

# СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ БЕЗПЕКИ ТА ОБОРОНИ

ISSN 2311-7249 (Print)

ISSN 2410-7336 (Online)

№ 1(37)  
2020

## 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 № 5, 25.05.2020 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

Дачковський В.О., Коцюрба В.І. Методика оцінювання ефективності функціонування відновлення озброєння та військової техніки .....5  
Доска О.М., Опенько П.В., Дудуш А.С., Сургай М.В. Визначення показника ефективності відновлення зенітного ракетного озброєння з урахуванням ресурсних обмежень .....15  
Білобородов О.О. Управління шириною діаграми направленості і потужністю випромінювання антенної системи .....21  
Машикін О.О. Елементи імітації у рівняннях моделей манчестерського типу .....27

#### Протиборство у кібернетичному просторі

Вдовенко В.Г., Даник Ю.Г., Пермяков О.Ю. Гібридні загрози у кіберпросторі: фактори впливу на природу виникнення .....31

#### Військово-космічні та геоінформаційні технології

Каневський Л.Б., Повх М.С., Шумський С.М. Перспективи комбінованого використання видових засобів повітряно-космічного базування для підвищення інформативності розвідувального забезпечення військ (сил) .....49  
Бекіров А.Е., Яценко В.Ж., Крейдун О.С. Технологія селекції областей аерофотознімку з різною насиченістю для стегаграфічного перетворення .....55  
Гусак Ю.А., Стринський І.М. Моделювання дії радіолокаційної розвідки в комплексній системі виявлення безпілотних літальних апаратів .....61

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

Сотник В.В., Расстрижін О.О., Купчин А.В. Методика відбору критичних технологій ... 67  
Гащенко С.С., Ліценко О.М., Сотніченко А.І., Жарков Я.А. Математична модель процесу розвідувально-інформаційної діяльності в умовах невизначеності .....77  
Зуйко В.В., Мельник С.А., Лук'яничков І.М., Повеценко О.В. Методика оцінювання інформаційних документів в інтересах забезпечення інформаційної діяльності .....85  
Сергієнко В.Д., Павлушко М.Я., Шапран О.О., Муляка А.С. Особливості впливу акустичної збій на особовий склад військових формувань в умовах ведення не конвенційних воєнних дій .....93  
Гащенко С.С., Костенко О.В., Кузьменко В.П., Мазуренко В.М. Методика ранжування джерел розвідувальних відомостей радіоелектронної розвідки при організації і веденні розвідки .....97  
Крайнов О.В., Маланчук М.Ф., Грозовський Р.І. Методика оцінки ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління .....103  
Кузнецов В.В., Повеценко О.В., Оксенчук І.С., Ніколаєнко В.П. Удосконалена методика раціонального розподілу інформації за важливістю і кількістю джерел радіомоніторингу в АСУ військами та зброєю .....107  
Боровик О.В., Боровик Л.В., Андрушко О.В. Удосконалення науково-методичного апарату розпізнавання рівня небезпеки ситуацій у разі зміни характеристик інформованості особи, яка приймає рішення .....115  
Пермяков О.Ю., Прибілес Ю.Б., Бобильов В.С. Підхід щодо побудови універсальної автоматизованої контрольної-випробувальної станції зі застосуванням експертних систем .....125

#### Інтерактивні моделі розвитку науково-освітнього простору

Чопя Д.А., Дерев'янчук А.І., Чехута Д.А. Деякі аспекти створення та застосування мобільних додатків для вивчення військово-технічних наук .....151  
Кравченко Ю.В., Мусієнко А.П., Тищенко М.Г., Гоголянц С.Ю. Методика опрацювання експертних даних для удосконалення системи дистанційного навчання в ЗС України .....157

#### Високотехнологічні аспекти воєнного мистецтва

Мацько О.Й., Солоніков В.Г., Костюченко С.М. Застосування моделі технічного обслуговування техніки з почасовою надмірністю для підвищення її надійності в ході виконання завдань підрозділами інженерних військ ЗС України при проведенні операції Об'єднаних сил .....163  
Боднакович В.Ю., Дублян О.В., Сиротенко А.М., Передній О.В., Прима А.М. Методика прогнозного оцінювання ефективності асиметричного реагування Збройних Сил України на загрози у воєнній сфері .....171  
Шевченко В.К., Волощенко О.І., Бобрун О.В. Спосіб визначення величини впливу фортифікаційного обладнання на живучість системи управління військами (силами) в операції (бойових діях) .....179  
Репіло Є.Ю., Мостовий А.І. Аналіз прикордонної безпеки на сході України та особливості її забезпечення силами та засобами прикордонних загонів в районі ООС .....185  
Гусак Ю.А., Шевченко В.К. Методичний підхід щодо аналізу живучості системи пунктів управління .....191

Стратегічні комунікації та когнітивні системи спеціального призначення  
Кривошеєв В.В., Кацалпа В.О. Аналіз експлуатації діючих макетів комплексу спеціальних апаратних підрозділів інформаційно-психологічних операцій .....197  
Солоніков В.Г., Войтко О.В., Пащенко Т.П. Обґрунтування реалізації стратегічного нарративу держави .....202

---

## **Редакційна колегія**

### ***Головний редактор***

**РАКУШЕВ Михайло Юрійович,**

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

### ***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)

№ 1(37)  
2020

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 №20490-10290IIP)

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 № 5, 25.05. 2020)*

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*

<i>Dachkovskiy V., Kotsiuruba V.</i> Method of evaluation of efficiency of functioning of arms and military engineering system.....	5
<i>Doska A., Open'ko P., Dudush A., Surgai M.</i> Determining the recovery efficiency index of anti-aircraft missile armament, taking into account resource constraints.....	15
<i>Biloborodov O.</i> Control beamwidth and radiation power of antenna system.....	21
<i>Mashkin O.</i> Imitation elements in the Lanchester model equations.....	27

