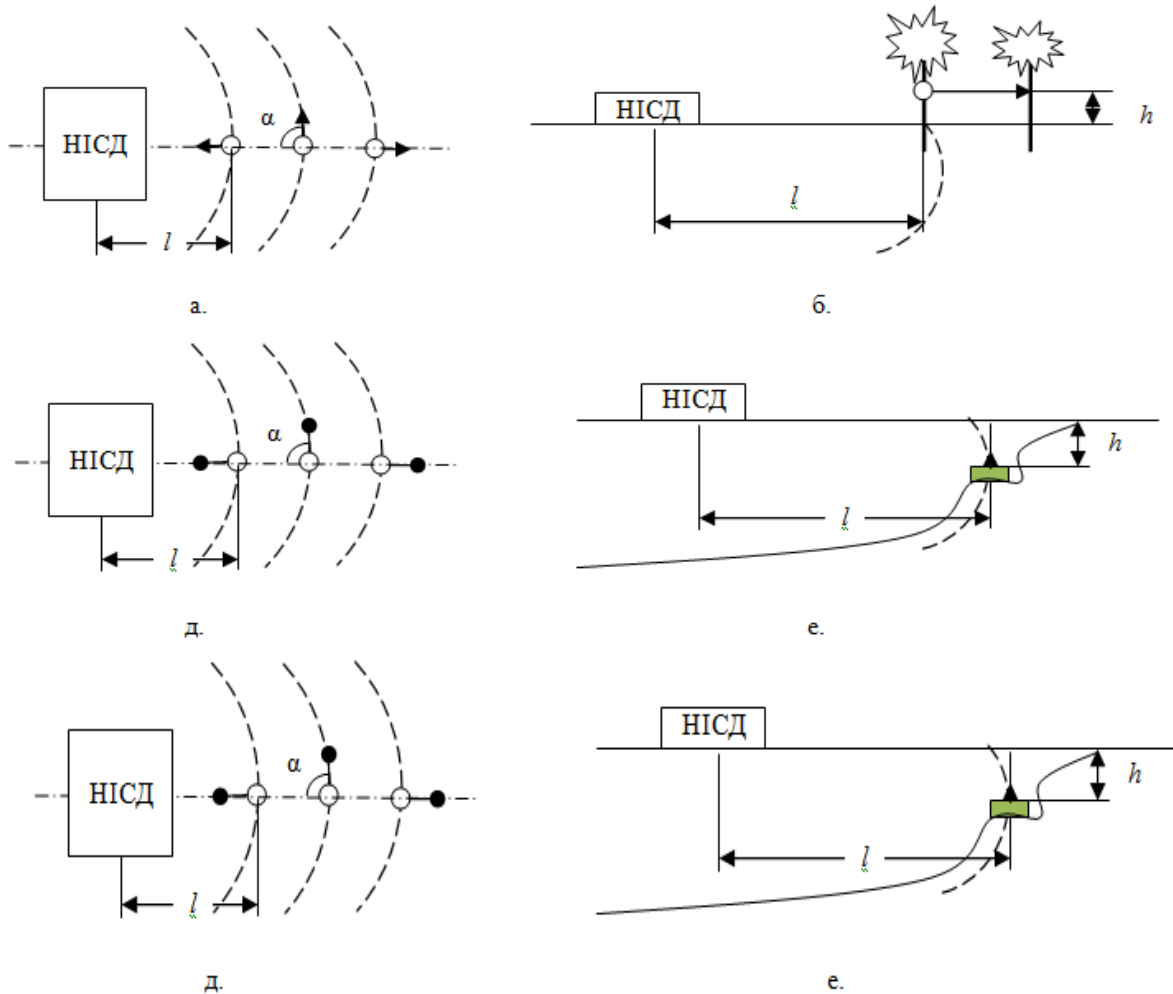


Рис. 4. Схеми розташування датчиків цілі ВП відносно НІСД:  
а – варіант № 1; б – варіант № 2; в – варіант № 3; г – варіант № 4; д – варіант № 5; е – варіант № 6

Таблиця 1

Рівні та інтервали варіювання факторів, позначення показників

Фактори	Кодоване позначення	Інтервал варіювання	Рівні факторів			Позначення показників
			+1	0	-1	
Варіант № 1						
$l$ – віддалення міни від пристрою, м	$x_1$	10	10	20	30	$y_1$
$\alpha$ – кут спрямування ДЦ міни, град	$x_2$	90	0	90	180	
$I$ – макс. тиск пристрою на ґрунт, кгс	$x_3$	10300	4600	14900	25200	
Варіант № 2						
$l$ – віддалення міни від пристрою, м	$x_1$	10	10	20	30	$y_2$
$h$ – висота встановлення міни, м	$x_2$	0,5	0,5	1,0	1,5	
$I$ – макс. тиск пристрою на ґрунт, кгс	$x_3$	10300	4600	14900	25200	



## High-tech aspects of martial arts

Фактори	Кодоване позначення	Інтервал варіювання	Рівні факторів			Позначення показників
			+1	0	-1	
Варіант № 3						
$l$ – віддалення міни від пристрою, м	$x_1$	4	0	4	8	$y_3$
$h$ – глибина встановлення міни, м	$x_2$	0,4	0	0,4	0,8	
$I$ – макс. тиск пристрою на ґрунт, кгс	$x_3$	10300	4600	14900	25200	
Варіант № 4						
$l$ – віддалення міни від пристрою, м	$x_1$	3	2	5	8	$y_4$
$I$ – макс. тиск пристрою на ґрунт, кгс	$x_2$	10300	4600	14900	25200	
Варіант № 5						
$l$ – віддалення міни від пристрою, м	$x_1$	5	5	10	15	$y_5$
$\alpha$ – кут спрямування ДЦ міни, град	$x_2$	90	0	90	180	
$I$ – макс. тиск пристрою на ґрунт, кгс	$x_3$	10300	4600	14900	25200	
Варіант № 6						
$l$ – віддалення міни від пристрою, м	$x_1$	10	5	15	25	$y_6$
$h$ – глибина встановлення міни, м	$x_2$	0,25	0,5	0,75	1,0	
$I$ – макс. тиск пристрою на воду, кгс	$x_3$	10300	4600	14900	25200	

Випробування електродинамічного імпульсного джерела сейсмічних сигналів ІДД-27 проводились влітку на відкритій місцевості на березі та на воді природної водної перешкоди. До проведення комплексних експериментальних досліджень залучались представники: Центрального науково-дослідного інституту озброєння і військової техніки Збройних Сил України, Товариства з обмеженою відповідальністю “Юг-нафтогазгеологія”, Національного університету оборони України імені Івана Черняхівського, Львівського центру Інституту космічних досліджень НАН України та НКАУ, Інституту геофізики імені С.І. Субботіна НАН України.

Додатково вимірювання параметрів розповсюдження сейсмічних хвиль здійснювалось за допомогою цифрової сейсмічної станції TEXAN-125A з сейсмодатчиками GS-11D (рис. 5) та сейсмографу (велосиметра) GURALP CMG-40TD (рис. 6).

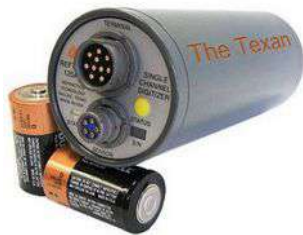


Рис. 5. Загальний вигляд автономної сейсмічної станції TEXAN-125A з елементами живлення



Рис. 6. Цифровий широкосмуговий сейсмограф (велосиметр) GURALP CMG-40TD

Для встановлення можливості знищення (знешкодження) ВП із неконтактними магнітними датчиками цілі проводилось дистанційне вимірювання параметрів розповсюдження електромагнітних хвиль від дії електродинамічного імпульсного джерела сейсмічних сигналів ІДД-27 за допомогою магнітотелуричної станції LEMI-423 (рис 7).



Рис. 7. Загальний вигляд комплексу магнітотелуричної станції LEMI-423

Аналіз одержаних результатів комплексних експериментальних досліджень [19-21] показав неоднозначність в питаннях можливості використання розглянутого принципу дії НІСД для знищення (знешкодження) ВП з різними датчиками цілі на суші та у воді.

Так результати дослідів на суші показали наступне. Натяжні (обривні) датчики цілі макетів ППМ та СВП, що встановлені на поверхні ґрунту та між деревами не спрацювали навіть при безпосередньому наближенні до них НІСД, тобто  $y_1=y_2=0$ . Це означає, що значення питомого імпульсу  $i_1$  та  $i_2$  впливу сейсмічних хвиль від НІСД на натяжні (обривні) датчики цілі ППМ та СВП нижче потрібного для спрацювання.

Питомий імпульс ( $i_3, i_4$ ), що фіксувався від НІСД на натискні та штиреві датчики цілі макетів ПТМ, які встановлені під поверхнею ґрунту виявилися незначними, навіть при проведенні дослідів за варіантом № 3 при

встановленні ПТМ безпосередньо під опорною поверхнею НІСД ( $y_3=y_4=0$ ).

Спрацювань вібраційних датчиків цілі (датчиків руху) макетів ПТрМ та СВП, що встановлені на поверхні ґрунту навіть у безпосередньому наближенні до НІСД ( $l < 1$  м), не було зафіксовано ( $y_5=0$ ).

Результати вимірювань параметрів розповсюдження сейсмічних хвиль від НІСД за допомогою цифрової сейсмічної станції TEXAN-125A з сейсмодатчиками GS-11D та сейсмографа

(велосиметра) GURALP CMG 40TD наведені згідно [20] на рис. 8. Для статистичного аналізу використовувались 20 сейсмічних трас, записаних сейсмостанціями (Z компонента), та коливання ґрунту у тривимірному просторі, які були записані велосиметром GURALP CMG 40TD (X, Y, Z компоненти). На сейсмічних трасах відбирались ділянки з максимальними значеннями амплітуди коливання, на основі обробки результатів яких встановлено приріст потужності (рис. 8).

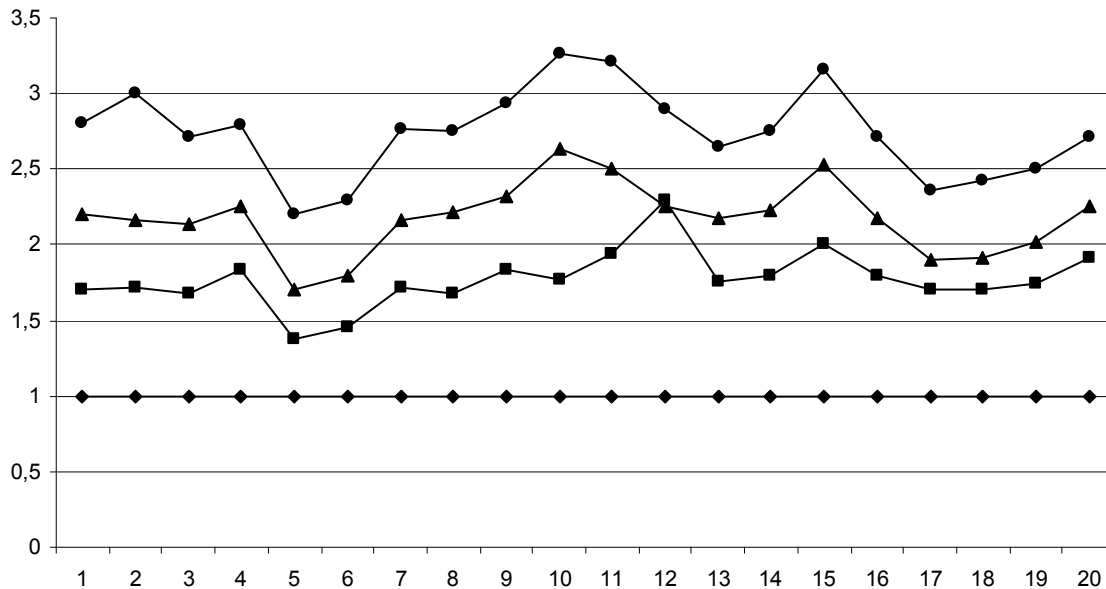


Рис. 8. Приріст потужності НІСД в залежності від кількості одночасно працюючих випромінювачів (вертикальна шкала – рази, горизонтальна – положення сейсмостанцій на поверхні землі). Позначення кривих: ромб – працював один випромінювач, квадрат – два, трикутник – три, круг – чотири [20].

Аналіз одержаних результатів (рис. 8) підтвердив можливість застосування досліджуваного принципу дії НІСД для ведення сейсмоакустичної розвідки крупних об'єктів (наприклад, авіабомб великого калібру), що знаходяться під поверхнею ґрунту, на відстані до 20 м. Достовірність одержаного результату підтверджується високим ступенем збіжності результатів співставлення значень вимірювань приросту потужності імпульсного джерела порохованого за допомогою двох сейсмічних приладів сейсмостанцій TEXAN-125A та велосиметра GURALP CMG 40TD.

Проведені вимірювання узагальнених параметрів НІСД, зокрема характеристики його електромагнітного поля (рис. 9) в практичному діапазоні відстаней за допомогою магнітотелуричної станції LEMI-423 [21] дозволяють зробити наступні висновки:

практичне значення має тільки вертикальна компонента магнітного поля НІСД. Вона має величину 0.2...1 нТл в діапазоні відстаней 66-102 м. Амплітуди інших горизонтальних компонент магнітного і електричного полів знаходяться в межах рівня завад в навколишньому середовищі;

частота коливань струму в соленоїді НІСД знаходиться в районі 30 Гц. Час існування поля в межах одного ударного циклу становить близько 0,7 с;

оцінка величини магнітного моменту  $M$  для серії вимірювань на відстані  $r=66$  м дає величину в межах 1,4...2,9 кА·м<sup>2</sup>. На відстані  $r=102$  м аналогічні оцінки дають величину  $M$  в межах 2,1...3,2 кА·м<sup>2</sup>. Для оцінки створюваного НІСД магнітного поля слід прийняти усереднену величину  $M = 2,4$  кА·м<sup>2</sup>, що не відповідає потрібному значенню цього показника для дистанційного спрацювання неконтактних магнітних датчиків цілі ВП або приведення в дію електричних вибухових мереж.

На відміну від дослідів на суші, більше зацікавлення викликають результати (табл. 2) вимірювань дії коливань від НІСД на штировий датчик цілі макету ПДМ, що встановлений у воді на глибині 2 м. Тарювання виготовленого пристрою для вимірювання питомого імпульсу  $i_5$ , розмішеного усередині макету ПДМ (рис 3.г), показало, що збільшенню його значення на 0,5 кгс при прикладанні зусилля в центрі штиря відповідало збільшення значення тиску на 1 мм рт. ст. шкали манометру.

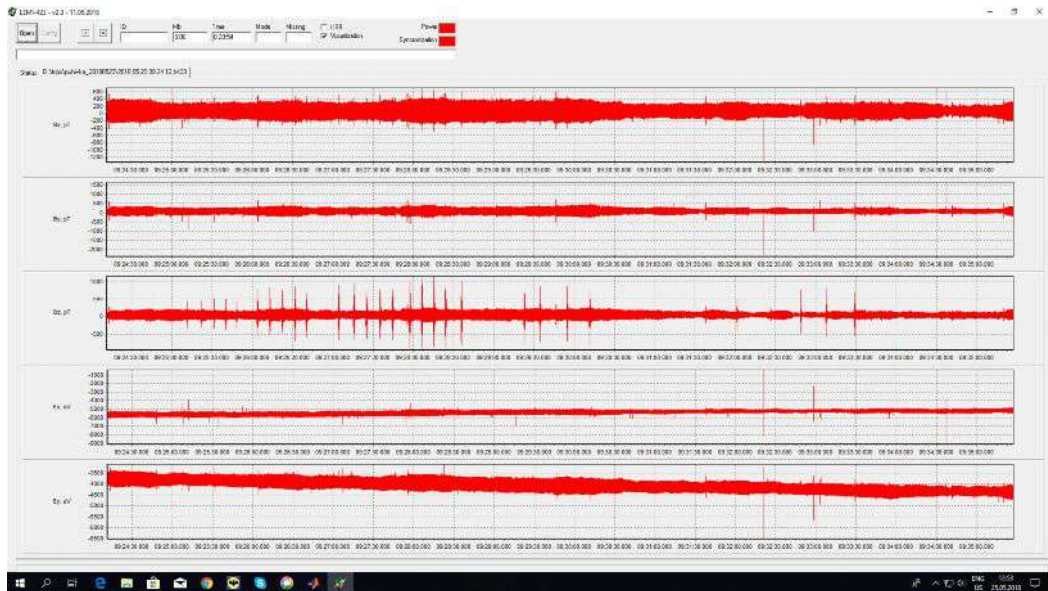


Рис. 9. Результати замірів магнітного та електричного полів.

Таблиця 2

Результати проведених експериментальних досліджень у воді [19]

№ дослідів	Кількість індукторів	Значення шкали тонометра на різних відстанях, мм рт. ст. (кгс):															
		0		1		2		3		4		5		10		15	
		За дослідом	Середнє	За дослідом	Середнє	За дослідом	Середнє	За дослідом	Середнє	За дослідом	Середнє	За дослідом	Середнє	За дослідом	Середнє	За дослідом	Середнє
1	1	-	-	10	-	4	-	1	-	0	-	0	-	0	-	0	-
2		-	-	9	-	5	-	2	-	0	-	0	-	0	-	0	-
3		-	-	10	9,2 (4,6)	4	4,4 (2,2)	1	1,2 (0,6)	0	0	0	0	0	0	0	0
4		-	-	8	-	4	-	1	-	0	-	0	-	0	-	0	-
5		-	-	9	-	5	-	1	-	0	-	0	-	0	-	0	-
6	2	-	-	15	-	9	-	4	-	2	-	0	-	0	-	0	-
7		-	-	16	-	8	-	3	-	1	-	0	-	0	-	0	-
8		-	-	15	15,4 (7,7)	9	9 (4,5)	4	3,8 (1,9)	0	1,2 (0,6)	0	0	0	0	0	0
9		-	-	16	-	9	-	4	-	1	-	0	-	0	-	0	-
10		-	-	15	-	10	-	4	-	2	-	0	-	0	-	0	-
11	3	-	-	20	-	16	-	9	-	4	-	1	-	0	-	0	-
12		-	-	19	-	15	-	9	-	4	-	2	-	0	-	0	-
13		-	-	20	19,8 (9,9)	15	15,4 (7,7)	10	9,4 (4,7)	4	3,8 (1,9)	1	1,4 (0,7)	0	0	0	0
14		-	-	21	-	16	-	9	-	3	-	1	-	0	-	0	-
15		-	-	19	-	15	-	10	-	4	-	2	-	0	-	0	-
16	4	-	-	24	-	21	-	14	-	11	-	4	-	0	-	0	-
17		-	-	23	-	19	-	16	-	9	-	5	-	0	-	0	-
18		-	-	24	23,8 (11,9)	20	20,8 (10,4)	14	14,8 (7,4)	10	9,4 (4,7)	4	4 (2)	0	0	0	0
19		-	-	25	-	21	-	15	-	8	-	3	-	0	-	0	-
20		-	-	23	-	19	-	15	-	9	-	4	-	0	-	0	-

Синтез отриманих середніх значень результатів вимірювань під час проведення експерименту на воді наведено на рис. 10.

Аналіз результатів досліджень (рис. 10) показав, що у воді мінімальне значення зміни тиску на штировий датчик цілі 1,4 мм рт. ст. зафіксоване при роботі 3-х індукторів НІСД та 2 мм рт. ст. – при роботі 4-х індукторів НІСД при поверхневому віддаленні 5 м від центру встановленого макету ПДМ. Максимальне значення зміни тиску на штировий датчик цілі 23,8

мм рт. ст. ( $i_5=11,9$  кгс) зафіксовано при роботі 4-х індукторів НІСД при поверхневому віддаленні 1 м від центру встановленого макету ПДМ. Таке значення питомого імпульсу  $i_5$  на 30% нижче ніж мінімально потрібне значення зусилля спрацювання міни типу ПДМ-1М, а отже є недостатнім. Для забезпечення спрацювання ПДМ у воді значення питомого імпульсу ударної хвилі від дії НІСД із врахуванням потреби віддалення на безпечну відстань (близько 10 м) потрібно значно збільшити.