### *Confrontation in the cybernetic*

<i>Vdovenko S., Danyk Y., Permiakov O.</i> Experience of development of cyber security systems and cyber defense foreign states.....	31
--	----

### *Military space and geoinformation technologies*

<i>Kanevskiy L., Povkh M., Shumskiy S.</i> Prospects of combined use of specific aircraft bases for improvement of informative sensitiveness.....	49
<i>Bekarov A., Yachenok V., Krejdan A.</i> Technology of selection of aerial photo area with various saturation for a stenographic transformation.....	55
<i>Husak Y., Shovkoshytnyi I., Starynskiy I.</i> The action simulation of radar intelligence in a complex system the discovery of unmanned aerial vehicles.....	61

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

<i>Sotnyk V., Rasstrygin O., Kupchyn A.</i> Method of the critical technologies selection.....	67
<i>Hatsenko S., Lishchenko O., Sotnichenko A., Zharkov Y.</i> Mathematical model of the research and information activity process in uncertainty.....	77
<i>Zuiko V., Melnyk S., Lukianchikov I., Poveshchenko O.</i> Method of evaluation information documents in interest providing information activities.....	85
<i>Serhiienko V., Pavlunko M., Shapran O., Muliavka A.</i> Peculiarities of acoustical weapon effects on personal composition of military formations in conditions of not conventional military action.....	93
<i>Hatsenko S., Kostenko O., Kurzenko V., Mazurenko V.</i> Methods of organizing resources sources of radio electronic intelligence in organization and exercise.....	97
<i>Krainov O., Malanchuk M., Hrozovskiy R.</i> Methodology for estimating the effectiveness of an integrated information protection system for automated information systems of military management bodies.....	103
<i>Kuznetsov V., Poveshchenko O., Oksenchuk L., Nikolaienko V.</i> The methodology of rational distribution of information by importance and quantity of radio monitoring sources is improved in ACS arms and weapons.....	107
<i>Borovyk O., Borovyk L., Andrushko A.</i> Improvement of the scientific and methodological apparatus by recognizing the level of danger of the situation in the case of changing the characteristics of the informing of the decision maker.....	115
<i>Permjakov A., Pribyliyev Y., Bobyluov V.</i> Approach to building a universal automated control and test station with use of expert systems.....	125
<i>Pravdyvets O., Kozlov V.</i> Method of determination of the number of clients's part kits of the unified state reservers register.....	133
<i>Degtyaryova L., Voloshko S., Loza V., Bulankina A.</i> The use of information technology for data processing in modern transport logistics systems.....	139
<i>Bychenok M.</i> Evaluation risks of live activity of people in natural and technogenic environment in conditions of special period.....	145

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

<i>Chopa D., Derevianchuk A., Chehuta D.</i> Some aspects of creating and using mobile applications for the learning of military technical disciplines.....	151
<i>Kravchenko Y., Musienko A., Tyshchenko M., Hohoniants S.</i> The expert data processing method for the distance learning system improvement in the armed forces of Ukraine.....	157

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

<i>Matsko O., Solonnikov V., Kostiuchenko S.</i> Application of the technical support model with variable redundancy to increase its reliability during tasks by the units of engineering aircraft of Ukraine when the joint force operations are performed.....	163
<i>Bohdanovych V., Dublian O., Syrotenko A., Peredrii O., Pryma A.</i> Methodology for forecasting assessing the effectiveness of the asymmetric response of the armed forces of Ukraine to threats in the military sphere.....	171
<i>Shevchenko V., Voloshchenko O., Bobrun O.</i> Method of determining the magnitude of the effect of fortification equipment on the survivability of the troops (forces) control system in the operations (combat actions).....	179
<i>Repilo L., Mostovyi A.</i> Border security analysis in eastern Ukraine and peculiarities of providing it by forces and facilities of border guard detachments in the area of joint forces operation.....	185
<i>Husak Y., Shevchenko V.</i> Methodical approach to analysis of survivability of control points system.....	191

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

<i>Krivoshchiv V., Katsalap V.</i> Analysis of operation of existing models of the complex of special machinery for information-psychological operations subsection.....	197
<i>Solonnikov V., Voitko O., Pashchenko T.</i> Reasons for implementation the strategic draft of the state.....	202

---

## 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

*Oleksandr MATSKO,*

candidate of military sciences, professor

*Yurii DANYK,*

doctor of technical sciences, professor

*Ivan KATERYNCHUK,*

doctor of technical sciences, professor

*Volodymyr KOTSIURUBA,*

doctor of technical sciences, associate professor

*Yurii KRAVCHENKO,*

doctor of technical sciences, professor

*Andrii ZINCHENKO,*

doctor of technical sciences, professor

*Serhii KOVBASJUK,*

doctor of technical sciences,  
senior research fellow

*Ihor RUBAN,*

doctor of technical sciences, professor

*Serhii HATSENKO,*

candidate of technical sciences

*Vitalii SAVCHENKO,*

doctor of technical sciences, professor

*Maryna MALANCHUK,*

candidate of economic sciences

*Goran SHIMIC,*

doctor of philosophy, professor

*Oleksandr PERMIAKOV,*

doctor of technical sciences, professor

*Oleksandr VOITKO,*

candidate of military sciences

*Ihor VARLAMOV,*

candidate of technical sciences,  
associate professor

*Anatolii LOBANOV,*

doctor of military sciences, professor

*Ihor ROMANCHENKO,*

doctor of military sciences, professor

*Vasyl TELELYM,*

doctor of military sciences, professor

*Yurii REPILO,*

doctor of military sciences, professor

*Volodymyr SHEMAIEV,*

doctor of military sciences, professor

*Vladyslav SOLONNIKOV,*

doctor of technical sciences, professor

*Oleksandr LAVRINCHUK,*

candidate of technical sciences,  
senior research fellow

### *Executive Secretary:*

*Oleksandr VOITKO,* candidate of military sciences

*Володимир Олександрович Дачковський (кандидат технічних наук)*

*Володимир Іванович Коцюруба (доктор технічних наук, доцент)*

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

## МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ВІДНОВЛЕННЯ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

*Аналіз застосування підрозділів та військових частин в локальних війнах та збройних конфліктах дозволяє стверджувати, що одним із основних показників, які впливають на успіх у виконанні завдань є наявність у військових частинах (підрозділах) працездатних зразків озброєння та військової техніки. При цьому, одним із основних джерел надходження працездатних зразків озброєння та військової техніки у військові частини (підрозділи) в ході ведення бойових дій є повернення їх із стаціонарних та рухомих ремонтно-відновлювальних військових частин (підрозділів) після виконання заходів з їх відновлення.*

*Тому для оцінювання ефективності відновлення озброєння та військової техніки запропонована методика оцінювання ефективності функціонування системи відновлення. Суть якої полягає в отриманні відомості про надійність відновлення озброєння та військової техніки за номенклатурою в кожній ланці структури системи відновлення, кількості відновлених зразків озброєння та військової техніки на кожному рівні ієрархії, кількості неохоплених ремонтно-відновлювальними роботами зразків озброєння та військової техніки в кожній ланці, кількості працездатних зразків озброєння та військової техніки на кожену добу операції (бойових дій). Методика дозволяє варіювати кількістю ремонтних бригад і їх розподілом за ланками структури. Введення змінних оперативно-тактичних ситуацій реалізується головним чином через фонд робочого часу.*

***Ключові слова:** озброєння та військова техніка; відновлення; моделювання; виробничі можливості; ремонтно-відновлювальні підрозділи.*

### Вступ

Успішне вирішення завдань військовими частинами (підрозділами) під час виконання завдань в операціях (бойових діях) забезпечується ефективним застосуванням всіх видів озброєння та військової техніки (ОВТ).

Аналіз ведення локальних війн та збройних конфліктів ХХ-ХХІ ст. дає змогу стверджувати, що розвиток концепції дальнього вогневого ураження з широким використанням засобів високоточної зброї, приводить до значного збільшення обсягу пошкоджень, які отримують зразки ОВТ [1-2]. Таким чином, вирішення завдання щодо підтримання боєздатності військових частин (підрозділів), за рахунок укомплектованості основними зразками ОВТ, стає досить актуальним і може бути частково розв'язане шляхом відновлення пошкоджених зразків ОВТ силами ремонтно-відновлювальних військових частин (підрозділів).

**Постановка проблеми.** Відновлення ОВТ, які вийшли з ладу в ході операції (бойових дій), є однією із головних та найбільш складних функцій системи логістики Збройних Сил України та сил оборони держави. Так, як для підтримання високої боєздатності військових частин та підрозділів в ході операції (бойових дій) основним джерелом поповнення справними або працездатними зразками ОВТ будуть зразки, які надходять з

ремонтно-відновлювальних військових частин (підрозділів).

Необхідність організації заходів з відновлення пошкоджених зразків ОВТ обумовлена [3]: обмеженими можливостями країни із створення та утримання необхідного для військ резерву зразків ОВТ; значно меншим часом на повернення у військові частини (підрозділи) відремонтованих зразків ОВТ у порівнянні з часом надходження ОВТ із арсеналів, баз, складів оперативного та стратегічного рівнів; недоцільністю відмови від повернення у військові частини (підрозділи) ремонтпридатних і відносно дорогих за вартістю зразків ОВТ.

Виконання заходів з відновлення ОВТ, які направлені на підтримання готовності військ до виконання бойових завдань за рахунок укомплектування їх боєздатними зразками ОВТ в смузі (районі) бойових дій військ забезпечується створенням відповідної системи ремонтно-відновлювальних органів, яка у своєму складі може мати як рухомі, так і стаціонарні ремонтно-відновлювальні підрозділи, в залежності від обсягу та складності завдань. Система відновлення складається з декількох рівнів ієрархії: стратегічного, оперативного та тактичного. Склад сил та засобів, що входять до кожного рівня ієрархії системи відновлення, відповідає завданням, які визначаються тому чи іншому

ремонтно-відновлювальному підрозділу [4-5].

Успішне вирішення завдань, які покладаються на систему відновлення будь якого рівня ієрархії, залежить, перш за все, від цілеспрямованого управління діяльністю усієї системи. Ефективність управління і, як наслідок, ефективність виконання завдань, які покладені на систему відновлення, залежить від виробничих можливостей ремонтно-відновлювальних військових частин (підрозділів) які залучаються до виконання завдань. Саме тому виникає низка проблемних питань серед яких особливе місце займає оцінювання ефективності функціональної системи відновлення ОВТ та визначення її надійності для різних ситуацій.

#### **Аналіз останніх досліджень і публікацій.**

Дослідженню питань функціонування системи відновлення ОВТ в мирний час і в особливий період присвячена ціла низка робіт, зокрема в роботі [6] запропоновано метод моделювання на основі комплексного підходу, що базується на побудові і дослідженні математичної моделі системи забезпечення боєздатності парку ОВТ угруповання військ. Дана модель враховує зовнішні чинники, які впливають на систему а саме чинники, які обумовлюють отримання пошкоджень зразкам ОВТ і потребу в боеприпасах і МТЗ. У роботі [7] розглядаються питання удосконалення інформаційного забезпечення перспективної автоматизованої системи управління матеріально-технічним забезпеченням шляхом формування процедури прогнозування очікуваних пошкоджень зразків ОВТ.