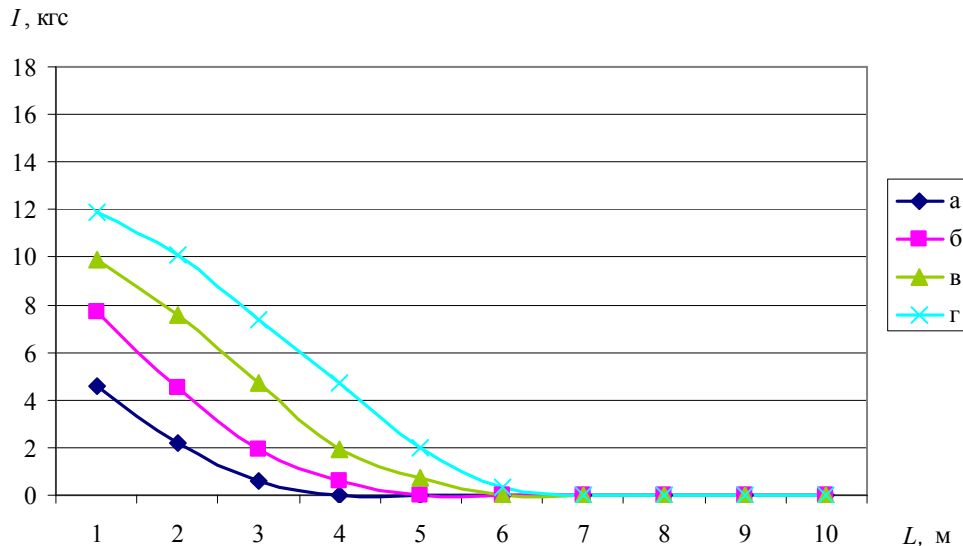


Рис. 10. Залежність тиску зафіксованого тонометром від дальності знаходження пристрою збудження імпульсних сейсмічних коливань: а – значення тиску при дії 1-го індуктору; б – значення тиску при дії 2-х індукторів; в – значення тиску при дії 3-х індукторів; г – значення тиску при дії 4-х індукторів.

### Висновки й перспективи подальших досліджень

Узагальнюючи вищевикладене, можна зробити наступні висновки.

1. Вимірювання за допомогою сейсмічних приладів сейсмостанції TEXAN-125A та велосиметра GURALP CMD 40TD підтвердили можливість застосування досліджуваного принципу дії НІСД для ведення сейсмоакустичної розвідки крупних об'єктів (наприклад, авіабомб великого калібру).

2. Результати вимірювань значень тиску пристроєм збудження імпульсних сейсмічних коливань ІДД-27 у воді підтвердили гіпотезу щодо можливості застосування пристроїв даного типу для знищення (знешкодження) окремих типів ПДМ при збільшенні потужності сейсмічних коливань.

3. Проведені вимірювання характеристики електромагнітного поля НІСД в практичному

діапазоні відстаней за допомогою магнітотелуричної станції LEMI-423 вказують про недостатність їх значень для забезпечення спрацювання неконтактних магнітних датчиків цілі ІМ та СВІ або завчасного приведення в дію електричних вибухових мереж навіть при значному їх наближенні до НІСД.

4. В цілому результати вимірювань показали, що існуючий на теперішній час пристрій збудження імпульсних сейсмічних коливань ІДД-27 виробництва ТОВ «Юг-нафтогазгеологія» має недостатню потужність для знешкодження ВП з будь-якими датчиками цілі, що встановлені в ґрунт або на поверхні ґрунту.

Як напрямок подальших досліджень є обґрунтування тактико-технічних вимог до перспективного засобу знищення (знешкодження) ПДМ з контактними датчиками цілі, в основу принципу дії якого лежить використання енергії збуджених імпульсних хвиль у воді.

### Література

1. Протимінна діяльність в Україні потребує нових підходів, – МінТОТ // Електронний ресурс. Режим доступу: <https://ua.112.ua/suspilstvo/protyminna-diialnist-v-ukraini-potrebuie-novykh-pidkhodiv-mintot-390493.html>.  
 2. Мінна загроза: щодесята жертва підривів – дитина // Електронний ресурс. Режим доступу: <https://rubryka.com/article/minna-zagroza>.  
 3. Польських Н.Л. Некоторые выводы по итогам инженерного обеспечения миротворческих сил в ходе грузино-абхазского конфликта // Арм. сб. 1997. № 1. С. 37-39.  
 4. Жуков С. Опыт разминирования местности в условиях локальных военных конфликтов // Зарубежное военное обозрение. № 6, 1998. С. 14-19.  
 5. Жуков С. Опыт разминирования местности в Боснии и Герцеговине // Зарубежное военное обозрение. № 8, 1998. С. 18-22.  
 6. Свірський Є. Ліван: місія триває // Військо України. № 3, 2003. С. 4-7.  
 7. Підсумковий звіт про виконання бойових завдань саперними підрозділами ЗС України в Ісламській Республіці Афганістан у складі Литовської групи з реконструкції провінції Гор (ГРП) за

період з листопада 2010 р. по листопад 2011 р. К.: ГШ ЗСУ, 2012. 47 с.  
 8. Петренко Е. С. Некоторые технические особенности решения проблемы гуманитарного разминирования // Специальная техника, 2002. №3. С. 12–13.  
 9. Керівництво по управлінню операціями по розмінуванню (офіційний переклад) // МСПМД (IMAS) 07.10. – USA New York: ЮНМАС ООН, 2001. – 30 с. // Електронний ресурс. Режим доступу: <http://www.mineactionstandards.org>.  
 10. Щербаков Г. Н. Новые методы обнаружения скрытых объектов: монография. М.: ООО Эльф ИПР, 2011. 503 с.  
 11. Карев А., Раевский В., Коняев Ю., Румянцев А., Аверченко А. Мобильный комплекс обнаружения взрывчатых веществ. Технология разминирования XXI века // Электроника: Наука, Технологии, Бизнес, 2000. № 1. С. 54-58.  
 12. Корытченко К. В. Экспериментальное исследование применения объемных шланговых зарядов / К.В. Корытченко, Д.П. Дубинин, С.В. Говаленков // Актуальні проблеми технічних та природничих наук у

забезпеченні цивільного захисту: III міжнар. наук.-практ. конф., 6-7 квітня 2010 р.: тези допов. – Черкаси, 2010. – С. 107 – 110. **13. Ментус І. Е.** Ефективність інженерних боєприпасів: навчальний посібник. Кам'янець-Подільський: ФВП ПДАТУ, 2008. 80 с. **14. Бочаров О.А.** Методы дистанционного обезвреживания ВОП // Артиллерийское и стрелковое вооружение / Конструкторское бюро "Артиллерийское вооружение". К.: МПГУ, 2008. № 2. С. 34-37. **15. Саламахин Т.М.** Основы моделирования и боевая эффективность зарядов разрушения. Ч. 1. М.: ВИА, 1983. 160 с. **16. Ментус І.Е.** Ефективність зарядів руйнування: навчальний посібник. Кам'янець-Подільський: ФВП ПДАТУ, 2008. 80 с. **17. Отчет о заводских приемочных испытаниях опытного образца электродинамического импульсного источника**

сейсмических сигналов ИДД-27. – Кимры: ЗАО "Геосвип", 2013. – 43 с. **18. Цивин М.Н.** Многофакторный эксперимент: графическая интерпретация данных – К.: ИГиМ, 2002. – 120 с. **19.** Звіт про проведення експериментальних досліджень 23.05.2018. – К.: ЦНДІ ОБТ ЗС України та ТОВ "Юг-нафтогазгеологія", 2018. 8 с. **20.** Науково-технічний звіт по темі: "Дослідження потужності імпульсного електор-механічного джерела сейсмічних хвиль на суші та у воді, при різній кількості одночасно працюючих індукторів". – К.: Інституту геофізики ім. С.І. Субботіна НАН України, 2018. – 25 с. **21.** Звіт про проведення спостережень з магнітотелуричною станцією LEMI-42. – Львів: Львівського центру Інституту космічних досліджень НАН України та НКАУ, 2018. – 7 с.

## ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ НЕВЗРЫВЧАТОЕ ИМПУЛЬСНОГО СЕЙСМИЧЕСКОГО ИСТОЧНИКИ ДЛЯ УНИЧТОЖЕНИЯ ВЗРЫВНЫХ УСТРОЙСТВ

*Владимир Иванович Коцюруба (доктор технических наук, доцент)<sup>1</sup>  
Анатолий Степанович Довгополь (доктор технических наук, профессор)<sup>2</sup>  
Олег Михайлович Гуслияков (кандидат технических наук)<sup>2</sup>  
Николай Павлович Лойко<sup>3</sup>*

<sup>1</sup> *Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

<sup>2</sup> *Центрального научно-исследовательского института вооружения и военной техники Вооруженных Сил, Киев, Украина*

<sup>3</sup> *Общество с ограниченной ответственностью "Юг-нафтогазгеологія", Киев, Украина*

Исследуется проблема гуманитарного разминирования и возможность использования принципа действия, что положено в основу невзрывного импульсного сейсмического источника для уничтожения (обезвреживания) взрывных устройств с различными датчиками цели, установленные на суше или в воде. Как невзрывное импульсное сейсмическое источник применено опытный образец электродинамического импульсного источника сейсмических сигналов ИСД-27 предоставлены обществом с ограниченной ответственностью "Юг-нафтогазгеологія". На основе анализа результатов проведенного комплексного натурального эксперимента проверены гипотезы о возможности использования устройства данного типа для уничтожения (обезвреживания) взрывных устройств путем воздействия возбужденных поверхностных и эпицентральных сейсмических и электромагнитных волн на контактные или неконтактные датчики цели взрывных устройств. Как контактные использовались макеты обрывные (натяжных), нажимных, штыревых, сейсмических датчиков цели противотанковых, протитранспортных, объектных, противопехотных мин, мин-сюрпризов и самодельных взрывных устройств, а также штыревых датчиков цели противодесантных мин.

Кроме того измерения параметров распространения сейсмических волн осуществлялось с помощью цифровой сейсмической станции TEXAN-125A с сейсмодатчики GS-11D и сейсмографа Guralp CMD 40TD. С целью установления возможности уничтожения (обезвреживания) взрывных устройств с неконтактными магнитными датчиками цели проводилось дистанционное измерение параметров распространения электромагнитных волн от действия электродинамического импульсного источника сейсмических сигналов ИСД-27 с помощью магнитотелурической станции LEMI-423. Анализ полученных результатов показал неоднозначность в вопросах возможности использования рассматриваемого принципа действия невзрывного импульсного сейсмического источника для уничтожения (обезвреживания) взрывных устройств с различными датчиками цели на суше и в воде.

**Ключевые слова:** гуманитарное разминирование; уничтожение (обезвреживание) датчик цели; взрывное устройство; взрывоопасный предмет; невзрывное импульсное сейсмическое источник; сейсмические волны; электромагнитное излучение.

## STUDIES ON THE POSSIBILITY OF USING THE NON-EXPLOSIVE PULSE SEISMIC SOURCE TO NEUTRALIZE EXPLOSION DEVICES

*Volodymyr Kotsiuruba (Doctor of Technical Sciences, Associate Professor)<sup>1</sup>  
Anatolii Dvohopolyi (Doctor of Technical Sciences, Associate Professor)<sup>2</sup>  
Oleh Husliakov (Candidate of Technical Sciences)<sup>2</sup>  
Mykola Loiko<sup>3</sup>*

<sup>1</sup>*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*<sup>2</sup>*Of the Central Research Institute of Armed Forces and Military Equipment of the Armed Forces, Kyiv, Ukraine*<sup>3</sup>*Yug-Neftegazgeologiya Limited Liability Company, Kyiv, Ukraine*

The problem of humanitarian demining and the possibility of using the principle of action that underlies the non-explosive pulse seismic source for the destruction (disposal) of explosive devices with different target sensors mounted on land or in water is investigated. As a non-explosive impulse seismic source a prototype of the electrodynamic impulse source of seismic signals IDD-27 was used, provided by the limited liability company "Yuh-Naftohazgheolohiia". Based on the analysis of the results of a comprehensive field experiment, the hypotheses were tested regarding the possibility of using a device of this type to destroy (neutralize) the explosive devices by the influence of excited surface and both epicentral seismic and electromagnetic waves on the contact or non-contact sensors of the target explosive devices. As the contact ones were used layouts of break-wire (tensioning), push, pin, seismic target sensors; anti-tank, anti-transport, object, anti-personnel land mines, mines-surprises, and improvised explosive devices as well as anti-landing target pin sensors.

In addition, seismic wave propagation parameters were measured using a TEXAN-125A digital seismic station with GS-11D seismic sensors and a Guralp CMD 40TD seismograph. In order to establish the possibility of destruction (neutralization) of explosive devices with non-contact magnetic sensors of the target, remote measurements of the parameters of propagation of electromagnetic waves from the action of the electrodynamic pulse source of seismic signals IDD-27 were carried out by means of the magnetotelluric station LEMI-423. The analysis of the obtained results showed ambiguity regarding the possibility of using the considered principle of action of non-explosive pulsed seismic source for destruction (neutralization) of explosive devices with different sensors of the target on land and in water.

**Key words:** humanitarian demining; destruction (neutralization); target sensor; explosive device; explosive object; non-explosive pulsed seismic source; seismic waves; electromagnetic radiation.

### References

1. Protyminna dijajlnistj v Ukrajinі potrebuje novykh pidkhodiv, – MinTOT // Elektronnyj resurs. Rezhym dostupu: <https://ua.112.ua/suspilstvo/protyminna-diialnist-v-ukraini-potrebuie-novykh-pidkhodiv-mintot-390493.html>.
2. Minna zagroza: shhodesjata zhertva pidryviv – dytyna // Elektronnyj resurs. Rezhym dostupu: <https://rubryka.com/article/minna-zagroza>.
3. Poljskykh N.L. Nekotorye vyvody po ytogham ynzhenemogho obespechenija myrotvorcheskykh syl v khode ghruzyno-abkhazskogho konfliktu // Arm. sb. 1997. № 1. S. 37-39.
4. Zhukov S. Opyt razmynyrovannya mestnosti v uslovyakh lokalnykh voennykh konfliktov // Zarubezhnoe voennoe obozrenye. № 6, 1998. S. 14-19.
5. Zhukov S. Opyt razmynyrovannya mestnosti v Bosnyy y Gherceghovyne // Zarubezhnoe voennoe obozrenye. № 8, 1998. S. 18-22.
6. Svirskij Je. Livan: misija tryvaje // Vijsjko Ukrajinu. № 3, 2003. S. 4-7.
7. Pidsumkovyj zvit pro vykonannya bojovykh zavdanj sapernomu pidrozdilamy ZS Ukrajinu v Islamskij Respublici Afghanistan u skladi Lytovskoji ghropy z rekonstrukciji provinciji Ghor (GhRP) za period z lystopada 2010 r. po lystopad 2011 r. K.: GhSh ZSU, 2012. 47 s.
8. Petrenko E. S. Nekotorye tekhnicheskyye osobennosti reshenija problemy ghumanitarnogho razmynyrovannya // Specjalnaja tekhnika, 2002. №3. S. 12–13.
9. Kerivnyctvo po upravlinnju operacijamy po rozminuvannju (oficijnyj pereklad) // MSPMD (IMAS) 07.10. – USA New York: JuNMAAS OON, 2001. – 30 s. // Elektronnyj resurs. Rezhym dostupu: <http://www.mineactionstandards.org>.
10. Shherbakov Gh. N. Novyye metody obnaruzhenija skrytykh obektov: monoghrafija. M.: OOO Əljf YPR, 2011. 503 s.
11. Karev A., Raevskij V., Konjaev Ju., Rumjancev A., Averchenko A. Mobylnyj kompleks obnaruzhenija vzryvchatykh veshhestv. Tekhnologhija razmynyrovannya XXI veka // Elektronika: Nauka. Tekhnologhyy. Buznes, 2000. № 1. S. 54-58.
12. Korytchenko K. V. Eksperymentalnoe issledovanye prymerenija obemnykh shlanghovykh zarjadov / K.V. Korytchenko, D.P. Dubynyn, S.V. Ghovalenko // Aktualni problemy tekhnichnykh ta pryrodnychkykh nauk u zabezpechenni cyvilnogho zakhystu: III mizhnar. nauk.-prakt. konf., 6-7 kvitnja 2010 r.: tezy dopov. – Cherkasy, 2010. – S. 107 – 110.
13. Mentus I. E. Efektyvnistj inzhenernykh bojeprypasiv: navchalnyj posibnyk. Kam'janecj-Podiljskij: FVP PDATU, 2008. 80 s.
14. Bocharov O.A. Metody dystancyonogho obezvezhyvannya VOP // Artylleryjskoe y strelkovoje vooruzhenye / Konstruktorskoe bjuro "Artylleryjskoe vooruzhenye". K.: MPPU, 2008. № 2. S. 34-37.
15. Salamakhyn T.M. Osnovy modelyrovannya y boevaja efektyvnostj zarjadov razrushenija. Ch. 1. M.: VYA, 1983. 160 s.
16. Mentus I.E. Efektyvnistj zarjadiv rujnuvannja: navchalnyj posibnyk. Kam'janecj-Podiljskij: FVP PDATU, 2008. 80 s.
17. Otchet o zavodskyykh pryemochnykh uspytanyjakh opytnogho obrazca elektrodynamycheskogho ymпульсноgho ystochnyka sejsmycheskykh syghnalov YDD-27. – K.: ZAO "Gheosvyp", 2013. – 43 s.
18. Cyvyn M.N. Mnoghofaktornyj eksperyment: ghrafycheskaja ynterpretacija dannykh – K.: YGhyM, 2002. – 120 s.
19. Zvit pro provedennja eksperymentalnykh doslidzhenj 23.05.2018. – K.: CNDI OVT ZS Ukrajinu ta TOV "Jugh-naftogazgheologhija", 2018. 8 s.
20. Naukovo-tekhnichnyj zvit po temi: "Doslidzhenija potuzhnosti impulsnogho elektor-mekhanichnogho dzherela sejsmichnykh khvylyj na sushi ta u vodi, pry riznij kiljkosti odnochasno pracujuchykh induktorakh". – K.: Instytutu gheofizyky im. S.I. Subbotina NAN Ukrajinu, 2018. – 25 s.
21. Zvit pro provedennja sposterezhenj z maghnitotelurychnoju stancijeju LEMI-42. – Ljviv: Ljvivs'kogho centru Instytutu kosmichnykh doslidzhenj NAN Ukrajinu ta NKAU, 2018. – 7 s.

*Юрій Васильович Пунда (доктор військових наук, с.н.с.)*

*Іван Павлович Козинець (кандидат історичних наук, с.н.с.)*

*Володимир Степанович Клименко (кандидат політичних наук, доцент)*

*Національний університет оборони України імені Івана Черняхівського, Київ, Україна*

## МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ РІВНЯ КОНФЛІКТНОСТІ МІЖДЕРЖАВНИХ ВІДНОСИН

У широкому спектрі проблем забезпечення національної безпеки важлива роль відводиться воєнній сфері. Оцінюючи реалії сьогодення, не слід нехтувати поняттям “воєнна небезпека”, яка розглядається як потенційна можливість будь-якої держави (групи держав) щодо застосування військової сили для вирішення міждержавних протиріч.

Незважаючи на задеклароване в стратегічних документах більшості держав та міжнародних міжурядових організацій прагнення до вирішення протиріч мирним шляхом, прогнозування результатів можливих конфліктів лишається важливим завданням, за результатами якого можна більш об'єктивно приймати воєнно-політичні рішення.

В даній статті автори поставили перед собою завдання запропонувати варіант методичного підходу до визначення рівня конфліктності міждержавних відносин, який доцільно впровадити в процес підготовки фахівців державного військового управління. Шляхом поєднання різних методик передбачається визначити ймовірний осередок можливого конфлікту та спрогнозувати його можливі результати. Авторами запропоновано ряд власних наукових та методичних доробок, що визначає перспективи подальших розвідок у даному напрямку досліджень, моніторингу та прогнозування рівня воєнної небезпеки з боку країн-сусідів.

**Ключові слова:** міждержавні відносини, воєнно-політична обстановка, воєнний конфлікт, національна безпека, національні інтереси, територіальна цілісність, суверенітет.

### Вступ

Розвиток безпекового середовища породив нові виклики та загрози національній безпеці України, які пов'язані із веденням Росією “гібридної війни” проти неї. Усе це вимагає пошуку нових дієвих засобів стримування агресора, активних кроків, в тому числі і у зовнішньополітичній сфері.

**Постановка проблеми.** Сьогодні досить часто виникають політичні, економічні, територіальні, етнічні та інші протиріччя у міждержавних відносинах. Особливо небезпечною є тенденція відновлення “законсервованих” протиріч між державами, що мають історичне підґрунтя та виникли внаслідок розпаду соціалістичного табору. Після виходу із зони впливу колишнього “центру сили”, разом із реальною незалежністю нові держави отримали і проблеми міждержавних відносин, які раніше жорстко контролювались ззовні. Не стала винятком і Україна.

Поряд з цим, реформування сектору безпеки і оборони України, реалізація зовнішньополітичного курсу держави, прийняття нової Стратегії національної безпеки, яка визначає загрози національній безпеці, найбільш актуальною з яких є агресивні дії Росії, вимагають постійної уваги до оцінки воєнно-політичної обстановки, прогнозування результатів можливих конфліктів, так як саме на їх підставі уточнюється

зміст зовнішньополітичної діяльності держави та напрями будівництва і підготовки Збройних Сил.

**Аналіз наукових досліджень і публікацій,** у яких розглядається дана проблематика, показує, що її дослідження охоплює тривалий історичний період, хоча обґрунтовані наукові результати опубліковані відносно недавно та базуються на дослідженні періоду новітньої історії. За висновком дослідників, досягнення людства привели до того, що за характером війни “...XX ст. більше відрізняється від XIX ст., ніж XIX ст. від II ст. Сьогодні наше завдання полягає не стільки в тому, щоб вирахувати можливість виникнення війни у визначений час в певній державі чи війни між двома певними державами, стільки в тому, щоб створити умови для попередження війни чи виробити процедури, які будуть сприяти її подавленню у зародку.” [1].

Проблеми природи соціально-політичного конфлікту вивчалися Т.Мальтусом, К.Клаузевіцом, дослідниками більш пізнього періоду Р.Квінсі, вченими “мічиганської групи” 50-60-х р.р. XX ст. (К.Боулдінгом, А.Рапопортом, Р.Енджелом та ін.), М. Лундом, досліджувались у працях вітчизняних вчених М.Капітоненка, В.Косецова, О.Маначинського, Г.Перепелиці, В.Телелима, М.Цюрупи та інших.

Враховуючи наукові здобутки зарубіжних і вітчизняних дослідників, у даній статті автори ставлять **за мету** дослідити чинники і фактори, які впливають на валідність запропонованих методик оцінки конфліктності двосторонніх міждержавних відносин та на підставі їх аналізу визначити доцільність впровадження даного методологічного підходу в практичну діяльність, в першу чергу військових керівників.

### **Виклад основного матеріалу дослідження**

Серед комплексу заходів, що здійснюються в процесі прийняття управлінських рішень у сфері національної безпеки, надзвичайно важливе місце займає прогнозування можливості вирішення міждержавних територіальних, економічних, етнічних, релігійних та інших суперечок шляхом застосування військової сили (воєнного конфлікту) будь-якою державою чи групою держав. Це вимагає комплексної оцінки великої кількості різноманітних чинників, що можуть призвести до виникнення воєнного конфлікту. Разом з тим, діяльність та структура системи забезпечення національної безпеки розподілена за сферами, що в певній мірі виправдано для раціонального розподілу повноважень між її структурними елементами [2]. Проте такий підхід має і недоліки, зокрема складність налагодження ефективної горизонтальної взаємодії між окремими елементами в процесі розробки та прийняття важливих рішень, що виходить за межі однієї сфери.

Тому в процесі підготовки та прийняття важливих рішень у сфері національної та воєнної безпеки, вибору найкращого варіанта із запропонованих, об'єктивно необхідна методика, що дозволить оперативно, із залученням доступних вихідних даних і обмеженої кількості експертів, з високою ймовірністю оцінити рівень напруженості двосторонніх відносин між Україною та іншими державами, прогнозувати наслідки прийняття варіантів воєнно-політичного рішення для вибору найменш конфліктогенного.

У сьогоденній практиці прийняття воєнно-політичних рішень використовуються методики, які дозволяють визначити рівень національної, воєнної, безпеки, небезпек та загроз. Вони застосовуються для оцінки існуючого стану і потребують великих часових витрат, залучення значної кількості компетентних експертів [3]. Для оперативного розрахунку наслідків прийняття воєнно-політичних рішень у сфері оборони необхідна нескладна, але досить точна методика прогнозування результатів можливого воєнного конфлікту. Очевидно, що така методика має базуватись на основі всебічного аналізу імовірних суб'єктів воєнного конфлікту, на кшталт PEST-аналізу – маркетингового інструменту, призначеного для виявлення політичних, економічних, соціальних і технологічних аспектів зовнішнього середовища, які впливають на бізнес.

Такий підхід у поєднанні зі SWOT-аналізом (сильні та слабкі сторони, можливості і загрози), MOST-аналізом (місія, мета, стратегія, тактика) або SCRS-аналізом (стратегія, поточний стан, вимоги, рішення) успішно використовується також і в оборонному та стратегічному плануванні.

В навчальних цілях авторами пропонується поєднання різних методик для визначення, по-перше, рівня напруженості воєнно-політичної обстановки навколо України і, по-друге, оцінки результатів можливого конфлікту з визначеною стороною.

Під оцінкою воєнно-політичної обстановки (ВПО) розуміється результат кількісно-якісного аналізу сукупності факторів, які характеризують стан відносин між державами (коаліціями держав), їхні воєнно-економічні потенціали, розстановку, співвідношення та взаємодію на даний момент часу військових, політичних та інших сил, а також визначають ступінь напруженості відносин між державами (коаліціями держав) та рівень небезпеки виникнення воєнних конфліктів (війни) (Військовий стандарт 01.101.004 - 2015 (02) (Воєнна розвідка. Розвідувально-інформаційна діяльність. Терміни та визначення.) [4, С.4]

ВПО оцінюється в інтересах безпеки держави та здійснюється постійно, незалежно від воєнного чи мирного часу, напруженої чи спокійної обстановки довкола України. На основі результатів оцінки ВПО уточнюється зміст зовнішньополітичної діяльності держави та напрями будівництва і підготовки Збройних Сил України. Висновки з оцінки ВПО є вихідними даними для подальшої оцінки воєнно-стратегічної обстановки.

Головна мета оцінки ВПО навколо України в мирний час полягає у виявленні ступеня її напруженості, своєчасному визначенні джерел воєнної небезпеки, наявності воєнної загрози Україні, а також загроз в інших сферах та забезпеченні розробки ефективних заходів з їхньої нейтралізації для запобігання можливим конфліктам, у першу чергу збройним.

Оцінювання ВПО пропонується провести методом експертних оцінок [5]. Вихідними даними для оцінювання ВПО є інформаційні документи (розвідувальна інформація, аналітичні огляди, інформаційні бюлетені, інформаційні та інформаційно-аналітичні довідки а також довідники по країнах світу), які надаються органами воєнної розвідки, а також результати обробки інформації з відкритих джерел.

Ступінь напруженості воєнно-політичних відносин між Україною та оцінюваною країною визначається за показниками, наведеними у відповідних методиках [4, С.36-37]. У даному випадку, як приклад, пропонується наступна шкала показників (анкета, на яку дають відповіді експерти), наведена у таблиці 1.

Оцінювання проводиться за шкалою від 0 до 1, де 0 – мінімальний рівень (напруженості), 1 – максимальний рівень (напруженості) як можлива



потенційна чи реальна загроза. Підсумкові показники для спрощення розрахунків пропонується обраховувати як середнє арифметичне.

За результатами оцінки воєнно-політичної обстановки визначається:

загальний стан ВПО між Україною та оцінюваною країною за ступенем напруженості;

причини, що призвели до нинішнього стану ВПО (у разі його погіршення);

ймовірна мета виявлених намірів та дій окремої країни стосовно України, рівень їх агресивності;

тенденції розвитку ВПО між Україною та окремою країною, чинники, якими вони зумовлені.

Ступені напруженості ВПО між Україною та окремою країною (коаліцією держав) пропонується визначати за методикою оцінки ВПО [4, С.37-39], застосовуючи відповідні індекси напруженості:

- 0 - 0,2 – спокійна;
- 0,3 - 0,4 – загострена;
- 0,5 - 0,7 – кризова;
- 0,8 - 0,9 – конфліктна;
- 1 – ВПО стану війни.

Таблиця 1

Оцінювання рівня напруженості двосторонніх відносин між Україною та сусідніми державами

№ з/п	Показники	Польща	РФ	Важливість показника
1.	Наявність територіальних претензій до України	0,4	0,8	0,6
2.	Ступінь підтримки сепаратистських сил в Україні	0,2	1	0,6
3.	Відносини з Україною у економічній, фінансовій, торговій сферах	0,2	0,8	0,5
4.	Прагнення до домінування в регіоні	0,6	0,9	<b>0,75</b>
5.	Співвідношення воєнних потенціалів як потенційна загроза	0,1	0,9	0,5
6.	Ступінь соціально-політичної нестабільності у сусідніх країнах	0,2	0,6	<b>0,4</b>
7.	Рівень впливу закордонних релігійних центрів на конфесії в Україні	0,3	0,9	0,6
8.	Заяви й акції, які дискредитують внутрішню і зовнішню політику України	0,4	0,8	0,6
9.	Наявність значних військових формувань поблизу кордонів України	0,2	0,9	0,55
10.	Спроби втручання у внутрішні справи України	0,2	0,9	0,55
<b>Рівень напруженості</b>		<b>0,28</b>	<b>0,85</b>	

Застосування даної методики, дає можливість отримати вихідні дані для наступного етапу дослідження. Після визначення ймовірного осередку конфлікту необхідно спрогнозувати його можливі результати. В цьому аспекті достатньо ефективною виявилася методика прогнозування результатів можливого міжнародного конфлікту по К. Райту [6]. Він запропонував обирати в якості вихідних даних: рівень важливості національних інтересів, які відстоюються в конфлікті; бойові можливості угруповань військ, що безпосередньо беруть участь у збройному протистоянні; вартість ресурсного забезпечення конфлікту; вплив світової

спільноти на учасників конфлікту; воєнно-економічні потенціали сторін, включаючи можливості союзників; рівень можливих втрат у ході воєнних дій.

Методику оцінки результатів можливого міжнародного конфлікту ( $D_x$ ) між сторонами X та Y у визначений момент оцінки ( $dt$ ) по Квінсі Райту [6] можна подати у вигляді:

$$D_x/d_t = (N_x + F_x) - (C_x + W_x) + (P_x - P_y) - (V_x - V_y),$$

$$D_y/d_t = (N_y + F_y) - (C_y + W_y) + (P_y - P_x) - (V_y - V_x)$$

де:  $N_x$  і  $N_y$  – рівень важливості національних інтересів відповідно для суб'єктів X і Y, які відстоюються у конфлікті;

$F_x$  і  $F_y$  – бойові потенціали угруповань військ сторін X і Y, що безпосередньо беруть участь у збройному протистоянні;

$C_x$  і  $C_y$  – «вартість» конфлікту для сторін X і Y (витрати на озброєння, матеріальні і людські втрати);

$W_x$  і  $W_y$  – тиск на сторони X і Y світової громадської думки на користь мирного вирішення конфлікту;

$P_x$  і  $P_y$  – воєнно-економічні потенціали сторін X і Y (включаючи союзників);

$V_x$  і  $V_y$  – рівень можливих втрат сторін X і Y у ході воєнних дій.

Розраховане чисельне значення вказує ступінь готовності до нарощування або згортання конфлікту. За матеріалами іноземних видань зазначена методика була апробована на даних 45 конфліктів [8], що відбулися в світі після Другої світової війни та довела свою високу ефективність. Разом з тим, детальних відомостей про порядок отримання вихідних даних та прикладів використання методики, в силу специфіки області застосування, у відкритих джерелах немає.

Запропоновані К. Райтом підходи можна охарактеризувати таким чином:

методика відображає домінуючий на заході прагматичний підхід до прийняття рішень у галузі воєнної безпеки в цілому, і стосовно участі в воєнному конфлікті зокрема. Сутність такого підходу полягає в тому, що рішення про підготовку або початок воєнного конфлікту приймається на основі ретельного аналізу співвідношення можливих втрат та вигравів як у результаті розгортання воєнного конфлікту, так і у випадку пасивної реакції;

в основу розрахунків покладено, так би мовити, „математизацію” основних законів війни;

- в методиці пропонується вважати рівними вагові коефіцієнти всіх чинників;

в методиці занадто опосередковане врахування, що зведене до врахування суспільної думки;

не враховуються непередбачувані обставини, що завжди істотно впливають на результат воєнного конфлікту.

Тому напрямками формування придатної для оперативних розрахунків методики прогнозування результатів можливого воєнного конфлікту можна вважати введення вагових коефіцієнтів для

кожного компоненту, додаткове врахування морального та інтелектуального чинників та врахування невизначеності.

Залишаючи в основі розрахунків прагматичний підхід, необхідно детальніше зупинитись на закономірностях, що встановлюють залежність ходу і результатів конфліктів від різнорідних чинників, які і будуть покладатись в основу розрахунків.

Питання ведення війни і вибору найкращої стратегії для перемоги розглядалось філософами з античних часів на протязі всієї історії людства. Довели свою життєздатність погляди Сун-цзи, який вважав, що перемога залежить від „Дао, Неба, Землі, Полководця і Закону”. Надалі закони та закономірності війни були узагальнені, проте можливість використання їх для математичних розрахунків та розробки рекомендацій для військово-політичного керівництва не розглядалась.

Слід також зазначити, що в теоретичних доробках вітчизняних вчених існує низка фундаментальних положень, які дозволяють прогнозувати результати можливого міжнародного воєнного конфлікту з високим ступенем імовірності та пропонується низка закономірностей збройної боротьби [7].

Можливість об'єднання закономірностей у групи та врахування підходів, запропонованих К.Райтом, дозволяють по-новому підійти до прогнозування результатів можливого міждержавного воєнного конфлікту. Зокрема, додатково врахувати рівень розвитку воєнного мистецтва сторін учасниць конфлікту, готовність населення і особового складу збройних сил до ведення конфлікту, та врахувати непередбачувані обставини, які майже завжди виникають у ході ведення конфлікту.

Придатну для використання в практиці функціонування воєнної сфери держави методику оперативного прогнозування результатів можливого воєнного конфлікту у визначений період часу в загальному вигляді можна запропонувати в такому вигляді:

$$D_x / d_t = k_N N_x + k_F F_x - k_C C_x - k_W W_x + k_P (P_x - P_e) - k_V (V_x - V_y) + k_M (M_x - M_y) + k_S S_x + \delta;$$

$$D_y / d_t = k_N N_y + k_F F_y - k_C C_y - k_W W_y + k_P (P_y - P_x) - k_V (V_y - V_x) + k_M (M_y - M_x) + k_S S_y + \delta$$

де:  $k_N, k_F, k_C, k_W, k_P, k_V, k_M, k_S$  – коефіцієнти відносної важливості;

$N_x$  і  $N_y$  – рівень важливості національних інтересів для суб'єктів  $X$  і  $Y$ , які відстоюються в конфлікті;

$F_x$  і  $F_y$  – бойові потенціали угруповань військ сторін  $X$  і  $Y$ , що безпосередньо беруть участь у збройному протистоянні;

$C_x$  і  $C_y$  – відносна вартість конфлікту для сторін  $X$  і  $Y$  ( витрати на озброєння, матеріальні і людські втрати);

$W_x$  і  $W_y$  – тиск на сторони  $X$  і  $Y$  світової громадської думки на користь мирного вирішення

конфлікту;

$P_x$  і  $P_y$  – воєнно-економічні потенціали сторін  $X$  і  $Y$  (включаючи союзників);

$V_x$  і  $V_y$  – рівень можливих втрат сторін  $X$  і  $Y$  в ході воєнних дій;

$M_x$  і  $M_y$  – рівень розвитку воєнного мистецтва сторін  $X$  і  $Y$ ;

$S_x$  і  $S_y$  – готовність населення і особового складу збройних сил сторін  $X$  і  $Y$  до ведення конфлікту;

$\delta$  – коефіцієнт невизначеності.

Значення всіх складових формули доцільно стандартизувати та розглядати в межах від 0 до 1.

Зокрема:

коефіцієнти важливості ( $k$ ) доцільно обчислювати методами експертних оцінок та аналізу ієрархій;

рівень важливості національних інтересів ( $N_x$  і  $N_y$ ) оцінювати методом експертних оцінок у межах від 0 до 1, де 0 – другорядний інтерес, 1 – життєво важливий інтерес;

бойові можливості угруповань військ, що безпосередньо беруть участь у збройному протистоянні ( $F_x$  і  $F_y$ ) оцінювати за формулами

$$F_x = \frac{B_x}{B_x + B_y}, F_y = \frac{B_y}{B_x + B_y}, \text{ де } B_x, B_y - \text{ бойові}$$

потенціали збройних сил сторін після приведення його до вигляду  $V_x:V_y$ .

відносну вартість конфлікту для сторін  $X$  і  $Y$  оцінювати в співвідношенні витрат на ведення конфлікту та внутрішнього валового продукту за

$$\text{формулою } C_x = \frac{K_x}{E_x}, C_y = \frac{K_y}{E_y}, \text{ де } K_x, K_y -$$

вартість матеріальних витрат і втрат для сторін;  $E_x, E_y$  – золотовалютний резерв сторін  $X$  і  $Y$ ;

тиск світової громадської думки на користь мирного вирішення конфлікту оцінювати методом експертних оцінок у межах від 0 до 1, де 0 – не сприйняття світової думки військово-політичним керівництвом сторони, 1 – повне підпорядкування вимогам світової спільноти;

воєнно-економічні потенціали сторін визначати через співвідношення золотовалютних сторін

$$\text{конфлікту } P_x = \frac{E_x}{E_x + E_y}, P_y = \frac{E_y}{E_x + E_y}, \text{ де } E_x,$$

$E_y$  – золотовалютний резерв сторін  $X$  і  $Y$ .

рівень можливих втрат сторін оцінювати методом експертних оцінок у межах від 0 до 1, де 0 – невідчутні втрати, 1 – неприпустимі втрати;

рівень розвитку воєнного мистецтва сторін  $X$  і  $Y$  оцінювати методом експертних оцінок у межах від 0 до 1;

готовність населення і особового складу збройних сил сторін  $X$  і  $Y$  до ведення конфлікту оцінювати методом експертних оцінок у межах від 0 до 1;

$\delta$  – коефіцієнт невизначеності враховує непередбачувані чинники, які можуть виникнути в

ході ведення конфлікту і дозволяє відображати результати розрахунків у визначеному інтервалі. Коефіцієнт невизначеності пропонується визначати в інтервалі  $(-0,5;0,5)$ .

За такого варіанта отримання вихідних даних значення  $Dx/dt$  та  $Dy/dt$  може коливатись у межах від  $-5,5$  до  $+5,5$ .

Якщо результат розрахунку має від'ємне значення, це свідчить про несприятливий прогноз результату конфлікту і вимагатиме термінового управляючого впливу.

Для аналізу розрахунків доцільно використовувати шкалу оцінки результатів можливого конфлікту (рис.1).

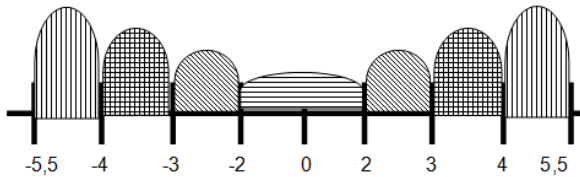


Рис.1. Шкала оцінки результатів можливого конфлікту

Результати оцінки в межах від  $-2$  до  $2$  вказують, що конфлікт є малоімовірним через незначні шанси досягнення мети будь-якою з сторін.

Результати оцінки в межах від  $2$  до  $3$  в залежності від знаку результату розрахунків вказують на зростання імовірності розв'язання конфлікту.

Результат оцінки в межах від  $3$  до  $4$  свідчать про готовність однієї зі сторін до розгортання

воєнного конфлікту.

Оцінки в межах від  $4$  до  $5,5$  свідчать про фактичну невідворотність конфлікту з прогнозованим результатом [8].

### Висновки і перспективи подальших досліджень

Запропонований варіант поєднання методик визначення рівня конфліктогенності у міждержавних відносинах та прогнозування результатів можливого воєнного конфлікту дозволяє оперативно, із залученням доступних вихідних даних і обмеженої кількості експертів, з високою ефективністю прогнозувати наслідки прийняття воєнно-політичного рішення з більш повним врахуванням чинників, що впливають на хід і результат конфлікту.

Таким чином, використання результатів проведеного дослідження дозволяє прогнозувати результати можливого воєнного конфлікту та обґрунтовувати шляхи зниження рівня напруженості у взаємовідносинах між країнами регіону. Перспективами подальших розвідок у даному напрямку досліджень є моніторинг та прогнозування рівня воєнної небезпеки для України з боку країн-сусідів.

Надалі методика прогнозування результатів можливого воєнного конфлікту може бути доведена до програмного продукту і забезпечити автоматизацію процесу визначення вихідних даних і отримання результатів розрахунків.

### Література

1. **Wright Q.** Problems of Stability and Progress of International Relations. Politics and International Stability. Berkeley and Los Angeles: University of California Press, 1954. P. III. Ch. 8. P. 129. 2. **Закон України** "Про національну безпеку України" від 21.06.2018 р. № 2469-VIII. 3. **Косецов В. О., Телелим В. М., Шевченко В. І.** Оцінка стану воєнної безпеки України // Наука і оборона. – 1998. №2 – С. 3-6. 4. Методика оцінки воєнно-політичної обстановки. – К.: НДІ ГУР МОУ, 2016. – 82 с. дск, інв. НУОУ № 16613. 5. **Грабовецький Б. Є.** Методи експертних оцінок: теорія, методологія, напрямки використання:

монографія / – Вінниця: ВНТУ, 2010. – 171 с. 6. **Wright Q.** The escalation of International Conflict/ - The Journal of Conflict Resolution. 1965. Vol. IX. №4. p.435. 7. **Щипанський П.В., Крикун П.М., Устименко О.В.** Нове безпекове середовище - прогнозовані виклики та загрози національній безпеці України // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського. - №1(53), 2015. – С.107-112. 8. **Пунда Ю.В.** Методика прогнозування результатів можливого воєнного конфлікту. Труды академії, – № 1(88), – 2009, – с. 40-46.

### МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ УРОВНЯ КОНФЛИКТНОСТИ МЕЖГОСУДАРСТВЕННЫХ ОТНОШЕНИЙ

**Юрий Васильевич Пунда (доктор военных наук, с.н.с.)**

**Иван Павлович Козинец (кандидат исторических наук, с.н.с.)**

**Владимир Степанович Клименко (кандидат политических наук, доцент)**

**Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина**

*В широком спектре проблем обеспечения национальной безопасности важная роль определена военной сфере. Оценивая реальности сегодняшнего дня, не следует пренебрегать понятием "военная опасность", которая рассматривается как потенциальная возможность любого государства (группы государств) относительно применения военной силы для решения межгосударственных противоречий.*

*Несмотря на задекларированное в стратегических документах большинства государств и международных межправительственных организаций стремление к решению противоречий мирным*

путем, прогнозирование результатов возможных конфликтов остается важной задачей, за результатами которой можно более объективно принимать военно-политические решения.

В данной статье авторы поставили перед собой задачу предложить вариант методического подхода к определению уровня конфликтности межгосударственных отношений, который целесообразно внедрить в процесс подготовки специалистов государственного военного управления. Путем последовательного применения различных методик предполагается определить возможный очаг конфликта и спрогнозировать его возможные результаты. Авторами предложено ряд собственных научных и методических доработок, что определяет перспективы дальнейших поисков в данном направлении исследований, мониторинге и прогнозировании уровня военной опасности со стороны соседних государств.

**Ключевые слова:** межгосударственные отношения, военно-политическая обстановка, военный конфликт, национальная безопасность, национальные интересы, территориальная целостность, суверенитет.

## METHODOLOGICAL APPROACHES TO DETERMINING THE CONFLICT LEVEL OF INTER-STATE RELATIONS

*Yuri Punda (Doctor of Military Sciences, PhD)*

*Ivan Kozynets (Candidate of Historical Sciences, PhD)*

*Volodymyr Klimenko (Candidate of Political Science, Associate Professor)*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*Military field plays an important role among a wide range of national security issues. In assessing the realities of today, we should not neglect the concept of "military danger", which is seen as a potential opportunity of any state (group of states) to use military force to resolve interstate contradictions.*

*Despite the stated in the strategic documents of the majority of states and international intergovernmental organizations the desire to resolve conflicts peacefully, the results prediction of possible conflicts remains an important task and can help to make military and political decisions more objectively.*

*In this article, the authors have set the task of proposing a methodological approach to determining the level of conflict of interstate relations, which should be implemented in the process of staff military management training. By combining different techniques, it is intended to determine the likely focus of a possible conflict and predict its possible outcomes. The authors propose a number of their own scientific and methodological achievements, which determines the prospects for further research, monitoring and forecasting of the level of military danger by neighboring countries.*

**Key words:** interstate relations, military-political situation, military conflict, national security, national interests, territorial integrity, sovereignty.

### References

- 1. Wright Q.** Problems of Stability and Progress of International Relations. Politics and International Stability. Berkeley and Los Angeles: University of California Press, 1954. P. III. Ch. 8. P. 129.
- 2. Law of Ukraine** "On National Security of Ukraine" dated 21.06.2018 № 2469-VIII.
- 3. Kosevtsov V.A., Telelim V.M., Shevchenko V.I.** Evaluation of the state of military security of Ukraine // Science and Defense. - 1998. №2 - P. 3-6.
- 4. Methods** of evaluation of the military-political situation. - K.: MOU GUR Research Institute, 2016. - 82 p. board, inv.
- 5. Grabovetsky B. E.** Expert Assessment Methods: Theory, Methodology, Directions of Use: Monograph / - Vinnytsia: VNTU, 2010. - 171 p.
- 6. Wright Q.** The escalation of International Conflict/ - The Journal of Conflict Resolution. - 1965. - Vol. IX. - №4- p.435.
- 7. Shchipanskiy P.V., Krykun P.M., Ustyenko O.V.** New Security Environment - Predictable Challenges and Threats to National Security of Ukraine // Collection of scientific papers of the Center for Military-Strategic Studies of Ivan Chernyakhovsky National University of Defense of Ukraine. - №1 (53), 2015. - P.107-112.
- 8. Punda Y.V.** Methods for predicting the outcome of a possible military conflict // Proceedings of the Academy, - № 1 (88), - 2009, - p. 40-46.

## ОСОБЛИВОСТІ СУЧАСНИХ ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

*Актуальність дослідження визначається продовженням бойових дій в окремих районах Донецької та Луганської областей, потужною інформаційною кампанією спрямованою на особовий склад Збройних Сил України, населення непідконтрольних Україні територій, а також на громадян інших держав.*

*Методом аналізу наукових праць та публікацій досліджуються психологічні операції, як складова стратегічних комунікацій, визначаються особливості проведення психологічних операцій під час анексії Автономної Республіки Крим та окупації частини Донецької та Луганської областей, наводиться орієнтовний склад підрозділів, які залучені до інформаційно-психологічних операцій на Сході України. Наголошується, що залежно від масштабів проведення й конкретних цілей психологічні операції ведуться на стратегічному, оперативному і тактичному рівнях. З'ясовано, що психологічні операції є невід'ємною частиною політики в умовах гібридної війни і координуються на державному рівні.*

*Структура підрозділів психологічних операцій противника характеризується тим, що в основному вони є штатним і практично незмінним спеціальним апаратом штабів із конкретними завданнями, які реалізуються через повний спектр каналів комунікацій. Також акцентовано увагу на тому, що підрозділи психологічних операцій мають змінну структуру залежно від покладених на них завдань та обстановки, в якій доведеться виконувати поставлені завдання. Запропоновані пропозиції для підвищення ефективності протидії інформаційно-психологічному впливу.*

**Ключові слова:** стратегічні комунікації, інформаційно-психологічний вплив, інформаційна операція, психологічна операція, сили та засоби психологічних операцій.

### Вступ

Серед актуальних воєнних загроз для України поруч з іншими визначено цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу нашої держави, залякування населення, позбавлення його волі до опору, активізація спеціальними службами противника розвідувально-підривної діяльності в Україні з метою дестабілізації внутрішньої соціально-політичної обстановки в Україні [1]

Виходячи із зазначених загроз, гарантування безпеки держави, особистості й суспільства на сьогодні – це комплексне завдання, реалізація якого значною мірою залежить від використання військових, політичних, економічних, інформаційних, психологічних засобів.

**Постановка проблеми.** Однією з форм протидії інформаційно-психологічному впливу є побудова дієвої системи стратегічних комунікацій Міністерства оборони України та ЗС України. Український правочин передбачає створення державної системи стратегічних комунікацій. Так, в Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України (затверджена наказом Міністерства оборони України 22.11.2017 № 612) визначається “Дієвим, адекватним та комплексним

інструментарієм ... виступає система стратегічних комунікацій, яка дає можливість ... організувати ефективну відсіч деструктивним інформаційним кампаніям, які веде агресор”.

В цих умовах існуюча система інформаційно-психологічної протидії нашої держави негативним впливам вимагає врахування можливостей сил та засобів інформаційно-психологічних операцій (ІПСО), завдань які вони вирішують, а особливо на Сході нашої держави. [2]

Суспільно-політична обстановка на тимчасово окупованих територіях Донецької та Луганської областей залишається складною. Незважаючи на розведення сил та засобів, не відновлений контроль над кордоном.

Напруження в гуманітарній та соціальній сферах життя місцевих мешканців викликають окупація окремих районів областей, що триває, постійна напружена деструктивна антиукраїнська діяльність ЗМІ та пропагандистська діяльність громадських організацій різної спрямованості, які контролюються військово-політичним керівництвом РФ, котра продовжує ведення політики направленої на створення умов для проросійського патріотичного виховання місцевого населення.[3]

Це актуалізує проблему дослідження інформаційно-психологічного впливу, як

прихованого так і відкритого, і недооцінка його під час загострення військово-політичного конфлікту може мати критичний характер та викликати фатальні наслідки.

**Аналіз останніх досліджень і публікацій.** Наукові дослідження інформаційно-психологічного впливу (ІПВ) на свідомість, психіку і поведінку військовослужбовців та населення країни противника в ході збройної боротьби свідчать про те, що ця галузь науки досить тривалий час була закритою, маловідомою для широкої громадськості. Специфіка цієї проблематики полягає також і в тому, що публічне висвітлення цієї діяльності – це лише частина видимого спектра проблеми. Задуми ПсО, технології їх здійснення ще багато років будуть недоступні для широкого загалу.

Між тим, на сьогодні немає повноцінних досліджень з аналізу інформаційно-психологічних операцій в умовах конфлікту на Сході України, а власне психологічної складової – психологічних операцій (ПсО). Така важлива тема потребує більш глибокого дослідження.

**Метою статті є** розкриття особливостей ведення ПсО, а також складу та завдань підрозділів, що залучаються до їх проведення в умовах гібридної війни.

### **Виклад основного матеріалу дослідження**

У сучасному інформаційному просторі Україна стала об'єктом гібридної війни, яка має всі ознаки організованої спеціальної інформаційно-психологічної операції з боку РФ, метою яких є постійний цілеспрямований ІПВ як на особовий склад Збройних Сил України (ЗС України), так і на населення нашої держави. Головною тенденцією, що впливає на розвиток воєнно-політичної обстановки довкола України, є поширення практики проведення ПсО та дій провокаційного характеру для створення конфліктних ситуацій.[1]

Слід визнати, що інформаційну та психологічну боротьбу люди ведуть здавна, але раніше вона не мала такого масштабного характеру, як сьогодні, і взагалі, про неї намагались не говорити, ніколи та ніде не афішувати. Вона була, головним чином, результатом ініціативи видатних полководців, а також відповідних органів і структур. Більше того, документи про конкретні особливості її проведення зберігають в таємниці. Відомо тільки, що фахівці психологічної війни акумулювали у своїй практиці всі скільки-небудь ефективні способи впливу на людські емоції й свідомість.

Аналіз ведення психологічних операцій [5,6] проти України показує, що використовуються всі сили та засоби проти своїх противників. Перед усім – це такий вплив на індивіда інформаційно-психологічними або іншими засобами, який викликає трансформацію психіки, зміну поглядів, думок, відносин, ціннісних орієнтацій, мотивів, стереотипів особистості з метою вплинути на її

діяльність і поведінку. Кінцевою його метою є досягнення певної реакції, поведінки (дії або бездіяльності) особистості, яка відповідає цілям психологічного впливу. Розрахунок робиться на те, що психіка людини найбільш уразлива, впливаючи на неї, можна особистий страх перетворити в масове боягузтво, сумніви – у недовіру, роздратування – у лють.

Отже, психологічний вплив (ПсВ) це прямий або опосередкований вплив на свідомість, підсвідомість та психіку цільової аудиторії з метою стимулювання певних змін в її поведінці. [4] Успішно вирішувати це завдання вдається завдяки оптимальній комбінації всіх форм і способів протиборства, включаючи до них й психологічну операцію.

Основна ціль ПсО полягає в зміні поведінки осіб, що приймають рішення, або цільової аудиторії противника. Це припускає, крім іншого, сформувати в нього переконання в безглуздість подальшого опору, позбавити віри у свій успіх, тобто змінити його ставлення до ситуації.

Як показало дослідження ПсО, фахівці розглядають її як активні дії ворогуючих сторін в інформаційно-психологічній сфері. Ведеться в мирний і воєнний час. Містить комплекс заходів, спрямованих на зміну поведінкових і емоційних установок певних груп людей і окремих осіб з тих або інших питань у бажаному напрямку. У збройних силах ці заходи здійснюються з метою підриву морально-психологічного стану військ і населення противника, захисту від ІПВ з його боку [7].

Керівними документами ПсО визначається як сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом психологічних акцій, психологічних дій та інших дій суб'єктів ПсО, які проводяться за єдиним замислом і планом для здійснення впливу на емоційний стан, мотивацію, раціональне мислення визначених цільових аудиторій та зміни моделей їх поведінки у спосіб, що сприятиме досягненню політичних і військових цілей. [4] ПсО – головний елемент змісту психологічної боротьби. Її проведення передбачає використання складної сукупності погоджених, скоординованих і взаємозалежних за цілями, завданнями, місцем й часом, об'єктами і процедурами видів, форм, способів і прийомів ПсВ. Її основними формами є друкована й усна пропаганда, пропаганда за допомогою теле-, радіо- і відео- засобів. До безпосередніх заходів ПсВ можуть залучатися психологи, психофізіологи, лікарі-психіатри, журналісти, артисти, військовополонені [8].

ПсО організується й ведеться на основі відповідних рішень командувачів (начальників) і розпоряджень штабів. У збройних силах існують спеціальні органи й підрозділи для вирішення цих завдань. В структурі збройних сил РФ ці завдання покладаються на сили спеціальних операцій та війська інформаційних операцій (рис 1)

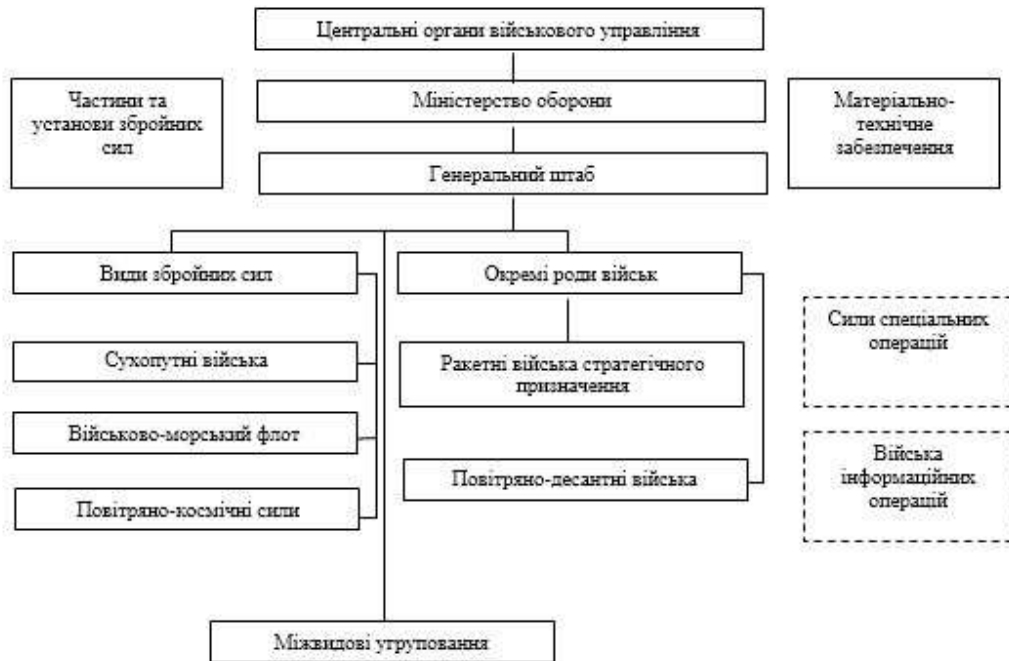


Рис 1. Місце спеціальних органів ПсО в структурі збройних сил РФ.

Залежно від масштабів проведення й конкретних цілей ПсО ведеться на стратегічному, оперативному і тактичному рівнях. Отже, розглянемо класифікацію ПсО.

Стратегічна ПсО – це комплекс різнобічного психологічного впливу на війська і населення як своєї, так і чужої (ворожої) країни з метою формування у них системи певних поглядів і ціннісних орієнтирів, які спрямовані на зміцнення (у своїх військах і населення) або руйнування (у військах і населення противника) морально-психологічного стереотипу, що сприяє у першому випадку формуванню морально-психологічної стійкості, надійності і в цілому високого рівня морально-психологічного стану, а в другому – його пониження. Стратегічні ПсО плануються і розробляються на рівні керівництва збройних сил та спеціальних державних органів. загальні принципові настанови, завдання і цілі, які формує керівництво збройних сил, складають концептуальні схеми стратегічних ПсО, де закладаються довготривалі цілі та способи їх досягнення, сили і засоби, визначаються етапи і проміжні цілі, методи визначення ефективності психологічного впливу на перших етапах з метою його корекції і т.ін.

Оперативні ПсО здійснюються на свої війська і на війська противника. Оперативна ПсО на особовий склад угруповань військ, які протистоять нашим військам, спрямована на підрив у них віри в можливість виконання поставлених бойових завдань, злам волі до опору, скосування ініціативи, зниження готовності і здатності мобілізувати свої духовні і фізичні сили в ході бойових дій та зробити спроби до збереження власного життя домінуючим мотивом в поведінці, а також орієнтувати військовослужбовців на навмисне

ухилення від участі в бойових діях, відмову від продовження подальшого опору, здачу в полон тощо. Оперативні ПсО на свої війська – це комплекс різнобічного впливу на свідомість військовослужбовців з метою формування у них міцного і стійкого морально-психологічного стереотипу, який забезпечує здоровий морально-психологічний стан, високу бойову активність та готовність виконувати будь-які поставлені командуванням завдання.

Тактичні ПсО на свої війська та війська противника здійснюються з метою вирішення ситуативних морально-психологічних завдань, які виникли в ході оборонних, наступальних або контрастнаступальних дій в смугі дій тактичного з'єднання, або на окремій ділянці дій об'єднання військ (сил). Тактичні ПсО на війська противника здійснюються з метою викликати негативні ситуативні психічні стани окремих військовослужбовців і груп, створити нездоровий психоз, паралізувати психіку в період конкретних бойових дій, забезпечити низьку ефективність застосування зброї та бойової техніки. Тактичні ПсО на свої війська мають за мету підготовку особового складу до виконання конкретних завдань військової діяльності в мирний і воєнний час, ліквідацію будь-якого негативного соціально-психологічного явища чи процесу, формування певних психологічних настанов.

Відповідно до спрямованості психологічні операції можуть бути проти цивільного населення, проти військ противника, проти командування противника, консолідуючі психологічні операції, а також сприяти опозиції та дисидентським рухам, здійсненню культурної експансії та диверсії. [9]

Аналіз досвіду інформаційно-психологічних операцій РФ свідчить, що ПсО стали невід'ємною

частиною її політики і координується на державному рівні. У цьому сенсі вона не тільки випередила розвинені європейські країни, а й стала суперничати в питаннях інформаційно-психологічного впливу зі США та Китаєм. Ця робота набула нових особливостей:

цілеспрямована координація діяльності засобів масової інформації і відповідних структур військового відомства РФ, а саме: тісна взаємодія сил спеціального призначення і військ для проведення психологічних операцій;

комплексний інформаційно-психологічний вплив на своє населення, населення східних регіонів, в цілому України, світову громадськість.

визнання легітимності незаконно утворених ДНР та ЛНР їх політичної системи та символічних атрибутів, спільної ідентичності їхніх громадян (“русского мира”);

Так, проведення воєнно-політичним керівництвом РФ незаконної анексії Крима супроводжувалось діями, які мали всі ознаки підготовленої та продуманої за цілями, заходами та наслідками ПсО, скерованої в першу чергу на російську аудиторію, а вже потім – на українську та західну [5, 6, 9].

Об’єктами психологічного впливу були визначені:

аудиторія об’єкта нападу – Україна (для формування у населення думки про справедливість рішень РФ і планів російського керівництва);

внутрішня аудиторія РФ та аудиторії підтримуючих її держав (для демонстрації впевненості дій російського керівництва і формування у населення думки щодо підтримки дій Кремля);

зовнішня аудиторія (для створення інформаційних умов позитивного сприйняття політики РФ).

Ключовими завданнями цієї операції було:

деморалізація населення України, поширення панічних настроїв та протестних рухів;

деморалізація особового складу збройних сил та силових відомств, підрив довіри до свого воєнно-політичного керівництва, а також спонукання їх до державної зради й переходу на бік супротивної сторони;

формування у громадян РФ та України викривленого “медіабачення” подій, що відбуваються, а не їх дійсних причин та наслідків;

створення вигляду масової підтримки дій РФ з боку населення Південно-Східних регіонів України;

психологічна підтримка українських прихильників радикального зближення регіонів Сходу й Півдня України з РФ.

Зазначені завдання реалізувались через майже повний спектр каналів комунікацій, до яких передусім слід віднести: традиційні ЗМІ; електронні ЗМІ (телебачення); інтернет ЗМІ; соціальні мережі. При цьому використовувалися усі методи інформаційно-психологічної боротьби

– від розміщення тенденційною інформації та напівправди до неприхованої неправди (“фейку”). Відповідно до мети та умов проведення конкретної ПсО можуть визначатися й інші завдання психологічного впливу, які спрямовуються на представників органів державної влади, військового командування, особовий склад військ та цивільне населення.