Так у роботі [8] запропоновано метод оцінювання надійності ремонтних підприємств ОВТ на основі експертного поведіння з процедурами та результатами впровадження експертних оцінок. В методі використовується аналітичний мережевий процес. Кластери, що складають мережу оцінювання, залежать від постачання комплектуючих та матеріалів від інших постачальників, а у роботі [9] проведений аналіз системи технічного забезпечення засобів зв'язку і автоматизації враховуючи потребу наближення системи військового управління Збройних Сил до стандартів НАТО. В роботі [10] запропоновано метод прогнозування величини втрат озброєння та військової техніки під час ведення операцій (бойових дій), а в роботі [11] запропоновано порядок кількісної оцінки ймовірнісних показників для підвищення якості прогнозування навантаження на військові ремонтні органи. В літературних джерелах [12] наведено напрямки удосконалення технологічного процесу відновлення ОВТ шляхом застосування нових рухомих засобів ремонту і технічного обслуговування, а у роботі [13] розглянуто задачі оптимального управління процесом відновлення ОВТ під час виконання завдань за призначенням в ланці батальйон. В якості критерію оптимізації розглянуто показник справності та бойової готовності зразків ОВТ а також питомі витрати на відновлення ОВТ. В роботі [14] розглянуто

систему технічного забезпечення військ зв'язку ЗС України за досвідом проведення бойових дій складовою якої є підсистема відновлення. Окремі аспекти даної проблематики викладені у роботі [15] яка присвячена оцінюванню ефективності застосування нової метрологічної техніки та направлена на забезпечення виконання завдання щодо забезпечення точності вимірювань основних параметрів системи, а робота [16] присвячена аналізу військових систем з метою виявлення проблемних питань та їх вирішення. Опрацювання цієї проблеми відображено також у роботі [17] яка присвячена аналізу факторів які впливають на ефективність функціонування системи відновлення ОВТ.

**Мета статті.** Мета статті полягає у розробленні методики оцінювання ефективності функціонування системи відновлення ОВТ, яка б дозволила порівнювати імовірний вихід ОВТ з ладу з виробничими можливостями ремонтно-відновлювальних військових частин (підрозділів) відповідного рівня ієрархії та визначити неохоплений ремонтного фонду, який необхідно передавати на вищий рівень ієрархії. Дослідження проводилося в рамках науково-дослідної роботи шифр "Потенціал". У ході дослідження використовувалися такі методи: аналіз теоретичних джерел з проблем функціонування системи відновлення ОВТ, метод багаторазової регресії та кореляційного аналізу для обчислення надійності відновлення в різних ситуаціях, моделювання процесу відновлення ОВТ, факторний аналіз для визначення взаємодії факторів.

#### **Виклад основного матеріалу дослідження**

З метою оцінювання ефективності функціональної системи відновлення ОВТ досить визначити надійність системи відновлення, яка має фіксовані характеристики, для можливо більшого набору ситуацій. Потім відомими методами слід визначити ймовірність того, що відхилення надійності відновлення від необхідного рівня буде не більше допустимого інтервалу. Отже завдання зводиться до багаторазового обчислення надійності відновлення в різних ситуаціях. Враховуючи відому структуру військ, способи оцінювання надійності відновлення: графоаналітичний з використанням номограм і моделювання процесу відновлення ОВТ [18]. В основі обох із них лежить порівняння очікуваного обсягу ремонтного фонду із виробничими можливостями ремонтно-відновлювальних військових частин (підрозділів). Разом з тим кожен з них має свої особливості.

Графоаналітичний спосіб з використанням номограм дозволяє обчислити надійність відновлення ОВТ для різних конкретних умов бойової обстановки з урахуванням великої кількості факторів як для окремого ремонтно-відновлювального підрозділу (військової частини),

так і для комплексу ремонтно-відновлювальних військових частин (підрозділів), які приймають участь в операції (бойових діях) [19]. Одним з основних недоліків цього способу є складність обліку та реалізації принципу подвійного пріоритету в системі відновлення ОВТ. Як правило, розрахунки ведуться для основних зразків ОВТ.

Інший його недолік, але вже з позицій виявлення можливих шляхів вдосконалення системи, полягає в складності введення тих чи інших змін у характеристики системи відновлення ОВТ. Це ускладнює його використання для оцінювання надійності відновлення ОВТ різних систем в однакових ситуаціях.

Моделювання процесу відновлення ОВТ забезпечує облік набагато більшої кількості факторів. Крім того, цей спосіб дає можливість здійснювати моделювання для різних організаційно-штатних структур системи відновлення на будь-якому рівні ієрархії військ [20]. Тому основну увагу необхідно зосередити саме на цьому способі.

З метою спрощення моделі приймемо деякі допущення:

рівень середньодобових втрат ОВТ не залежить від номенклатури ОВТ і місця військових частин (підрозділів) в оперативній побудові військ. Таке припущення забезпечує достатню точність отриманих результатів при моделюванні процесу відновлення ОВТ у оперативно-тактичному, оперативному угрупованні військ;

технічною розвідкою виявляються усі несправні зразки ОВТ;

евакуація пошкоджених зразків ОВТ з-під вогню противника здійснюється в найближче укриття або на збірний пункт пошкоджених машин (ЗППМ) до підходу ремонтних засобів;

ремонт ОВТ повністю забезпечений необхідними матеріально-технічними засобами (МТЗ), (вузлами, агрегатами, тощо);

увесь ремонтний фонд, не охоплений ремонтно-відновлювальними органами нижчої ланки, передається до вищої ланки;

вихід ОВТ в плановий ремонт протягом даної операції виключається;

цикл відновлення ОВТ в ремонтно-відновлювальних підрозділах тактичного рівня становить одну добу, для оперативного рівня – дві доби, для оперативного рівня при виконанні середніх ремонтів – чотири доби і для стратегічного рівня, які виконують середній ремонт – десять діб;

розподіл ремонтного фонду по трудомісткості робіт описується експоненціальним законом.