Крім того, були використані і більш традиційні заходи, що мали посилити вплив зазначених каналів на населення (як російське, так і українське), зокрема – перешкоджання діяльності ЗМІ на Кримському півострові, спроби припинення функціонування мережі Інтернет. Також використовувались механізми блокування веб-ресурсів, що активно спростовували (могли спростовувати) неправдиві повідомлення. Зокрема, на виконання вимог Роскомнагляду в соцмережі “В контакте” було заблоковано сторінки “Правого сектору” (начебто за розміщення заклику до Доку Умарова розпочати терористичну активність у Росії та “Євромайдану”. [8,10]

Слід зазначити, що воєнно-політичне керівництво РФ приділяє важливу увагу підготовці апарату ПсО як одного з вагомих елементів забезпечення будь-яких видів операцій. При цьому значна увага надається вдосконаленню концепцій застосування цих сил, їхньої структури, матеріально-технічної бази, а також рівня підготовки фахівців. ПсО віднесли до одного з найважливіших видів оперативного забезпечення і їх підготовка розглядається як комплекс заходів, що включає: планування операції; організаторську роботу; підготовку органів управління та суб’єктів ПсО до виконання завдань; підготовку каналів, джерел здійснення психологічного впливу, районів і місць проведення заходів в її інтересах. Загальне керівництво й контроль над організацією ПсО здійснює начальник штабу через начальника розвідки [9].

Безпосереднім організатором виконання заходів ПсО є начальник відділу (відділення, групи) ПсО. Він відповідає за стан бойової й мобілізаційної готовності підлеглих частин і підрозділів психологічних операцій і управління ними. Особливістю моделі органів ПсО, є те, що її підрозділ є штатним і практично незмінним спеціальним апаратом штабів всіх рівнів.

Управління силами й засобами психологічної боротьби, здійснюється з пункту управління розвідкою, створюваних у загальній системі пунктів управління військами, на якому розміщається основний склад відділу (відділення, групи) ПсО.

На відділ ПсО покладають: вивчення, оцінка соціально-психологічної обстановки, показників психологічного стану військ конфронтуючого угруповання супротивника й місцевого населення в районі бойових дій; вироблення пропозицій командуючому, начальнику штабу, з питань психологічної боротьби; розробка плану психологічної боротьби, своєчасна підготовка й



доведення розпоряджень (бойових розпоряджень); розробка основних матеріалів інформаційно-психологічного впливу; узагальнення й доведення до військ досвіду ведення психологічної боротьби; контроль виконання поставлених завдань.

До складу частин та підрозділів, які займаються ПсО на Сході України увійшли:

загін ПсО – здійснює основну керівну роль в інформаційно-психологічних заходах на території України. Його завданнями є збір, обробка і аналіз інформації про поточний морально-психологічний стан населення України і військових підрозділів (зона інтересів загону ПсО поширюється на усю територію України), керівництво підрозділами ПсО, що виконують спеціальні завдання з інформаційного впливу, розробка і здійснення інформаційно-психологічних операцій на території України. Дислокується біля м. Ростов-на-Дону спільно з пунктом управління розвідцентру Головного розвідувального управління (ГРУ) ГШ збройних сил РФ;

оперативні групи ПсО (4 групи) – мобільні підрозділи у складі 2-4 осіб, які на території окупованого Донбасу виконують завдання з усної пропаганди, поширення пропагандистської літератури та іншої необхідної інформації, створення пропагандистських груп в населених пунктах, що складаються з місцевих активістів, та організації і координації їхніх дій, сприяння роботі російських журналістів, збору інформації і визначення найбільш гострих проблем у населення для використання цього як інформаційного приводу, моніторингу поточного морально-психологічного стану місцевого населення;

групи спеціальних журналістів (8-10 окремих груп) – працюють безпосередньо на російській інформаційні канали. До їхнього складу входять 3-4 особи – журналіст, оператор, водій, може бути охоронець;

агенти диверсійної психологічної роботи в інших областях України – фахівці від ГРУ або ФСБ, які виконують завдання зі створення диверсійно-пропагандистських груп серед місцевого авторитетного населення, навчання місцевих груп проведенню підривних пропагандистських акцій, забезпечення груп необхідними матеріально-технічними засобами, безпосереднього проведенню мітингів, акцій протесту і поширення пропагандистських матеріалів.

Загін ПсО підпорядкований начальнику розвідки сил підтримки українських сепаратистів. На нього покладена роль командного центру інформаційно-психологічних операцій. Сам же загін ПсО не має постійної структури. Існуюча структура доповнюється відповідно до покладених завдань. У загоні ПсО, як правило, функціонують такі штатні елементи:

штаб – організує виконання завдань з ефективного застосування підрозділів загону;

відділ поширення друкарської та іншої

пропагандистської продукції – поширює пропагандистські матеріали серед визначеної аудиторії;

відділ усної пропаганди – використовує звукопідсилюючу апаратуру (звукомовні станції), проводить індивідуальні бесіди з місцевим населенням, працюють з полоненими та ін.;

відділ пропаганди по радіо- і телевізійним каналам – забезпечує радіо- і телевізійне мовлення з використанням апаратних ресурсів на захопленій території або пересувних станцій;

відділ по роботі в Інтернет-просторі – приданий підрозділ, який виконує завдання з розвідки, блокування або зміни інформації в мережах, несанкціонованого входження в пристрої, пов'язані з Інтернетом;

редакція та друкарня – складають макети друкарських продуктів пропаганди та друкують їх. [9].

На початку 2014 року в армії РФ були створені кібер-війська, завданням яких є захист національних комп'ютерних мереж, що обслуговують оборонні потреби, а також проведення атак на мережі потенційного противника. Ця нова категорія оборонного відомства торкається сфери інформаційної війни в Інтернет-просторі в оперативних і стратегічних масштабах. За наявною інформацією, військові кібер-фахівці збройних сил РФ залучаються до виконання завдань інформаційно-психологічних операцій не лише по окупованому Донбасу, але й території всієї України.

Окрім цього, є дані, що фахівці інших підрозділів ПсО збройних сил РФ, що дислокуються за тисячі кілометрів від Донбасу, віддалено працюють в мережі Інтернет з контентного наповнення сайтів терористів ("Новороссія", "Сварог", "Штаб російської армії" та ін.), а також по троллінгу в соціальних мережах та блогах. Починаючи з вересня 2014 року до такої роботи стали залучати курсантів ВВНЗ.

Підрозділи збройних сил РФ, які входять до складу військ інформаційних операцій:

управління інформаційного протиборства головного оперативного управління Генерального штабу збройних сил РФ;

центр закордонної військової інформації й комунікації збройних сил РФ;

група закордонної військової інформації й комунікації ЧФ;

відділи й центри інформаційного протиборства військових округів, а також армій які входять до складу округів;

відділення інформаційного протиборства оперативних відділів армій і флотів і підлегли їм оперативні центри інформаційного протиборства;

окремі загони психологічних операцій;

загони психологічних операцій окремих розвідувальних бригад;

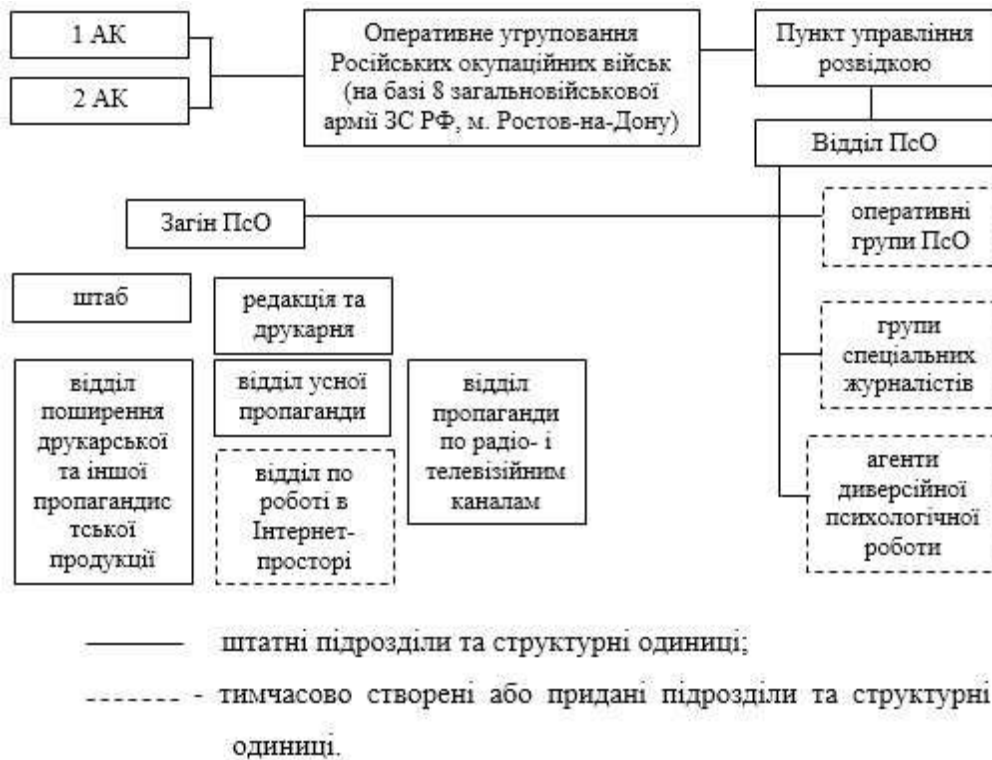


Рис 2. Орієнтовна структура підрозділів, яка здійснює заходи ПСО на Сході України.

Основними зразками озброєння загонів ПСО є: технічні засоби розсилання текстових повідомлень – комплекс радіоелектронної боротьби РБ-341В “Леер-3” із БПЛА “Орлан-10”;

технічні засоби організації телевізійного й радіомовлення – пересувний телемовний комплекс із віртуальною студією (МНИТИ), комплекс технічних засобів інформаційного забезпечення (МНИТИ);

технічні засоби для організації радіомовлення в мережах радіозв'язку супротивника – технічні засоби підрозділів зв'язку й РЕБ збройних сил РФ;

звукомовні станції – ЗС-82 “Декоратор”, ЗС-88 “Дільник”, ЗС-96.03, МЗС-83 “Грім”;

засоби виготовлення агітаційної друкованої продукції – похідні автотипографії БПК-63МКЛ, рухомий автоматизований видавничо-поліграфічний комплекс АТОФ-97, рухомі автоматизовані видавничо-поліграфічні комплекси “Журналіст”, пересувні цифрові друкарні ПЦД-07;

В інтересах поширення агітаційної друкованої продукції використовуються засоби доставки, які знаходяться на озброєнні загонів – 82-мм агітаційні мінометні міни А-832(А), 122-мм постріли ЗВА2 (ЗВА2Д) і ЗВА4 (ЗВА4Д) з агітаційним снарядом ЗА1 (ЗА1Д), 122-мм реактивні агітаційні снаряди 9М28Д, вертольоти, літаки, БПЛА “Орлан-10”.

### Висновки і перспективи подальших досліджень

Проведений аналіз ПСО на різних етапах їхнього становлення, оцінка можливостей, функцій та завдань органів управління ПСО в

збройних силах РФ дозволять відповідним органам ЗС України завчасно розробляти заходи протидії і формувати відповідні структури у власних військових формуваннях, підвищувати їх можливості в умовах гібридної війни. Необхідно враховувати те, що заходи ПСО розповсюджуються всіма доступними інформаційними каналами не лише на території АР Крим та окупованих частин Донецької та Луганської областей, а й на всю територію України.

Плануючи заходи щодо захисту населення та особового складу ЗС України, треба зважати на постійні зміни в структурі підрозділів ПСО, які відбуваються з метою виконання певних завдань та оперативно реагують на зміни обстановки.

З метою формування нормативної бази та розвитку можливостей Сил спеціальних операцій ЗС України доцільно прискорити відпрацювання проекту Настанови з психологічних операцій ЗС України та розробити методичні рекомендації військовим частинам інформаційно-психологічних операцій щодо підготовки та проведення заходів ПСО.

Закономірна постановка питання про розвиток промислового виробництва та забезпечення ЗС України необхідними технічними засобами. Захист населення та військ (сил) нашої держави від негативного інформаційно-психологічного впливу може здійснюватися лише цілеспрямованим використанням всіх наявних сил і можливостей держави. Скоординована система морально-психологічного забезпечення сил оборони

дозволить більш ефективно впливати на психіку окремого воїна і морально-психологічний стан військових колективів частин, підрозділів в цілому.

Потребують подальшого дослідження питання вивчення сучасного стану сил психологічних операцій армій передових країн НАТО та врахування його в ході проведення реформ у ЗС України.

### Література

1. Военная доктрина Украины: затв. Указом Президента Украины від 24 вересня 2015 року № 555/2015. URL: <https://zakon.rada.gov.ua/laws/show/555/2015> (дата звернення: 18.11.2019). 2. Нарис теорії і практики інформаційно-психологічних операцій: навч. посіб. / Дзюба М.Т., та ін.; за ред. В.В. Балабіна. Київ: ВПІ НТУУ “КПІ”, 2006. 471 с. 3. Військові новини. веб-сайт. URL: <https://www.unian.ua/war> (Дата звернення 11.11.2019). 4. Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України: затв. наказом Міністерства оборони України від 22.11.2017 № 612. URL: <https://zakon.rada.gov.ua/rada/show/v0612322-17>. (Дата звернення 11.11.2019) 5. **Алещенко В.І.** Феноменологія “гібридної війни” та її особливості у виконанні Російської Федерації: інформаційно-психологічний аспект. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки.* 2016. Вип. 1. С. 6-11. 6. Щодо інформаційно-

психологічної складової агресії Російської Федерації проти України (за результатами подій 1-2 березня 2014 року). URL: <http://www.niss.gov.ua/articles/1476/>. (Дата звернення 11.11.2019) 7. **Ліпкан В.А.** Сучасний зміст інформаційних операцій проти України. *Актуальні проблеми міжнародних відносин.* Випуск 102. Ч. I. 2011, С.34-43 8. **Гусаров В.** Силы информационных операций России: каким должен быть ответ Украины? URL: <http://sprotyv.info/ru/news/5931-sily-informacionnyhoperaciy-rossii-kakim-dolzen-byt-otvet-ukrainu>. (Дата звернення 11.11.2019) 9. **Певцов Г.В.** Аналіз структури, функцій та завдань органів управління інформаційно-психологічної боротьби в збройних силах провідних країн світу. *Наука і техніка Повітряних Сил Збройних Сил України.* №3(20). 2015. С. 37-46. 10. **Сафін О.Д.** Індоктринація як інструмент гібридної війни Росії. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки.* №2(37). 2017. С. 24-27.

## ОСОБЕННОСТИ СОВРЕМЕННЫХ ПСИХОЛОГИЧЕСКИХ ОПЕРАЦИЙ В УСЛОВИЯХ ГИБРИДНОЙ ВОЙНЫ

*Виктор Иванович Алещенко (доктор психологических наук, профессор)*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*Актуальность исследования определяется продолжением боевых действий в отдельных районах Донецкой и Луганской областей, мощной информационной кампанией направленной на личный состав Вооруженных Сил Украины, население неподконтрольных Украине территорий, а также на граждан других государств.*

*Методом анализа научных работ и публикаций исследуются психологические операции, как составляющая стратегических коммуникаций, определяются особенности проведения психологических операций во время аннексии Автономной Республики Крым и оккупации части Донецкой и Луганской областей, приводится ориентировочный состав подразделений, вовлеченных в информационно-психологические операции на Востоке Украины. Отмечается, что в зависимости от масштабов проведения и конкретных целей психологические операции ведутся на стратегическом, оперативном и тактическом уровнях. Выяснено, что психологические операции являются неотъемлемой частью политики в условиях гибридной войны и координируются на государственном уровне.*

*Структура подразделений психологических операций противника характеризуется тем, что в основном они являются штатным и практически неизменным специальным аппаратом штабов с конкретными задачами, которые реализуются через полный спектр каналов коммуникаций. Также акцентировано внимание на том, что подразделения психологических операций имеют переменную структуру в зависимости от возложенных на них задач и обстановки, в которой придется выполнять поставленные задачи. Предложены рекомендации для повышения эффективности противодействия информационно-психологическому воздействию.*

**Ключевые слова:** стратегические коммуникации, информационно-психологическое воздействие, информационная операция, психологическая операция, силы и средства психологических операций.

## PECULIARITIES OF MODERN PSYCHOLOGICAL OPERATIONS IN THE CONDITIONS OF THE HYBRID WAR

*Viktor Aleshchenko (Doctor of Psychological Sciences, Professor)*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*The relevance of the study is determined by the continuation of hostilities in some areas of Donetsk and Lugansk regions, a powerful information campaign aimed at personnel of the Armed Forces of Ukraine, the population of territories not controlled by Ukraine, as well as citizens of other countries.*

*The method of analysis of scientific works and publications investigates psychological operations as a component of strategic communications, determines the peculiarities of psychological operations during annexation of the Autonomous Republic of Crimea and occupation of part of Donetsk and Lugansk regions, gives the indicative composition of the units involved in information-psychological operations of Ukraine. It is emphasized that psychological operations are conducted at strategic, operational and tactical levels, depending on the scope and specific objectives. Psychological operations have been found to be an integral part of hybrid warfare policy and are coordinated at the state level.*

*The structure of units of psychological operations of the enemy is characterized by the fact that they are basically a full-time and practically unchanged special apparatus of staffs with specific tasks that are implemented through a full range of communication channels. Attention is also drawn to the fact that the units of psychological operations have a variable structure depending on the tasks assigned to them and the environment in which they will have to perform their tasks. Suggestions are made to improve the effectiveness of counteracting information and psychological impact.*

**Key words:** *strategic communications, information-psychological influence, information operation, psychological operation, forces and means of psychological operations.*

### References

1. Voienna doktryna Ukrainy: zatv. Ukazom Prezidenta Ukrainy vid 24 veresnia 2015 roku № 555/2015. URL: <https://zakon.rada.gov.ua/laws/show/555/2015> (data zvernennia: 18.11.2019).
2. Narys teorii i praktyky informatsiino-psykholohichnykh operatsii: navch. posib. / Dziuba M.T., ta in.; za red. V.V. Balabina. Kyiv: VITI NTUU "KPI", 2006. 471 s.
3. Viiskovi novyny. veb-sait. URL: <https://www.unian.ua/war> (Data zvernennia 11.11.2019)
4. Kontsepsiia stratehichnykh komunikatsii Ministerstva oborony Ukrainy ta Zbroinykh Syl Ukrainy: zatv nakazom Ministerstva oborony Ukrainy vid 22.11.2017 № 612. URL: <https://zakon.rada.gov.ua/rada/show/v0612322-17>. (Data zvernennia 11.11.2019)
5. Aleshchenko V.I. Fenomenolohiia "hibrydnoi viiny" ta yii osoblyvosti u vykonanni Rosiiskoi Federatsii: informatsiino-psykholohichnyi aspekt. Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Viiskovo-spetsialni nauky. 2016. Vyp. 1. S. 6-11.
6. Shchodo informatsiino-psykholohichnoi skladovoi ahresii Rosiiskoi Federatsii proty Ukrainy (za rezultatamy podii 1-2 bereznia 2014 roku). URL: <http://www.niss.gov.ua/articles/1476/>. (Data zvernennia 11.11.2019)
7. Lipkan V.A. Suchasnyi zmist informatsiinykh operatsii proty Ukrainy. Aktualni problemy mizhnarodnykh vidnosyn. Vypusk 102. Ch. I. 2011, S.34-43
8. Husarov V. Silyi informatsionnykh operatsiy Rossii: kakim dolzhen byt otvet Ukrainyi? URL: <http://sprotyv.info/ru/news/5931-silyi-informatsionnykh-operatsiy-rossii-kakim-dolzhen-byt-otvet-ukrainyi>. (Data zvernennia 11.11.2019)
9. Pietvsov H.V. Analiz struktury, funktsii ta zavdan orhaniv upravlinnia informatsiino-psykholohichnoi borotby v zbroinykh sylakh providnykh krain svitu. Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy. №3(20). 2015. C. 37-46.
10. Safin O.D. Indoktrynatsiia yak instrument hibrydnoi viiny Rosii. Visnyk Kyivskoho natsionalnoho universytetu im. Tarasa Shevchenka. Viiskovo-spetsialni nauky. №2(37). 2017. S. 24-27.