Принципи функціонування системи відновлення враховуються в даній методиці наступним чином:

ремонтно-відновлювальні підрозділи тактичного рівня відновлюють усі зразки ОВТ, які потребують поточного ремонту з об'ємом робіт до 100 люд./год., а ремонтно-відновлювальні

військові частини оперативного рівня – зразки ОВТ які потребують поточного ремонту з об'ємом робіт понад 100 люд./год., та ті які потребують середнього ремонту;

ремонтний фонд, який передається з ремонтно-відновлювальних органів нижчої ланки до вищої, відновлюється в ньому в першу чергу;

в кожній ланці зразки ОВТ відновлюються за пріоритетом значимості:

машини управління, засоби ведення вогню, базові платформи ракетних комплексів, базові платформи артилерійських комплексів, танки, БМП, БТР, тощо.

Застосування агрегатного методу ремонту враховується введенням в трудомісткості ремонту головним чином демонтажно-монтажних робіт по заміні несправних агрегатів і вузлів [21-22].

Сутність методики моделювання процесу відновлення ОВТ полягає у послідовному порівнянні ремонтного фонду певної трудомісткості протягом кожної доби операції з виробничими можливостями ремонтно-відновлювальних підрозділів відповідного рівня ієрархії, у визначенні обсягу неохопленого ремонтного фонду і у передачі його на вищий рівень.

Для підготовки і виконання зазначених операцій приймемо такі позначення:

$i$  – індекс номенклатури ОВТ за пріоритетом значимості (для простоти будемо розглядати п'ять груп зразків ОВТ:  $i=1$  – машини управління і базові платформи,  $i=2$  – танки,  $i=3$  – БМП,  $i=4$  – БТР і  $i=5$  – допоміжні машини тощо);

$I$  – кількість номенклатури ОВТ, для якої ведеться розрахунок (в розглянутому прикладі  $I=5$ );

$j$  – індекс ланки структури військ і відповідної ланки структури системи відновлення ( $j=1$  – батальйон і його підрозділ, які призначені для відновлення ОВТ,  $j=2$  – бригада та її ремонтно-відновлювальний підрозділ,  $j=3$  – оперативно-тактичне угруповання військ і ремонтно-відновлювальна військова частина, яка входить до його складу;

$J$  – кінцева кількість різних ланок структури військ в залежності від рівня, до якого ведеться розрахунок.  $J$  залежить від угруповання військ, яке розглядається;

$k$  – індекс виду ремонту (трудомісткості). За перспективною класифікацією:  $k=1$  – поточний ремонт першого ступеня;  $k=2$  – поточний ремонт другого ступеня;  $k=3$  – поточний ремонт третього ступеня;  $k=4$  – середній ремонт тощо. (в розглянутому прикладі  $k_{\max}=7$ );

$K$  – кінцеве значення рівня структури системи відновлення, для якого ведеться розрахунок.

Аналогічно можна відпрацювати індексацію для решти групи змінних факторів, що діють як при визначенні ремонтного фонду, так і при визначенні виробничих можливостей системи

відновлення ОВТ [23]. Можна розглядати  $\zeta$  напрямків і ешелонів дії військових частин (підрозділів) (головний та інші напрямки, перший і другий ешелон тощо),  $\eta$  причин виходу з ладу зразків ОВТ (технічні причини, бойові пошкодження).

Для спрощення обчислень обмежимося введеними змінними факторами. В цьому випадку для кожного рівня структури системи відновлення різницю  $Q$  між обсягом ремонтного фонду та виробничими можливостями за номенклатурою ОВТ можна виразити за допомогою рівняння

$$Q_{ik} = \sum_{j=1}^j A_{ij} P_{ij} \beta_{ik} - \sum_{j=1}^j B_{kj} \lambda_{ki} \rho_k \varepsilon_k \quad (1)$$

де:  $A_{ij}$  – кількість  $i$ -ї номенклатури ОВТ в  $j$ -й ланці структури військ на початок операції;

$P_{ij}$  – ймовірний середньодобовий вихід ОВТ з ладу  $i$ -ї номенклатури в  $j$ -й ланці структури військ;

$\beta_{ik}$  – ймовірність наявності в загальному обсязі ремонтного фонду  $i$ -ї номенклатури ОВТ з  $k$ -ю трудомісткістю робіт, тобто  $k$ -го виду ремонту;

$B_{kj}$  – кількість  $k$ -х ланок структури системи відновлення в  $j$ -й ланці структури військ;

$\lambda_{ki}$  – виробничі можливості  $k$ -ї ланки структури системи з відновлення  $i$ -ї номенклатури ОВТ;

$\rho_k$  – коефіцієнт, що враховує рівень кваліфікації спеціалістів-ремонтників  $k$ -ї ланки системи відновлення;

$\varepsilon_k$  – ймовірні середньодобових втрат спеціалістів-ремонтників в  $k$ -й ланці системи відновлення.

Якщо враховуються причини виходу ОВТ з ладу  $\eta$ , положення військових частин (підрозділів), в бойових порядках військ  $\xi$  тощо, тоді від кількості врахованих факторів, які впливають або на формування потоку ремонтного фонду, або на формування виробничих можливостей ремонтних засобів буде залежати кількість сум.

Кількість ОВТ  $i$ -ї номенклатури на початок операції визначається добутком штатної кількості цієї номенклатури ОВТ на коефіцієнт її укомплектованості

$$A_i = A_i^{\text{шт}} K_i^{\text{ук}} \quad (2)$$

Ймовірний вихід ОВТ у ремонт  $P_i$  за добу бойових дій може бути визначений з використанням статистичних даних або результатів прогнозування втрат  $R_i$  ОВТ в різних видах бойових дій, а також коефіцієнта безповоротних втрат  $r_i$  в цих ситуаціях

$$P_i = R_i (1 - r_i) \quad (3)$$

Використовуючи гіпотезу про те, що випадкові величини трудомісткості ремонту – пошкоджених зразків ОВТ незалежні і розподілені за експоненціальним законом, а також знаючи діапазони трудомісткості ремонтних робіт, які виконуються в  $k$ -й ланці системи відновлення, можна визначити ймовірність  $\beta_{ik}$  наявності в загальному обсязі ремонтного фонду  $i$ -ї номенклатури ОВТ з  $k$ -ю трудомісткістю

$$\beta_{ik} = e^{-q\tau_1} - e^{-q\tau_2} \quad (4)$$

де:  $q$  – величина, обернена середній трудомісткості ремонту розглянутої сукупності зразків ОВТ;

$\tau_1, \tau_2$  – відповідно початкове і кінцеве значення трудомісткості в діапазоні розглянутого виду і ступені ремонту.

Таким чином, наявні дані дозволяють визначити перший доданок в рівнянні (1).

Визначення першого співмножника  $B_{kj}$  другого доданка не викликає ускладнень. Коефіцієнт  $\rho_k$  враховує рівень кваліфікації ремонтників в  $k$ -му ремонтному засобі і визначається з урахуванням характеру робіт, які виконуються. За розрахункову одиницю прийнята кваліфікація робітників заводів, які проводять капітальний ремонт ( $\rho_{k=6} = \rho_{k=7} = 1$ ). Найнижчий коефіцієнт ( $\rho_1 = 0,66$ ) має кваліфікацію особового складу ремонтних підрозділів, які виконують поточний ремонт [21].

Ймовірні добові втрати спеціалістів-ремонтників  $\varepsilon_k$  беруться рівними середньодобовим втратам особового складу відповідних типових підрозділів в різних видах бойових дій.

У другому доданку рівняння (1) розрахунок виробничих можливостей  $k$ -ї ланки  $i$ -ї номенклатури ОВТ визначається із співвідношення

$$\lambda_{ki} = \frac{n_k m t_k}{K_{\tau} \bar{\tau}_{ik}} \quad (5)$$

де:  $n_k$  – розрахункова кількість ремонтних бригад в  $k$ -й ланці структури системи відновлення;

$m$  – кількість спеціалістів-ремонтників в бригаді;

$t_k$  – фонд робочого часу  $k$ -ї ланки структури системи відновлення;

$K_{\tau}$  – коефіцієнт зниження середньої трудомісткості ремонту при прийомі ремонтного фонду з нижчої ланки системи відновлення;

$\bar{\tau}_{ik}$  – середня трудомісткість ремонту  $i$ -ї номенклатури ОВТ в  $k$ -й ланці структури системи відновлення.

Для експоненціального розподілу

$$\bar{\tau}_{ik} = \frac{e^{-q\tau_1} (\tau_1 + \frac{1}{q}) - e^{-q\tau_2} (\tau_2 + \frac{1}{q})}{e^{-q\tau_1} - e^{-q\tau_2}} \quad (6)$$



Визначення членів рівняння (1) є необхідною, але недостатньою умовою для його розв'язання. Слід також реалізувати принцип пріоритету за значимістю зразків ОВТ в алгоритмі його розв'язання. З цією метою позначимо обсяг ремонтного фонду кожної номенклатури ОВТ, що підлягає ремонту в конкретній  $k$ -й ланці структури системи відновлення, через  $G$  та складемо систему нерівностей

$$\left. \begin{aligned} \lambda_k - 0,75G_{1,k} - 0,75G_{2,k} - G_{3,k} - 0,5G_{4,k} - 0,9G_{5,k} &\geq 0 \\ \lambda_k - 0,75G_{1,k} - 0,75G_{2,k} - G_{3,k} - 0,5G_{4,k} &\geq 0 \\ \lambda_k - 0,75G_{1,k} - 0,75G_{2,k} - G_{3,k} &\geq 0 \\ \lambda_k - 0,75G_{1,k} - 0,75G_{2,k} &\geq 0 \\ \lambda_k - 0,75G_{1,k} &\geq 0 \end{aligned} \right\} (7)$$

В даній системі цифрові коефіцієнти перед  $G_{ik}$ , є коефіцієнти приведення трудомісткості різної номенклатури ОВТ до основних типових розрахункових зразків ОВТ.

Алгоритмом визначено послідовний розгляд кожної з цих нерівностей в разі невиконання попередньої. Якщо перша нерівність виконана, то вся номенклатура ОВТ, що підлягає відновленню в  $k$ -й ланці, буде в ній відновлена. Якщо ж ця нерівність не виконана, розглядається друга нерівність. У разі її виконання отримуємо кількість відновлених зразків ОВТ  $i = 1-4$ , а решту зразків ОВТ підсумовуємо в масив ремонтного фонду ланки  $k + 1$ . Якщо ж не виконується і друга нерівність, тоді перевіряється третя нерівність і в разі її виконання в ланку  $k + 1$  передаються зразки ОВТ номенклатури  $i = 5$  і  $i = 4$  в кількості, яка не охоплена ланкою  $k$ , тощо.