Леонід Михайлович Артюшин (доктор технічних наук, професор)<sup>1</sup>

Олександр Васильович Лагодний (кандидат технічних наук)<sup>2</sup>

<sup>1</sup>Державний науково-дослідний інститут авіації, Київ, Україна

<sup>2</sup>Житомирський військовий інститут імені С. П. Корольова, Житомир, Україна

## ІНДИКАТОРИ ВІЯВЛЕННЯ НЕГАТИВНОГО ПСИХОЛОГІЧНОГО ВПЛИВУ ПІД ЧАС МОНІТОРИНГУ ЕЛЕКТРОННИХ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ

Подання спрямованої інформації у вигляді текстових повідомлень дозволяє здійснювати психологічний вплив на визначені цільові аудиторії з метою формування передбачуваних наслідків, в тому числі і корисних противнику. Проаналізовано існуючі підходи до практики моніторингу мережі Інтернет щодо виявлення негативного психологічного впливу та встановлено їх недоліки. У статті запропоновано індикатори виявлення негативного психологічного впливу на особовий склад Збройних Сил України під час моніторингу електронних засобів масової інформації. Система наведених індикаторів дозволяє кількісно оцінювати рівень негативного психологічного впливу під час проведення противником в інтернет-мережі спеціальних дій. Це дає можливість прогнозувати розвиток подій та своєчасно вживати заходи інформаційної протидії. Кількісні показники негативного психологічного впливу в текстових повідомленнях електронних засобів масової інформації дозволяють об'єктивно оцінювати рівень небезпеки визначеній цільовій аудиторії та мінімізувати рівень суб'єктивізму під час моніторингу інтернет-ресурсів. Індикатори поєднують комплексний підхід до виявлення негативного психологічного впливу за рахунок семантичних та статистичних методів. Результати даної роботи можуть бути реалізовані у вигляді модуля спеціалізованого програмного забезпечення в підсистемі виявлення негативного психологічного впливу особовому складу Збройних Сил України.

**Ключові слова:** мережа Інтернет; психологічний вплив; індикатори.

### Вступ

Характер сучасних воєн показав істотне зростання значущості такої сфери протиборства, як інформаційна. Нова реальність військових конфліктів та війн сучасності полягає в перенесенні військових дій саме в цю сферу [1]. При цьому інформаційні технології стають, по суті, одним із найперспективніших видів зброї, яка з кожним роком удосконалюється і розширює свої можливості, що призвело до більшого масштабу її застосування. Суттєве збільшення загроз інформаційно-технічного й інформаційно-психологічного впливу (ПсВ) зумовило створення спеціальних підрозділів, які використовують системи виявлення та оцінювання рівня загроз для вжиття адекватних заходів інформаційної протидії [2]. Проте для виявлення таких загроз мають бути розроблені відповідні індикатори (показники), що й спричинило виникнення актуального наукового завдання в даній сфері дослідження.

**Постановка проблеми.** П'ятий рік збройного конфлікту на сході України з Російською Федерацією (РФ) показує, що противник продовжує застосовувати гібридні дії в інформаційному просторі, у тому числі мережі Інтернет, які відзначаються низкою інформаційно-психологічних акцій проти особового складу Збройних Сил (ЗС) України. Під час

інформаційно-психологічних акцій противник вживає заходи щодо дискредитації керівництва ЗС України, погіршення морально-психологічного стану особового складу, який виконує завдання в районі проведення Операції об'єднаних сил тощо. В інформаційному просторі нашої держави поширюються інформаційні приводи у вигляді текстових повідомлень в мережі Інтернет, які своїм змістом спонукають особистість до певних дій [3]. Протидія такому негативному ПсВ є важливою складовою у сфері забезпечення національної безпеки, що визначено Доктриною інформаційної безпеки України [4].

Практика виявлення такого негативного ПсВ показала, що під час моніторингу електронних засобів масової інформації (е-ЗМІ) особовий склад стикається з низкою проблем:

1. Завдання щодо моніторингу мережі Інтернет здійснюється в режимі ручного пошуку, що впливає на якість та ефективність виявлення ПсВ.

2. Спеціалізоване програмне забезпечення (СПЗ), яке дозволяє автоматизувати процес моніторингу (наприклад, Semantic Force), є комерційним і високовартісним. Крім того, воно не адаптоване для виконання специфічних завдань і дозволяє тільки збирати масив даних. При цьому одним із розробників СПЗ є компанія з РФ, яка в

умовах збройної агресії може використовувати його у своїх цілях для збору необхідної розвідувальної інформації.

3. Відсутність єдиної системи індикаторів для спеціальних підрозділів, за якими можливо виявляти негативний ПсВ, що ускладнює процес оцінювання рівня небезпеки особовому складу ЗС України та не дає своєчасно вживати заходи інформаційної протидії.

**Аналіз останніх досліджень і публікацій.** Завданням організації моніторингу інформаційного простору з метою виявлення негативних інформаційно-психологічних впливів на цільові аудиторії присвячено низку робіт як закордонних, так і вітчизняних дослідників [5–11]. Так, у [5] запропоновано методологічний підхід до створення підсистеми виявлення та оцінювання негативного інформаційно-психологічного впливу, який базується на тривірневій підсистемі моніторингу інформаційного простору. Автори робіт [6–9] пропонують кількісні показники оцінки негативного інформаційно-психологічного впливу під час організації моніторингу мережі Інтернет з метою протидії такому впливу. У публікаціях [10, 11] визначено впливи, які здійснюються РФ на цільові аудиторії, зокрема й України, та запропоновано індекси стійкості до них. Проведений аналіз показав, що на даний час до кінця не сформований єдиний підхід до виявлення та оцінювання негативного ПсВ за встановленою системою індикаторів (показників).

Тому **метою статті** є розроблення індикаторів виявлення негативного ПсВ на визначену цільову аудиторію, які є найбільш вагомими, на наш погляд, під час моніторингу мережі Інтернет.

### Виклад основного матеріалу дослідження

Аналіз воєнно-політичної обстановки навколо України та суспільно-політичної в самій країні свідчить про те, що держава з дня своєї незалежності стала об'єктом російської пропаганди та напрямком зосередженого й потужного інформаційно-психологічного впливу [3]. В стані гібридних дій РФ проти України протягом останніх п'яти років актуальним залишається питання забезпечення інформаційної безпеки держави. Пріоритетним напрямком досліджень щодо забезпечення національних інтересів у воєнній сфері є захист особового складу ЗС України від негативного ПсВ РФ, що можливо забезпечити за рахунок створення системи і механізмів протидії спеціальним інформаційним (психологічним) операціям агресора [4].

Спеціальні підрозділи РФ широко використовують мережу Інтернет для поширення негативного інформаційно-психологічного впливу на військово-політичне керівництво держави, особовий склад ЗС України та населення [12]. З метою протидії такому негативному впливу виникає потреба у створенні нових і модернізації

існуючих систем виявлення та оцінювання рівня негативного ПсВ на цільові аудиторії.

На сьогодні такі системи переважно базуються на семантичних методах із використанням якісних показників впливу. Оперативне виявлення такого впливу і прогнозування ситуації можуть реалізовуватися за рахунок введення кількісних індикаторів негативного ПсВ та розроблення методики динаміки відслідковування його поширення в мережі Інтернет. Виникає потреба в удосконаленні існуючих систем оперативного виявлення загроз національній безпеці на основі введення необхідних індикаторів негативного ПсВ у процесі моніторингу відкритої інформації глобальної мережі. Впровадження підходу на їх основі дасть змогу розробити відповідне СПЗ, що дозволить автоматизувати даний процес. До індикаторів, які вважатимуться критеріями для виявлення негативного ПсВ на особовий склад ЗС України, належать:

частота публікацій текстового повідомлення з негативним ПсВ за обраною тематикою  $C_i$ ;

динаміка появи текстового повідомлення з негативним ПсВ за обраною тематикою  $D_i$ ;

показник важливості е-ЗМІ (PageRang) у пошуковій системі Google  $PR_i(A)$ ;

показник поширеності текстового повідомлення з негативним ПсВ за обраною тематикою  $M_i$ ;

показник тональності текстового повідомлення  $L_{п,н,нт}$ .

Частота публікацій текстового повідомлення з негативним ПсВ за обраною тематикою  $C_i$  – це співвідношення кількості публікацій текстових повідомлень за досліджуваною тематикою  $y_i$  до загальної кількості публікацій  $N_{пуб.}$  за усіма тематиками за визначений проміжок часу  $t_i$  спостереження в е-ЗМІ:

$$C_i = \frac{\sum_{i=1}^k y_i}{N_{пуб.} \cdot \sum_{i=1}^k t_i} \cdot 100\%, \quad (1)$$

де  $k$  – дискрети, у які отримані текстові повідомлення.

Динаміка появи текстового повідомлення з негативним ПсВ за обраною тематикою  $D_i$  – це розподілення публікацій текстових повідомлень  $y_i$  на часовій шкалі  $\Delta t$ :

$$D_i = \frac{\sum_{i=1}^k y_i}{\Delta t}, \quad (2)$$

де  $\Delta t$  – період (доба, тиждень, місяць...).

Показник важливості е-ЗМІ (PageRang) у пошуковій системі Google  $PR_i(A)$  – це числова величина, яка визначає авторитетність інтернет-

ресурсу з урахуванням якісної характеристики посилань на них з інших сайтів [13]:

$$PR_i(A) = (1-d) + d \left( \frac{PR(T_1)/C(T_1) + \dots}{+PR(T_j)/C(T_j)} \right), \quad (3)$$

де  $PR_i(A)$  – це вага PageRang сторінки сайта  $A$ , яку необхідно обрахувати;

$d$  – сталий коефіцієнт затухання, який дорівнює 0,85;

$PR(T_1)$  – це вага PageRang сторінки, яка вказує на сторінку сайта  $A$ ;

$C(T_1)$  – кількість посилань із цієї сторінки сайта;

$PR(T_j)/C(T_j)$  – обрахунок для кожної сторінки сайтів, які вказують на сторінку сайта  $A$ .

Показник поширеності текстового повідомлення з негативним ПсВ за обраною тематикою  $M_i$  – це відношення е-ЗМІ  $q$ , у яких виявлено текстові повідомлення з негативним ПсВ, до загальної кількості сайтів, які перебувають на моніторингу,  $Q$ :

$$M_i = \frac{q}{Q}. \quad (4)$$

Для визначення категорій рівня небезпеки поширеності текстових повідомлень із негативним ПсВ за обраною тематикою наведено трирівневу шкалу оцінювання, яку часто використовують у багатьох сферах сектора національної безпеки і оборони держави [14]. При цьому виділяють такі рівні небезпеки: високий, середній, низький (табл. 1).

Таблиця 1

Якісна шкала небезпеки рівнів поширеності текстових повідомлень із негативним ПсВ

Інтегральна оцінка, $M_i$	Категорія рівня небезпеки	Якісна характеристика
$0,71 \leq M_i \leq 1,0$	Високий	Проведення противником психологічної акції
$0,51 \leq M_i \leq 0,7$	Середній	Поширення противником текстових повідомлень із негативним ПсВ
$0,0 < M_i \leq 0,5$	Низький	Розміщення противником текстових повідомлень із негативним ПсВ

На відміну від нормованої фундаментальної шкали, яка передбачає п'ять категорій оцінки, застосування трирівневої шкали забезпечує подання базових усталених рівнів небезпеки та уникання надлишкової деталізації.

Показник тональності текстового повідомлення  $L_{п,н,нт}$  – це відношення кількості публікацій за тональністю ( $I_{п,н,нт}$ ) до загальної кількості публікацій  $N_{пуб.}$ :

$$L_{п} = \frac{I_{п}}{N_{пуб.}} \cdot 100\%, \quad L_{н} = \frac{I_{н}}{N_{пуб.}} \cdot 100\%, \quad (5)$$

$$L_{нт} = \frac{I_{нт}}{N_{пуб.}} \cdot 100\%.$$

Окрім базових показників, які характеризують негативний ПсВ та використовуються для обчислення узагальненого показника рівня негативного ПсВ, доцільним є оцінювання статистичних характеристик процесу розповсюдження ПсВ за кожним із напрямів реалізації впливу. Дане оцінювання дозволяє отримати обґрунтоване рішення щодо випадкового або не випадкового характеру виникнення текстових повідомлень із негативним ПсВ та їх розповсюдження.

Одним із підходів є застосування статистики, яка ґрунтується на показнику Херста ( $H$ ) [15, 16].

Використання даного показника знайшло поширення під час аналізу часових рядів. Для калібрування часових вимірювань Херст ввів безрозмірний коефіцієнт шляхом ділення розмаху на стандартне відхилення спостережень. Цей метод називається методом нормованого розмаху ( $R/S$  – аналіз).

*Розрахунок показника Херста*

Популярність показника Херста викликана його високою стійкістю, можливістю класифікації досліджуваних часових вибірок і визначення їх випадкового чи не випадкового характеру. Його розрахунок ґрунтується на персистентності (схильності часових рядів до трендів). Кожне спостереження містить пам'ять про всі попередні події. Це не короточасна пам'ять, яку часто називають "марківською", а інша – довготривала, теоретично вона зберігається назавжди. Нещодавні події мають більший вплив, ніж давно минулі, але їхній залишковий вплив завжди відчутний. Те, що відбувається сьогодні, впливає на майбутнє, і стан системи, у якому вона перебуває, визначається тим, якою вона була в минулому. Час виявляється важливим чинником. Показник Херста має таке значення:

1)  $0 \leq H < 0,5$  – антиперсистентний або ергодичний часовий ряд, постійно змінюється тенденція зростання і спадання. Чим ближче це значення до нуля, тим ряд більш нестійкий, спостерігається броунівський рух і невизначеність. Такий тип поведінки називають "поверненням до середнього". Якщо для системи відбувається зростання певного показника в попередній період, то, швидше за все, в подальшому почнеться спад. І, навпаки, якщо йшло зниження, то ймовірний близький підйом;

2)  $H = 0,5$  – часовий ряд абсолютно випадковий. Події випадкові і некорельовані, відсутня довготривала статистична залежність. Сьогодення не впливає на майбутнє. Функція щільності ймовірності може бути нормальною, проте це не обов'язкова умова.  $R/S$  – аналіз може ідентифікувати довільний ряд незалежно від типу функції розподілу, яка йому відповідає;

3)  $0,5 < H \leq 1,0$  – персистентний часовий ряд (“чорний шум”), спостерігається тренд, збереження тенденції до зростання чи спадання показника як у минулому, так і в майбутньому. Трендостійкість поведінки, або сила персистентності, збільшується в разі наближення  $H$  до 1 або 100% кореляції. Чим ближче  $H$  до 0,5, тим більше ряд зашумлений і тим менше виражений його тренд.

Показник Херста пов'язаний з такими коефіцієнтами, як  $R$  та  $S$ :  $R$  – різниця максимального і мінімального накопиченого відхилення від вимірюваного значення – “розмах”;  $S$  – стандартне відхилення від вимірювального значення [16, 17]. Показник Херста можна розрахувати за такою послідовністю: спочатку обчислюють середнє значення появи текстового повідомлення за  $n$  періодів (кількість разів, годин, днів, місяців тощо), протягом яких проводилося вимірювання:

$$y_{cp} = \frac{1}{n} \sum_{t=1}^n y_i(t). \quad (6)$$

Потім розраховують накопичене відхилення членів ряду від середнього його значення за  $n$  періодів:

$$X_u = \sum_{i=1}^u (y_i(t) - y_{cp}), \quad (7)$$

де  $u$  – конкретний елемент ряду.

Після цього визначають різницю максимального і мінімального накопиченого відхилення, яка і називається “розмахом”:

$$R = \max_{1 \leq u \leq n} (X_u) - \min_{1 \leq u \leq n} (X_u). \quad (8)$$

Стандартне відхилення числового ряду одиниці аналізу розраховують за таким виразом:

### Література

**1. Почепцов Г.** Сучасні інформаційні війни : монографія. Київ : Дім “Киево-Могилянська академія”, 2015. 497 с. **2. Аргюшин Л. М., Чернишук С. В.** Шляхи підвищення ефективності системи виявлення та оцінювання інформаційних загроз // Сучасні інформаційні технології у сфері безпеки та оборони. Київ : НУОУ, 2018. № 3. С. 99–106. **3. Горбулін В. П.** Світова гібридна війна: український фронт : монографія / За заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с. **4.** Про Доктрину інформаційної безпеки України : Указ Президента України від 25 лютого 2017 р. № 47/2017. URL: <http://www.president.gov.ua/documents/472017-21374> (дата звернення: 03.05.2019). **5.** Підсистема моніторингу інформаційного простору як необхідна складова протидії негативному інформаційно-психологічному впливу на особовий склад Збройних

$$S = \sqrt{\frac{1}{n} \sum_{i=1}^n (y_i(t) - y_{cp})^2}. \quad (9)$$

Сил України / Сніцаренко П. М., Саричев Ю. О., Ткаченко В. А., Мотузьяник О. А. // Наука і оборона. Київ : НУОУ, 2018. № 1. С. 29–33. **6. Левченко О. В., Косогов О. М., Сірик А. О.** Методика оцінювання кількісних показників негативного інформаційного впливу // Сучасні інформаційні технології у сфері безпеки та оборони. Київ : НУОУ, 2017. № 1. С. 31–35. **7. Гришук Р. В., Манько О. В., Оришук І. О.** Особливості організації та ведення моніторингу електронних засобів масової комунікації // Інформаційна безпека. Луганськ : СНУ ім. В. Даля, 2014. № 3. С. 10–14. **8. Дзюба Т. М., Волошина Н. М., Пампуха І. В.** Механізм інформаційно-психологічного впливу на психіку людини у гібридній війні // Зб. наук. праць Військ. ін-ту Київськ. нац. ун-ту ім. Тараса Шевченка. Київ : ВІКНУ, 2016. Вип. 51. С. 91–99. **9.** Інформаційно-

$$H = \frac{\ln \frac{R}{S}}{\ln \frac{n}{2}}. \quad (10)$$

Для проведення аналізу пропонується обирати тільки часові ряди текстових повідомлень, які характеризуються ознаками персистентності, а показник Херста знаходиться в межах  $0,5 < H \leq 1,0$ .

Важливим є також оцінювання трендостійкості зміни ПсВ за період аналізованого часу та проведення статистичного аналізу активності тематичного контенту в мережі Інтернет [18].

### Висновки і перспективи подальших досліджень

Таким чином, запропоновано індикатори виявлення негативного ПсВ у текстових повідомленнях під час моніторингу е-ЗМІ: частота публікацій текстового повідомлення з негативним ПсВ за обраною тематикою; динаміка появи текстового повідомлення з негативним ПсВ за обраною тематикою; показник важливості е-ЗМІ (PageRang) у пошуковій системі Google; показник поширеності текстового повідомлення з негативним ПсВ за обраною тематикою; показник тональності текстового повідомлення; показник Херста (ознака персистентності). Урахування запропонованих індикаторів дозволяє більш об'єктивно та всебічно оцінювати рівень ПсВ на обрану цільову аудиторію, що мінімізує його залежність від суб'єктивного фактора.

Перспективами подальшого дослідження є впровадження зазначених індикаторів виявлення негативного ПсВ у модуль СПЗ для підвищення ефективності застосування спеціальних підрозділів ЗС України в процесі проведення заходів інформаційного протиборства в мережі Інтернет.

Сил України / Сніцаренко П. М., Саричев Ю. О., Ткаченко В. А., Мотузьяник О. А. // Наука і оборона. Київ : НУОУ, 2018. № 1. С. 29–33. **6. Левченко О. В., Косогов О. М., Сірик А. О.** Методика оцінювання кількісних показників негативного інформаційного впливу // Сучасні інформаційні технології у сфері безпеки та оборони. Київ : НУОУ, 2017. № 1. С. 31–35. **7. Гришук Р. В., Манько О. В., Оришук І. О.** Особливості організації та ведення моніторингу електронних засобів масової комунікації // Інформаційна безпека. Луганськ : СНУ ім. В. Даля, 2014. № 3. С. 10–14. **8. Дзюба Т. М., Волошина Н. М., Пампуха І. В.** Механізм інформаційно-психологічного впливу на психіку людини у гібридній війні // Зб. наук. праць Військ. ін-ту Київськ. нац. ун-ту ім. Тараса Шевченка. Київ : ВІКНУ, 2016. Вип. 51. С. 91–99. **9.** Інформаційно-



психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії / Певцов Г. В., Залкін С. В., Сідченко С. О., Хударковський К. І. // Наука і оборона. Київ : НУОУ, 2015. № 2. С. 28–32. **10.** Cyber and Information warfare in the Ukrainian conflict / Center for Security Studies (CSS), ETH Zurich. 2017. URL: <http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf> (дата звернення: 21.05.2019). **11.** Disinformation Resilience in Central and Eastern Europe. URL: [http://prismua.org/wp-content/uploads/2018/06/DRI\\_CEE\\_2018.pdf](http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf) (дата звернення: 21.05.2019). **12. Левченко О. В.** Класифікація інформаційної зброї за засобами ведення інформаційної боротьби // Сучасні інформаційні технології у сфері безпеки та оборони. Київ : НУОУ, 2014. № 2 (20). С. 142–146. **13. Плеханова А. О.** Методи вибору і оцінки ефективності інформаційних систем // Информационные технологии в управлении,

образовании, науке и промышленности : монография / Под ред. В. С. Пономаренко. Харьков : Издатель Рожко С. Г., 2016. С. 491–505. **14. Горбулін В. П., Качинський А. Б.** Стратегічне планування: вирішення проблем національної безпеки : монографія. Київ : НІСД, 2010. 288 с. **15. Федер Е.** Фракталы. Москва : Мир, 1991. 254 с. **16. Hurst Н. Е.** Long Term Storage Capacity of Reservoirs // Transactions of the American Society of Civil Engineers, 1951. № 116. P. 770–799. **17. Дербенцев В. Д., Сердюк О. А., Соловійов В. М., Шарапов О. Д.** Синергетичні та еконофізичні методи дослідження динамічних та структурних характеристик економічних систем : монографія. Черкаси : Брама-Україна, 2010. 287 с. **18. Лагодний О. В., Писарчук О. О., Міхеев Ю. І.** Статистичний аналіз активності тематичного контенту в мережі Інтернет для прогнозування розвитку інформаційних загроз // Траектория науки. Словаччина. 2017. Т. 3, № 8. С. 3011–3019.