При передачі в ланку  $k + 1$  зразків ОВТ з ланки  $k$  в залежності від їх кількості автоматично відповідно до алгоритму знижується середня трудомісткість ремонту у вищій ( $k + 1$ ) ланці.

Спрощений алгоритм рішення задачі представлений на рис. 1. Вихідна інформація заноситься у (блок 1). У блоці 2 відбувається визначення суми ОВТ, які залишились в строю разом із відновленими зразками ОВТ. Таким чином, блок 2 видає інформацію про кількість ОВТ на будь-який день операції. Для видачі цієї інформації попередньо визначається потік ремонтного фонду за номенклатурою ОВТ і дням операції (блок 3) і його розподіл по трудомісткості і пріоритету (блок 4).

Далі визначення ремонтного фонду проводиться на двох рівнях: тактичний рівень (блоки 5-10) і оперативний рівень (блоки 11-20). На кожному рівні на підставі вихідної інформації визначаються виробничі можливості кожної ремонтної ланки структури (блоки 7 і 13). У блоках 6 і 12 виділяється ремонтний фонд кожної ланки відповідного рівня. Порівняння результатів, отриманих в блоках 6 і 7, а також 12 і 13, дозволяє визначити кількість зразків ОВТ, які будуть відновлені в цій ланці (блоки 8 і 15) і кількість ремонтного фонду, переданого або у вищестоящу

ланку цього ж рівня (блоки 9 і 16), або на наступний рівень (блок 11). На виході блоку 5 до ремонтного фонду, який передається додаються зразки ОВТ, які заново надійшли і подається знову в блок 6 тактичного рівня. На виході блоку 11 до ремонтного фонду, що надійшов з тактичного рівня, додається ремонтний фонд оперативного рівня і знову подається в блок 12.

Алгоритмом даної моделі передбачено виділення ремонтних бригад для надання допомоги ланкам тактичного рівня. Кількість ремонтного фонду, що припадає на частку цих бригад, визначається у блоці 11. Кількість бригад, необхідних для обробки цього ремонтного фонду, визначається в блоці 14. Відновлені ними зразки ОВТ і бригади які закінчили виконання ремонтних робіт враховуються блоками 17 і 19. Надійність відновлення на кожному рівні ієрархії визначається в блоках 10 і 18. Визначення усієї номенклатури відновлених зразків ОВТ відбувається в блоці 20, дані з якого надходять в блок 2.

Як результат отримуємо відомості про надійність відновлення за номенклатурою зразків ОВТ в кожній ланці структури системи відновлення; про кількість відновлених зразків ОВТ на кожному рівні ієрархії; про кількість неохоплених ремонтно-відновлювальними роботами зразків ОВТ в кожній ланці; про кількість працездатних зразків ОВТ на кожен добу, тощо.

Рішення рівняння (1) передбачає виконання перебору значної кількості змінних величин, що входять в рівняння (2) - (6), а також їх поєднань.

В інтересах вирішення завдання щодо вдосконалення структури системи відновлення, можна варіювати кількістю ремонтних бригад  $n_k$  в рівнянні (5) і їх розподіл по  $k$ -х ланках структури. Це дає можливість проаналізувати вплив такого перерозподілу на надійність відновлення на кожному рівні структури системи.

Введення змінних оперативно-тактичних ситуацій реалізується головним чином через величину в рівнянні (5) – фонд робочого часу, який залежить, як відомо, від глибини завдань, темпу просування військ, швидкості передислокації ремонтних засобів, тощо [24].

Розрахунки даної моделі забезпечують можливість економічної оцінки прийнятих рішень за критерієм ефективність – вартість [25].

Збільшення кількості ремонтних відділень в ланках вищого рівня  $k > 3$  може забезпечити задану ефективність функціонування системи. Однак економічна-ефективність створення відділень, призначених для виконання трудомістких ступенів ремонту, природно різко зростає в порівнянні з вартістю ланок  $k \leq 3$ , а залучати дані ланки доведеться для відновлення ремонтного фонду незначної трудомісткості, кількість якого часто більше, ніж кількість ремонтного фонду  $k > 3$ . Отже, затрати в цьому випадку будуть невиправдано високі.