## ИНДИКАТОРЫ ВЫЯВЛЕНИЯ НЕГАТИВНОГО ПСИХОЛОГИЧЕСКОГО ВЛИЯНИЯ ВО ВРЕМЯ МОНИТОРИНГА ЭЛЕКТРОННЫХ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ

*Леонид Михайлович Артюшин (доктор технических наук, профессор)<sup>1</sup>  
Александр Васильевич Лагодный (кандидат технических наук)<sup>2</sup>*

<sup>1</sup>Государственный научно-исследовательский институт авиации, Киев, Украина  
<sup>2</sup>Житомирский военный институт имени С. П. Королева, Житомир, Украина

*Представление направленной информации в виде текстовых сообщений позволяет осуществлять психологическое влияние на определенные целевые аудитории с целью формирования предполагаемых последствий, в том числе и полезных противнику. Проанализированы существующие подходы к практике мониторинга сети Интернет по выявлению негативного психологического влияния и установлено их недостатки. В статье предложены индикаторы выявления негативного психологического влияния на личный состав Вооруженных Сил Украины во время мониторинга электронных средств массовой информации. Система приведенных индикаторов позволяет количественно оценивать уровень негативного психологического влияния при проведении противником в интернет-сети специальных действий. Это дает возможность прогнозировать развитие событий и своевременно принимать меры информационного противодействия. Количественные показатели негативного психологического влияния в текстовых сообщениях электронных средств массовой информации позволяют объективно оценивать уровень опасности определенной целевой аудитории и минимизировать уровень субъективизма при мониторинге интернет-ресурсов. Индикаторы объединяют комплексный подход к выявлению негативного психологического влияния за счет семантических и статистических методов. Результаты данной работы могут быть реализованы в виде модуля специализированного программного обеспечения в подсистеме обнаружения негативного психологического влияния личному составу Вооруженных Сил Украины.*

*Ключевые слова:* сеть Интернет; психологическое влияние; индикаторы.

## DETERMINATION INDICATORS OF NEGATIVE PSYCHOLOGICAL INFLUENCE UNDER MONITORING OF ELECTRONIC MASS MEDIA

*Leonid Artushin (Doctor of Technical Sciences, Professor)<sup>1</sup>  
Oleksandr Lahodnyi (Candidate of Technical Sciences)<sup>2</sup>*

<sup>1</sup>State Research Aviation Institute, Kyiv, Ukraine  
<sup>2</sup>Koroljov Zhytomyr Military Institute, Zhytomyr, Ukraine

*The submission of directed information in the form of text messages allows to carry out psychological influence on certain target audiences in order to form the foreseeable consequences, including useful to the opponent. The existing approaches to monitoring the Internet for the detection of negative psychological influence, as well as their disadvantages are analyzed. Indicators of detection of negative psychological influence on the personnel of the Armed Forces of Ukraine during monitoring of electronic mass media were suggested. The system of the given indicators allows to quantify the level of negative psychological influence during the conduct of the enemy's special actions on the Internet. It allows to predict the development of events*

and to timely take measures of information counteraction. Quantitative indicators of negative psychological impact in text messages of electronic mass media allow to objectively assess the level of danger to a specific target audience and to minimize the level of subjectivity during monitoring of Internet resources. Indicators combine a comprehensive approach to detecting negative psychological effects through semantic and statistical methods. The results of this work can be implemented as a module of specialized software in the subsystem of detecting negative psychological impact on the personnel of the Armed Forces of Ukraine.

**Keywords:** Internet; psychological influence; indicators.

## References

- Pochepcov Gh.** (2015), Modern information wars: a monograph. [Suchasni informacijni vijny: monoghracija], Kyiv, dim "Kyjevo-Moghyljansjka akademija", 497 p.
- Artyushin L. M., Chernyshuk S. V.** (2018), Approaches of improvement of effectiveness of information threats detection and estimation system. [Shljakhy pidvyshhennja efektyvnosti systemy vyjavlennja ta ocinjuvannja informacijnykh zaghroz], Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony, No. 3, pp. 99–106.
- Ghorbulin V. P.** (2017), World hybrid war: Ukrainian front: monograph. [Svitova ghibrydna vijna: ukrajinsjkyj front: monoghracija za zagh. red. V. P. Ghorbulina], NISS, Kyiv, 496 p.
- On the Doctrine of Information Security of Ukraine: Decree of the President of Ukraine dated February 25, 2017 No. 47.** [Pro Doktrynu informacijnoji bezpeky Ukrajiny: Ukaz Prezydenta Ukrajiny vid 25 ljutogho 2017 roku No 47/2017], available at: <http://www.president.gov.ua/documents/472017-21374> (posting date 03.05.2019).
- Snicarenko P. M., Sarychev Ju. O., Tkachenko V. A., Motuzjanyk O. A.** (2018), Subsystem of monitoring of the information space as an essential component of countering the negative informational and psychological impact on the personnel of the Armed Forces of Ukraine. [Pidsystema monitorynghu informacijnogho prostoru jak neobkhdna skladova protydiji neghatyvnomu informacijno-psykhologhichnomu vplyvu na osobovyj sklad Zbrojnykh Syl Ukrajiny], Nauka i oborona, No. 1, pp. 29–33.
- Levchenko O. V., Kosoghov O. M., Siryk A. O.** (2017), Method of estimation of quantitative indicators of negative informational influence. [Metodyka ocinjuvannja kiljisknykh pokaznykiv neghatyvnogho informacijnogho vplyvu], Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony, No. 1, pp. 31–35.
- Ghryshhuk R. V., Manjko O. V., Oryshhuk I. O.** (2014), Features of organization and monitoring of electronic media of mass communication. [Osoblyvosti orghanizaciji ta vedennja monitorynghu elektronnykh zasobiv masovoji komunikaciji], Informacijna bezpeka, No. 3, pp. 10–14.
- Dzjuba T. M., Voloshyna N. M., Pampukha I. V.** (2016), Mechanism of informational and psychological influence on human psyche in hybrid warfare. [Mekhanizm informacijno-psykhologhichnogho vplyvu na psykhiku ljudyny u ghibrydnij vijni], zb. nauk. pracj. Vijsjkovogho instytutu Kyjivsjkogho nacionaljnogho universytetu imeni Tarasa Shevchenka, No. 51, pp. 91–99.
- Pjevcev Gh. V., Zalkin S. V., Sidchenko S. O., Khudarkovsjkyj K. I.** (2015), Information-psychological operations of the Russian Federation in Ukraine: models of influence and directions of counteraction. [Informacijno-psykhologhichni operaciji Rosijsjkoji Federaciji v Ukrajini: modeli vplyvu ta naprjamy protydiji], Nauka i oborona, No. 2, pp. 28–32.
- Cyber and Information Warfare in the Ukrainian Conflict** (2017), [Kiber ta informacijna vijna v ukrajinsjkomu konflikti], Centr doslidzhenj bezpeky (CSB), available at: <http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf> (posting date 21.05.2019).
- Disinformation Resilience in Central and Eastern Europe.** [Dezinformacijna stijkistj u Centralnijij ta Skhidnij Jevropi], available at: [http://prismua.org/wp-content/uploads/2018/06/DRI\\_CEE\\_2018.pdf](http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf) (posting date 21.05.2019).
- Levchenko O. V.** (2014), Classification of information weapons by means of conducting an information struggle. [Klasyfikacija informacijnoji zbroji za zasobamy vedennja informacijnoji borotjby], Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony, No. 2, pp. 142–146.
- Plehanova A. O.** (2016), Methods of selection and evaluation of the effectiveness of information systems//Information technologies in management, education, science and industry: monograph/ed. V. S. Ponomarenko. [Metody viybora i otsenki effektivnosti informatsionnyh sistem//Informatsionnye tehnologii v upravlenii, obrazovanii, nauke i promyshlennosti: monografiya/pod red. V. S. Ponomarenko], Kharkov, Izdatel Rozhko S. G., pp. 491–505.
- Ghorbulin V. P., Kachynsjkyj A. B.** (2010), Strategic planning: solving problems of national security: monograph. [Strateghichne planuvannja: vyrishennja problem nacionaljnoji bezpeky: monoghracija], Kyiv, NISD, 288 p.
- Feder E.** (1991), Fractals. [Fraktalyi], Moscow, Mir, 254 p.
- Kherst Kh. E.** (1951), Long Term Storage Capacity of Reservoirs. [Dovghotryvala potuzhnistj vodoskhovyssh], Operaciji Amerykansjkogho tovarystva cyviljnykh inzheneriv, pp. 770–799.
- Derbencev V. D., Serdjuk O. A., Solovjov V. M., Sharapov O. D.** (2010), Synergetic and econophysical methods of study of dynamic and structural characteristics of economic systems: monograph. [Synerghetychni ta ekonofizychni metody doslidzhennja dynamichnykh ta strukturyjnykh kharakterystyk ekonomichnykh system: monoghracija], Cherkasy, Brama-Ukrajina, 287 p.
- Lahodnyi O. V., Pysarchuk O. O., Mikhhejev Ju. I.** (2017), Statistical Analysis of the Activity of the Thematic Content on the Internet for Predicting the Development of Information Threats. [Statystychnyj analiz aktyvnosti tematychnogho kontentu v merezhi Internet dlja prohnozuvannja rozvytku informacijnykh zaghroz], Traektorija nauky, Volume 3, No. 8, pp. 3011–3019.

*Олександр Володимирович Войтко (кандидат військових наук)*

*Віталій Олександрович Кацалап (кандидат військових наук)*

*Володимир Миколайович Чернега (кандидат технічних наук)*

*Національний університет оборони України імені Івана Черняховського, Київ, Україна*

## ОСОБЛИВОСТІ СПРИЙНЯТТЯ ТА РЕАГУВАННЯ НА ОТРИМАНУ ІНФОРМАЦІЮ

*Аналіз подій з початку загострення відносин між Україною та Російською Федерацією свідчить про те, що практичні заходи протидії інформаційно-психологічним впливам з боку противника були малоефективними.*

*Розвиток та інформатизація суспільства вимагає від збройних сил нових підходів до ведення збройної боротьби, центр якої інтенсивно зміщується з поля бою в інформаційний простір, де відбувається головна битва за людину, через її внутрішній емоційний стан.*

*Емоційний стан відіграє величезну роль в процесі підготовки та проведення маніпуляції свідомістю людини або масовою свідомістю при здійсненні впливу на, мотивацію, раціональне мислення з метою зміни моделей поведінки визначених цільових аудиторій, що в свою чергу посилює негативний психологічний вплив. При виробленні матеріалів для організованого цілеспрямованого втручання у свідомість, необхідно враховувати як та чи інша особистість (цільова аудиторія) буде сприймати надану їй інформацію.*

*Метою даної статті є аналіз особливостей сприйняття та реагування суспільства (певних цільових аудиторій) на інформацію, що циркулює в їхньому інформаційному просторі. Визначається, класифікація цільових аудиторій по способам сприйняття та реагування на отриману інформацію.*

***Ключові слова:** цільова аудиторія, інформаційно-психологічний вплив, сприйняття інформації, реагування на інформацію, психологічний портрет.*

### Вступ

“В XXI веке прослеживается тенденция стирания различий между состоянием войны и мира. Войны уже не объявляются, а начавшись – идут не по привычному нам шаблону”. Такою тезою розпочав свій виступ начальник ГШ ЗС РФ Валерій Герасимов на зібранні військової академії наук РФ.

Досвід військових конфліктів, які розв’язала Росія, підтверджує, що цілком мирна держава за лічені місяці і навіть дні може перетворитися в арену запеклої збройної боротьби, стати жертвою, зануритися в пучину хаосу, гуманітарної катастрофи і війни.

Особливої актуальності в сучасних конфліктах набуває інформаційно-психологічний вплив на населення та захоплення об’єктів і комунікацій силами спеціальних операцій противника.

Для здійснення таких впливів на думку суспільства в значній мірі використовуються соціальні медіа.

**Постановка проблеми.** Приклад успішного використання соціальних медіа став Гонконг. Більше 80% жителів цього міста вважають себе активними користувачами соціальних мереж. Саме такі мережі стали одним із головних інструментів в руках опозиції під час протестів 2019 року.

Соціальні мережі допомагали контролювати емоційну хвилю протестуючих та зробити цей протест організованим і багатомісячним.

З початком агресії РФ проти України її окупаційні війська в широкій мірі використовували інформаційні та психологічні впливи на населення України, військово-політичне керівництво, лідерів та особовий склад Збройних Сил України. З 2014 року для протистояння цим впливам та захисту свого суспільства наша держава стала на шлях виправдання та проведення інформування, однак цих

дій не достатньо. Розвиток та інформатизація суспільства вимагає від Збройних Сил нових підходів до ведення збройної боротьби, центр якої інтенсивно зміщується з поля бою в інформаційний простір, де відбувається головна битва за людину її внутрішній емоційний стан. Тому підходи до сприйняття і реагування на інформацію, що отримує суспільство, є актуальними як для збройних сил, так і для держави в цілому.

**Аналіз останніх досліджень і публікацій.** В останні роки з’явилось дуже багато матеріалів, які проводять оцінку подій, що відбувалися. Однак праць, які висвітлюють планування інформаційно-психологічних впливів, на превеликий жаль немає. Також відсутні матеріали, що дають можливість прогнозувати сценарій розвитку тих чи інших подій.

Так, вагомий внесок в дослідженні впливу інформації на психологію людини та суспільства зробили ряд провідних вітчизняних та зарубіжних вчених, таких як Бандурка О.М., Асмолов О.Г. [1, 2], та багато інших. Однак їх праці мають лише теоретичний характер досліджень та більш притаманні для медицини.

Праці Зелінського С.О. [3], присвячені інформаційно-психологічним впливам на масову свідомість, та можуть виступити суттєвим науковим підґрунтям для проведення дослідження.

В попередніх працях [4,5,6] авторами було розглянуто та запропоновано завдання із захисту від негативного інформаційно-психологічного впливу та проведено аналіз особливостей маніпуляції, як інструменту психологічного впливу на свідомість.

**Метою статті** є розглянути особливості сприйняття та реагування суспільства (певними цільовими аудиторіями) на інформацію, що циркулює в їхньому інформаційному просторі.

## Виклад основного матеріалу дослідження

В сучасних умовах, значна частка бойових дій вже перенесена безпосередньо в мережу Інтернет. Дуже часто таке мережеве відображення впливає на результат протидії конкуруючих сторін. Активне залучення до віртуальної мережі багатомільйонної аудиторії дозволяє маніпулювати громадською думкою і суттєво впливати на процеси протидії сторін. Активне використання соціальних мереж дозволяє оперативно впливати на думку і поведінку людей, що перетворює їх на “холодну зброю” в умілих руках. Для якісного та ефективного використання таких груп (цільових аудиторій) необхідно визначити, як вони сприймають інформацію. За сприйняттям інформації, осіб що входять до цих цільових аудиторій, можна розподілити на три основні сфери сенсорного сприйняття інформації: візуальної, аудіальної і кінестетичної.

Особам візуального типу сприйняття інформації інформація може надаватися їм у вигляді ярих фарб, зорових образів; розповідаючи щось, ці люди часто жестикують, як би малюючи в повітрі що подаються образи. У момент спогадів зазвичай дивляться прямо перед собою, вгору, вліво вгору або вправо вгору.

Аудіальний тип людей, вживає в основному аудіальні слова та те, що вони згадують, як би підказані їм внутрішнім голосом слова, або ті що вони чули від інших. При згадці погляд розвернутий вправо, вліво або вправо вниз.

Люди кінестетичного типу добре запам'ятовують відчуття, рухи. Згадуючи, ці люди намагаються відтворити, повторюючи рухи і відчуття тіла. Згадуючи, вони дивляться вниз або вправо вниз.

Тобто за способом сприйняття інформації людей можна розподілити на дві групи, такі як психологічного сприйняття та нейрофізіологічного сприйняття.

Всі особи в різній мірі схильні до психологічного впливу (сприйняття), в різній мірі володіють здатністю відізнати правду від вигадки і брехні, вловлювати обман, нещирість і приховані задуми. Одні - більш проникливі, інші - менш. Ця обставина знайшла підтвердження і при розробці психодіагностичних методик, зокрема, особистісних тестів. Так, наприклад, було виявлено двополосний чинник в концепції особистості “Кетелла”, що відображає ступінь розвитку і вираженості у людини здібності розпізнавання, розуміння та використання методів і прийомів прихованого психологічного впливу на людей. Він відомий під назвою фактора “Макиавеллі-Руссо” або як фактор “проникливість – наївність”. Цей фактор досить добре вивчений і інтерпретується як штучність, розважливості поведінки до опозиції природності і простоти.

Особи з високими оцінками даного фактору “Кетелла” характеризуються штучністю, ошадливістю, проникливістю, умінням холодно і раціонально діяти, не піддаватися емоційним поривам, здатністю бачити за ефектом логіку. Вони до всього підходять розумно і несентиментально, перш ніж зробити що-небудь, з холодною аналітичністю оцінюють можливі шанси, вміло будують свою поведінку, скептично ставляться до гасел і призовів, схильні до інтриг, хитрості і витонченій підступності.

Відповідно, низькі показники по даному фактору, свідчать про відсутність проникливості і соціальної

спритності, про прямотинійність, невміння ясно мислити. Такі люди зазвичай відкриті, товариські, компанійські. Вони люблять прості, буденні речі і чуттєві радості, погано розуміють мотиви поведінки оточуючих, все приймають на віру, легко спалахують загальними захопленнями, сентиментальні, чутливі, не можуть приборкати емоції логікою, не вміють хитрувати і обманювати, поводяться природно, просто і навіть грубувато.

Безсумнівно, яскрава вираженість психологічних особливостей людини, відповідних максимальним значенням протилежних полюсів даного чинника, зустрічаються не дуже часто. Для більшості людей властиво поєднання в певних пропорціях характеристик даного чинника з більшою або меншою тенденцією відповідності одному з його полюсів. Ступінь вираженості і близькості його до полюсів “Макиавеллі-Руссо” у людей різна – у одних менше, у інших – більше. Хтось більшою мірою може вловити і виявити використовувані маніпулятивні прийоми, хтось в значно меншій.

Вважається, що проникливість не дається у спадок чи при народженні, а в більшій мірі формується, що виробляється з роками в процесі практичної діяльності, пов'язаної з інтенсивним спілкуванням і взаємодією з людьми, а також при навчанні і проведенні спеціальних тренінгових процедур.

Здатність сприймати та реагувати на інформацію, що надходить залежить від особистісних особливостей людини. В нашому випадку вона представлена концепцією нейрофізіологічних рис і типів особистості Айзенка. У своєму ранньому дослідженні Айзенк виявив два основних типи, які він назвав інтроверсія-екстраверсія і нейротизм-стабільність (іноді цей фактор називають нестабільність-стабільність). Ці два виміри особистості ортогональні, тобто, вони статистично залежать один від одного. Відповідно, людей можна розділити на чотири групи, кожна з яких представляє собою якусь комбінацію високої або низької оцінки в діапазоні одного типу разом з високою або низькою оцінкою в діапазоні іншого типу.

Умовно він розділив людей на чотири групи. У своїй теорії він спробував встановити нейрофізіологічну основу для кожної з рис або з типів особистості. Та використав термін «активація» для позначення ступеня збудження, який змінює свою величину від нижнього екстремуму (наприклад, сон) до верхнього екстремуму (наприклад, стан паніки). Він вважає, що інтроверти надзвичайно збудливі і, отже, надзвичайно чутливі до інформації що надходить, з цієї причини вони уникають ситуацій, які надмірно чи сильно подіють (по впливають) на них. І навпаки, екстраверти недостатньо збудливі і тому менш чутливі до інформації що надходить; відповідно, вони постійно вишукують ситуації, які можуть їх зворушити.

Також він припускає, що індивідуальні відмінності по стабільності-нейротизму відображають силу реакції автономної нервової системи на інформацію (стимули). Особливо він пов'язує цей аспект з лімбічною нервовою системою, яка впливає на мотивацію і емоційну поведінку. Люди з високим рівнем нейротизму зазвичай реагують на повідомлення болочого, незвичного, та подібного тренду інформацію швидше, ніж більш стабільні особистості. У таких осіб виявляються більш тривалі реакції, що тривають навіть після надходження неприємної для них інформації

(стимулів), ніж у осіб з високим рівнем стабільності.

Теорію Айзенка підкріплює когнітивний підхід до особистості Келлі, згідно з яким, можна припустити, що інтроверти з високим рівнем нейротизму більш схильні до негативних емоційних станів: тривоги, вини, загрози і ворожості, так як більш чутливі до зовнішнього впливу.

Келлі визначив тривогу, як “усвідомлення того, що події, з якими стикається людина, лежать поза діапазоном застосовності його конструктивної системи”. Тобто неясне почуття невизначеності і безпорадності визначається як “тривога”. Келлі підкреслював: зовсім не факт, що наша конструктивна система не функціонує ідеально, провокує тривогу; ми не турбуємося просто тому, що наші очікування не точні. Тривога утворюється тільки тоді, коли ми визнаємо, що у нас немає адекватних конструктивів, за допомогою яких ми можемо інтерпретувати події нашого життя.

Засновник психодинамічної теорії особистості З. Фрейд виділив природу тривоги, виходячи зі своєї концепції, в дещо іншому контексті – в її психічному походженні, а не фізіологічному. І ця зацікавленість вперше привела його (у 1890 році) до припущення про те, що тривога, була наслідком неадекватної розрядки енергії лібідо. Надалі він зробив висновок, що стан наростаючої напруги є результатом виходу енергії лібідо. Тривога, незавершена розрядка, перетворюється і проявляється в неврозах і страхах.

Однак у міру накопичення досвіду Фрейд прийшов до розуміння, що подібна інтерпретація тривоги і страху є невірною. Через 30 років він переглянув свою теорію і прийшов до наступного висновку: тривога є функцією страху, і призначення її полягає в тому, щоб попереджати людину про небезпеку, що насувається, яку треба зустріти або уникнути. Тривога як така дає можливість особистості реагувати в загрозових ситуаціях адаптивним способом.

Ще один емоційний стан, частіше притаманний людям з високим рівнем інтроверсії, – загроза, що розглядається Келлі як усвідомлення того, що наша конструктивна система може бути суттєво змінена внаслідок якихось подій. Почуття загрози з’являється, коли неминуче велике протистояння наших особистісних конструктивів. Келлі вважав, що загроза для людини – це психологічне насильство.

Почуття провини, робить висновок Келлі, передбачає, що у всіх нас є стержнева система конструктивів. Певні аспекти цієї стержневої структури, які він називав стержневими ролями, є важливими детермінантами нашого сприйняття ідентичності. Прикладами таких стержневих ролей є наші професійні ролі, батька і дитини, близького друга, студента тощо. Так як стержневі ролі є важливими детермінантами нашому житті, їх неадекватне виконання може мати неприємні наслідки.

За Келлі, якщо інша людина інтерпретує ваше виконання стержневої ролі як невдале, з’являється почуття провини: “Вина виникає, коли людина усвідомлює, що відступає від ролей, за допомогою

яких вона зберігає найбільш важливі взаємини з іншими людьми”. Винна людина усвідомлює, що вона вчинила не відповідно до свого внутрішнього я. Концепція провини Келлі в чомусь нагадує концепцію моральної тривоги Фрейда. З точки зору Келлі, ми відчуваємо провину щоразу, коли наші вчинки суперечать нашому сприйняттю самих себе.

З точки зору Фрейда, ми відчуваємо моральну тривогу щоразу, коли наші вчинки суперечать нашому сприйняттю того, що правильно і неправильно (совість). Як вважають обидва теоретики, ми відчуваємо дискомфорт, коли бачимо себе не у відповідності з тим, що очікують від нас, або з тим, чого ми чекаємо від себе: вина – по Келлі, моральна тривога – по Фрейду.

За визначенням Келлі, ворожість – це “постійні спроби отримати факти, які говорять на користь такого типу соціального прогнозу, який вже довів свою неспроможність”. Традиційно розглядається як схильність вести себе мстиво по відношенню до інших або прагнення заподіяти їм шкоду, ворожість в теорії Келлі – просто спроба дотримуватися непридатного конструктиву при зіткненні з протилежним фактором.

Джордж Келлі вважав, що люди сприймають навколишній світ за допомогою чітких систем або моделей, званих конструктивами. Він порівнював людей з ученими, які постійно висловлюють і перевіряють гіпотези про природу речей для того, щоб можна було дати адекватний прогноз майбутніх подій на підставі інформації що надходить та життєвого досвіду.

Емоційний стан відіграє величезну роль в процесі підготовки та проведення маніпуляції свідомістю людини або масовою свідомістю при здійсненні впливу на, мотивацію, раціональне мислення з метою зміни моделей поведінки визначених цільових аудиторій, що в свою чергу посилює негативний психологічний вплив. При виробленні матеріалів для організованого цілеспрямованого втручання у свідомість, фізичний стан цільової аудиторії необхідно враховувати як та чи інша особистість (цільова аудиторія) буде сприймати надану їй інформацію.

### Висновки і перспективи подальших досліджень

Отже, Російською Федерацією здійснювалися інформаційно-психологічні впливи на різні цільові аудиторії під час анексії Автономної республіки Крим та на початку воєнного конфлікту на Донбасі. Інформаційними заходами Російська Федерація продовжує дестабілізувати ситуацію в Україні, сповільнює наш рух до інтеграції з Євросоюзом та НАТО. Проведений аналіз дозволив визначити основні особливості сприйняття та реагування на інформацію, що в свою чергу дасть можливість ефективно скласти психологічний портрет особистості чи відповідної цільової аудиторії з метою вироблення правильних матеріалів інформаційно-психологічного впливу.

### Література

1. Бандурка О.М. Психологія натовпу // Харків: Тітул, 2006. – 208 с. 2. Асмолов О.Г. Психологія особистості: підручник. // Москва: МДУ. 1990, – 259 с. 3. Зелінський С.О. Інформаційно-психологічний вплив на масову свідомість. Засоби масової комунікації, інформації й пропаганди – як провідник маніпулятивних методик впливу на підсвідомість і моделювання вчинків

індивіда й мас. // СПб.: Скіфія. 2008, – 416 с. 4. Войтко О.В., Бочаров М.М., Тіщенко М.Г. Завдання захисту загальновійськових підрозділів від негативного інформаційно-психологічного впливу в ході антитерористичної операції. Науковий журнал “Сучасні інформаційні технології у сфері безпеки та оборони”. 2015. – №2(23). – С. 139-143. 5. Кацалп В.О.,

Войтко О.В., Чернега В.М. Методика оцінки загроз інформаційній безпеці України у війсьній сфері. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". 2018. – №1(31). – С.149-154.

особливостей маніпуляції, як інструменту психологічного впливу на свідомість. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". 2019. – №2(35). – С.121-126.

6. Войтко О.В., Кацалап В.О., Рахімов В.В. Аналіз

## ОСОБЕННОСТИ ВОСПРИЯТИЯ И РЕАГИРОВАНИЯ НА ПОЛУЧЕННУЮ ИНФОРМАЦИЮ

*Александр Владимирович Войтко (кандидат военных наук)  
Виталий Александрович (кандидат военных наук)  
Владимир Николаевич Чернега (кандидат технических наук)*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

*Анализ событий с начала обострения отношений между Украиной и Российской Федерацией свидетельствует о том, что практические меры противодействия информационно-психологическим воздействиям со стороны противника были малоэффективными.*

*Развитие и информатизация общества требует от вооруженных сил новых подходов к ведению вооруженной борьбы, центр которой интенсивно смещается с поля боя в информационное пространство, где происходит главная битва за человека, через его внутреннее эмоциональное состояние.*

*Эмоциональное состояние играет огромную роль в процессе подготовки и проведения манипуляции сознанием человека или массовым сознанием при осуществлении воздействия на, мотивацию, рациональное мышление с целью изменения моделей поведения определенных целевых аудиторий, в свою очередь усиливает негативное психологическое воздействие. При создании материалов для организованного целенаправленного вмешательства в сознание, необходимо учитывать как та или иная личность (целевая аудитория) будет воспринимать предоставленную ей информацию.*

*Целью данной статьи является анализ особенностей восприятия и реагирования общества (определенных целевых аудиторий) на информацию, циркулирующую в их информационном пространстве. Определяется, классификация целевых аудиторий по способам восприятия и реагирования на полученную информацию.*

*Ключевые слова: целевая аудитория, информационно-психологическое воздействие, восприятие информации, реагирование на информацию, психологический портрет.*

## THE PECULIARITIES OF PERCEPTION AND RESPONSE TO THE INFORMATION PRODUCED

*Oleksandr Voitko (Candidate of Military Sciences)  
Vitalii Katsalap (Candidate of Military Sciences)  
Volodymyr Cherneha (Candidate of Technical Sciences)*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*An analysis of the events from the beginning of the aggravation of relations between Ukraine and the Russian Federation suggests that practical measures to counter the information and psychological influences from the enemy were ineffective.*

*The development and informatization of society requires the armed forces to take new approaches to the conduct of armed struggle, the center of which is being intensively shifted from the battlefield to the information space, where the main battle for man takes place, through his internal emotional state.*

*The emotional state plays a huge role in the process of preparing and manipulating a person's consciousness or the mass consciousness; effects on motivation and rational thinking are carried out. The goal is to change the behavior patterns of certain target audiences. This enhances the negative psychological impact. When creating materials for organized targeted intervention in the consciousness, it is necessary to consider how the person (target audience) will perceive the information provided.*

*The purpose of this article is to analyze the peculiarities of the perception and response of society (certain target audiences) to the information that circulates in their information space. It determines the classification of target audiences according to the methods of perception and response to the information produced.*

*Key words: the target audience, information psychological impact, perception of information, response to the information, psychological picture.*

### References

1. Bandurka O.M. (2006). Psychology of crowd. Kharkiv: Titul. 208 p. 2. Asmolov O.Gh. (1990). Psychology of Personality. Moskva: MDU, 259 p. 3. Zelinsky S.O. (2008) Information and psychological impact on the mass consciousness. The media of communication, information and propaganda – as a conductor of manipulative methods of influencing the subconscious and modeling the actions of the individual and the masses. SPb.: Skifija. 416 p. 4. Bocharov M.M., Voitko O.V., Tyshchenko M.H. (2015). The combined arms units protection task from the negative information and psychological warfare during the anti terrorist operation. Scientific journal "Modern Information

Technologies in the Sphere of Security and Defence". №2(23). pp. 139-143. 5. Katsalap V.O., Voitko O.V., Cherneha V.M. (2018). Methodology of estimation of threats of information security of Ukraine in the military field. Scientific journal "Modern Information Technologies in the Sphere of Security and Defence". №1(31). pp. 149-154. 6. Katsalap V.O., Voitko O.V., Rakhimov V.V. (2019). Analysis of features of manipulation, as to instrument of psychological influence on consciousness. Scientific journal "Modern Information Technologies in the Sphere of Security and Defence". №2(35). pp. 121-126

# Шановні колеги!

Запрошуємо до участі в науковому журналі

“Сучасні інформаційні технології у сфері безпеки та оборони”,

Видавець: Національний університет оборони України імені Івана Черняхівського

Наказом Міністерства освіти і науки України

від 29 грудня 2014 р. №1528 журнал включено до Переліку наукових фахових видань України в галузях “технічні науки” та “військові науки”

Наклад – 100 примірників, відкрите видання.

## Основні тематичні напрями журналу:

- |   |   |
|---|---|
| 1. Військова кібернетика та системний аналіз  | інформаційно-телекомунікаційних систем                                    |
| 2. Протиборство у кібернетичному просторі   | 7. Стратегічні комунікації та когнітивні системи спеціального призначення |
| 3. Військово-космічні та геоінформаційні технології                                   | 8. Інтерактивні моделі розвитку науково-освітнього простору;              |
| 4. Інтелектуальні інформаційні технології та робототехніка у сфері безпеки та оборони | 9. Високотехнологічні аспекти воєнного мистецтва                          |
| 5. Інформаційно-аналітична діяльність у сфері безпеки та оборони                      | 10. Історичний дискурс розвитку високих оборонних технологій              |
| 6. Розвиток теорії та практики створення  |   |

## Схема оформлення статей

**DOI** (Arial, кегль – 11 пт.)

← 1 пустий рядок – 6 пт.

**УДК** (Arial, кегль – 11 пт.)

← 1 пустий рядок – 10 пт.

<sup>1</sup> **Анатолій Анатолійович Іванов** (д-р техн. наук, професор)

← (кегль – 11 та 8 пт.)

<sup>2</sup> **Іван Іванович Петров** (канд. техн. наук, доцент, доцент кафедри)

← 1 пустий рядок – 6 пт.

<sup>1</sup> **Університет..., Київ, Україна**

<sup>2</sup> **Інститут..., Київ, Україна**

← (кегль – 11 пт.)

← 1 пустий рядок – 10 пт.

**НАЗВА СТАТТІ** (Arial, кегль – 14 пт.; накреслення – “напівжирне”, по правому краю)

← 1 пустий рядок – 10 пт.

Текст анотації мовою тексту статті (в даному випадку – українською). Зміст анотації має стисло і достатньо інформативно підсумовувати основні ідеї та отримані результати дослідження. Розмір анотації повинен становити не менше 250 слів. Зверніть увагу на те, що дані про авторів, назва, ключові слова та анотація будуть використані як метадані для опису Вашої статті, тому вони повинні максимально чітко описувати її зміст. Для більш якісного пошуку даного контенту в мережі, будь ласка, уникайте занадто узагальнених та складних формулювань, використовуйте тільки загальновідомі аббревіатури. (Обсяг анотації – не менше 250 слів.)

**Ключові слова:** поняття1; поняття2; поняття3. (кегль – 10 пт.)

## Вимоги до набору

**Формат аркуша:** А4 (21 × 29,7 см).

**Параметри сторінки** (відступи від краю): зліва – 3 см.; справа – 2 см.; зверху – 2 см.; знизу – 2 см.

**Шрифт статті** – Times New Roman; накреслення – пряме; кегль – 10 пт.; міжрядковий інтервал – одинарний.

**Текст статті** розташовується у два стовпчики однакової ширини – 7,75 см.; відстань між стовпчиками – 0,5 см.; відступ першого рядка абзацу – 0,5 см.; вирівнювання – за шириною.

**Підзаголовок** – кегль – 12 пт.; накреслення – напівжирне; відступів немає; вирівнювання – центроване.

Не використовуйте для форматування тексту пропуски, табуляцію тощо. Не встановлюйте ручне перенесення слів, не використовуйте колонитиули. Між значенням величини та одиницею її вимірювання ставте нерозривний пропуск (Ctrl + Shift + пропуск).

**УВАГА! Остання сторінка статті заповнюється не менше 3/4, рекомендована парна кількість аркушів.**

**Кількість авторів – не більше трьох.**

**Набір формул:** редактор формул MS Equation.

**Забороняється** використовувати для набору формул графічні об'єкти, кадри й таблиці.

В меню “Размер → **Определить**” ввести такі розміри: Обычный – 10 пт.; Крупный индекс – 8 пт.; Мелкий индекс – 7 пт.; Крупный символ – 15 пт.; Мелкий символ – 9 пт.

Стиль формул – “прямий”, тобто в меню “Стиль → **Определить**” поля “Формат символів” – пусті.

Табличний заголовок (10 пт.) – **обов’язковий**.

Рисунки **обов’язково** супроводжуються центрованими підписаними підписами (кегль – 10).

**Не допускаються** кольорові та фонові рисунки.

Допускається розташування великих рисунків, формул та таблиць в одну колонку (до 16 см.).

Список літератури виділяється підзаголовком “**Література**” та оформлюється згідно з міждержавним стандартом ДСТУ 8302:2015” (кегль – 9 пт.).

## Структура рукопису

Відповідно до постанови ВАК України від 15.01.2003 № 7-05/1 текст статті повинен мати таку структуру: **постановка проблеми** у загальному вигляді та її зв’язок із важливими науковими чи практичними завданнями; **аналіз останніх досліджень і публікацій**, на які спирається автор; **формулювання мети статті** (постановка завдання); **виклад основного матеріалу дослідження з повним обґрунтуванням отриманих**

наукових результатів; висновки з даного дослідження і перспективи подальших досліджень у даному напрямку.

Текст статті розбивається на відповідні розділи з підзаголовками, які виділені напівжирним шрифтом.

Робочі мови – українська, російська, англійська.

На останньому аркуші статті після списку літератури наводяться: назва статті, прізвище, ім'я, по батькові, науковий ступінь та вчене звання автора (співавторів),

назва організації, у якій працює автор (співавтори), анотація та ключові слова українською, російською та англійською мовами (крім основної мови статті) за нижченаведеним зразком (10 кегль (8 для наукового ступеня, звання, посади), міжрядковий інтервал – 1,0, вирівнювання – по центру). **Обсяг анотації – не менше 250 слів.**

## НАЗВАННЯ СТАТТІ

<sup>1</sup>*Анатолій Анатолієвич Іванов (д-р техн. наук, професор)*  
<sup>2</sup>*Іван Іванович Петров (канд. техн. наук, доцент, доцент кафедри)*  
<sup>1</sup>*Університет..., Київ, Україна*  
<sup>2</sup>*Інститут..., Київ, Україна*

*Перевод текста аннотации и ключевых слов*

## ARTICLE TITLE

<sup>1</sup>*Anatolii Ivanov (Doctor of technical sciences, professor)*  
<sup>2</sup>*Ivan Petrov (Candidate of technical Sciences, associate professor)*  
<sup>1</sup>*University..., Kyiv, Ukraine*  
<sup>2</sup>*Institute..., Kyiv, Ukraine*

*Translation of the abstract and keywords*

англійською мовою за зразком (9 кегль):

Після цього наводиться список літератури

## References

1. Концепція розвитку телекомунікацій в Україні, схвалена Розпорядженням Кабінету Міністрів України від 7 червня 2006 р. № 316-р. 2. **A.O. Moskalenko, Gh.V. Sokol.** Pereshkodostijkistj syghnaliv moduljaciji cyklichnym zsumom kodu z adaptacijeju po shvydkosti peredachi informaciji. *Systemy upravlinnja, navigaciji ta zv'jazku.* Kyjiv. 2018. № 3(49). S. 175-180. 3. **A.O. Moskalenko, S.V. Voloshko, I.I. Sljusarj** Pereshkodostijkistj syghnaliv udoskonalenoji moduljaciji cyklichnym zsumom kodu z adaptacijeju po shvydkosti peredachi informaciji v umovakh baghatopromenevogo

rozpovsjudzhennja radiokhvylyj. *Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony.* Kyjiv. 2015. № 2 (23). S. 35–39. 4. **A.A. Moskalenko, Gh.V. Sokol** Metod synteza syghnalov usovershenstvovannoji moduljaciji cyklycheskym sdvyghom koda s adaptacijeju po skorosty peredachy ynformacyy. *Informacijno kerujuchi systemy na zaliznychnomu transporti.* Kharkiv. №3 (100).2013.S.71-75. 5. **G.M. Dillard et all,** Cyclic Code Shift Keying: A Low Probability of Intercept Communication Technique // *IEEE Trans. Aersp. Electron. Systems., vol. AES-39, July 2003,* pp. 786 -798.

**Корисні посилання для здійснення транслітерації:**

<http://translit.kh.ua/?passport> – автоматична транслітерація з української мови

<http://translate.meta.ua/ua/translit/> – автоматична транслітерація з російської мови

**На окремому аркуші наводяться відомості про рецензента та авторів.**

**Рецензент:** Прізвище, ім'я та по-батькові; посада; наукова ступінь та вчене звання; адреса електронної поштової скриньки; контактний телефон; ORCID ID в форматі: <http://orcid.org/0000-0001-9037-787X>

**Автор:** Прізвище, ім'я та по-батькові; посада; вчена ступінь та вчене звання; адреса електронної поштової скриньки; контактний телефон; ORCID ID в форматі: <http://orcid.org/0000-0001-9037-787X>

## Подання матеріалів

Обсяг рукопису – від 4 до 10 аркушів українською, російською або англійською мовами.

Для публікації необхідно надіслати статтю у електронній формі (**doc** та **pdf** – копія оригіналу з відомостями щодо відсутності інформації з обмеженим доступом та підписаними всіма авторами статті кожного аркуша).

Рукопис супроводжується рецензією доктора наук (професора), витягом з протоколу засідання кафедри (відділу).

Подані матеріали автору не повертаються.

Матеріали просимо подавати через сайт журналу або до інституту інформаційних технологій Національного університету оборони України імені Івана Черняхівського за адресою: 03049, м. Київ, Повітрофлотський пр., 28, тел.: (044) 271-07-31, Войтку Олександр Володимировичу, каб. 2/309, тел.: 098-2734862, e-mail: [sitnuou@ukr.net](mailto:sitnuou@ukr.net).

З питань оплати звертатись до редакції.

Редколегія залишає за собою право відмови у публікації статей, що не відповідають проблематиці журналу, умовам оформлення матеріалів.