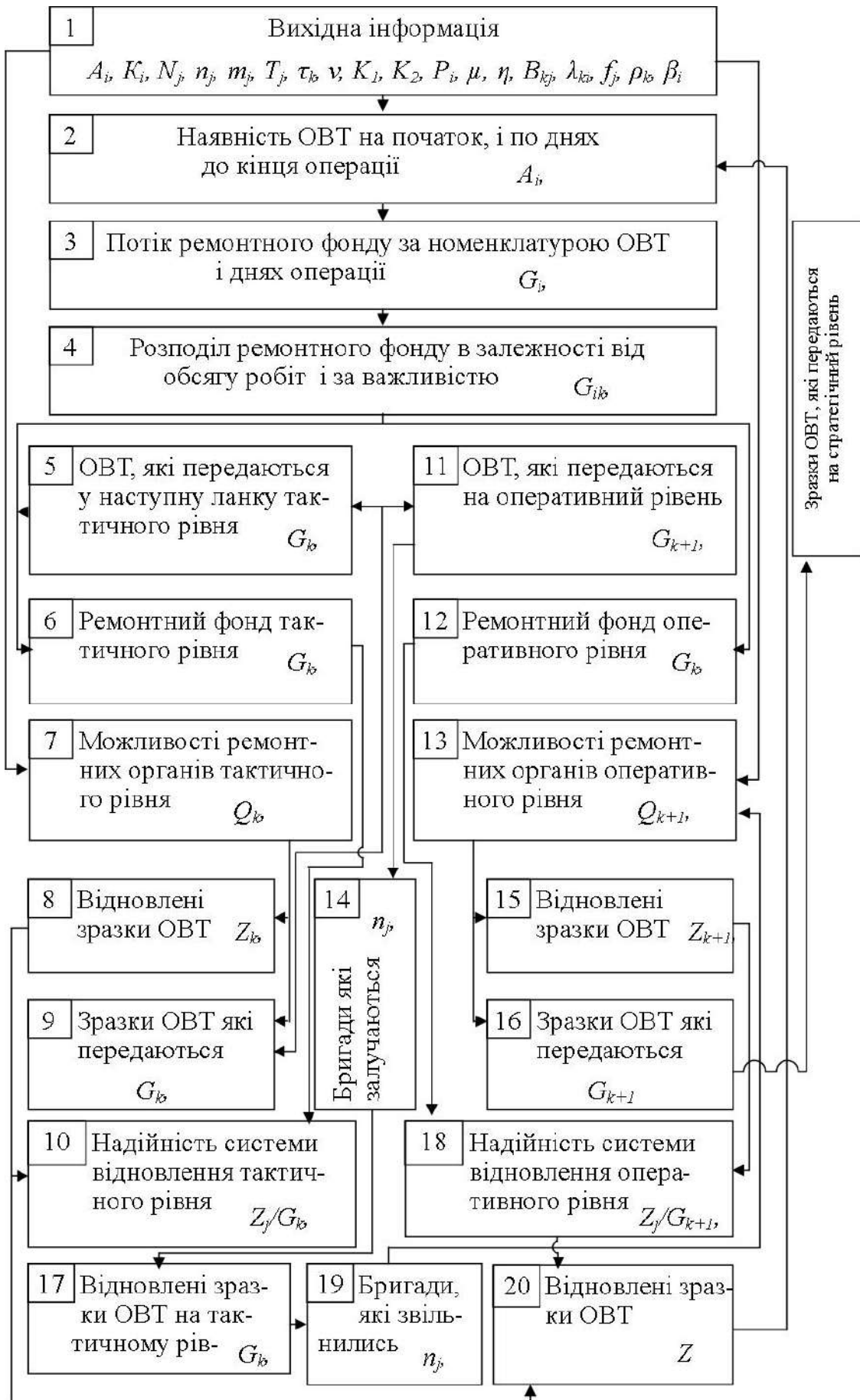


Рис. 1 Структурно-логічна схема функціонування системи відновлення ОВТ

Оптимальною була б така структура системи відновлення, при якій перша нерівність системи (7) завжди б виконувалась для кожного значення  $k$ . Але система, одного разу розроблена, повинна добре працювати в різних ситуаціях, в яких  $G_k$  змінюється в досить широких межах. Тому важливо, з одного боку, найбільш раціонально розподілити кількість ланок структури за рівнями, а з іншого – передбачити можливість маневру цими ланками як по горизонталі, тобто на одному і тому ж рівні ієрархії, так і по вертикалі, тобто між рівнями ієрархії.

Так в загальному вигляді можна представити моделювання процесу відновлення ОВТ. Даний спосіб, як видно, базується на використанні великої кількості вхідних даних, які значно рознесені. Тому результати, отримані даним способом, вимагають перевірки на більш реальних моделях, до яких можна віднести проведення у військах командно-штабних, тактичних та інші види навчань. Ці моделі можуть бути використані для вирішення різних завдань. Одним із показників, які в значній мірі впливають на надійність системи відновлення, слід вважати розподіл втрат ОВТ за обсягом робіт або за їх трудомісткістю. Експоненціальний розподіл яких використовується при розрахунках отримано на основі обробки великої кількості статистичних даних з досвіду ООС (АТО) та навчань. Однак реальні середні значення трудомісткості для різних умов можуть змінюватися в широких межах.

Введення в якості вихідних даних уточнених для конкретної ситуації показників дає можливість отримати більш достовірні результати. Іншими словами, прогнозовані на основі того чи іншого методу показники надійності системи відновлення слід не тільки коригувати на основі реальних результатів, отриманих в ході навчань, а й аналізувати причини розбіжностей, оцінюючи правильність прийнятих вихідних даних.

Важливими показниками, що визначають надійність системи відновлення ОВТ, є темп бойових дій і глибина завдання, які виконуються військами. У викладених методах прогнозування надійності системи відновлення ОВТ ці показники певним чином враховуються. Однак реальна обстановка може внести суттєві корективи у кількісні вираження цих показників. Збільшення плеча евакуації ОВТ може різко ускладнити роботу евакуаційних засобів, затрудняти виявлення, зосередження і відновлення ремонтного фонду тощо.

Отже, розглянута модель процесу функціонування системи відновлення ОВТ надає великі можливості для накопичення статистичних даних за показниками надійності системи відновлення з різними характеристиками, що

діють в широкому діапазоні зміни ситуацій. Як було зазначено, цей статистичний матеріал дозволить, з одного боку, визначити необхідну ефективність функціонування системи, а з іншого – намітити шляхи її вдосконалення, які і включаються в тактико-технічне завдання [26].

Кінцевим результатом вдосконалення, мають бути виражені показники спрямовані на поліпшення роботи системи, які повинні оцінюватися тільки в комплексі з тими витратами, які планується затратити для досягнення запланованого результату. Така оцінка повинна носити не характер констатації факту, а характер прогнозу. Будь-які пропозиції щодо розвитку системи повинні базуватися на реально можливих витратах засобів і на той ефект, який очікується від їх реалізації. Розглянута модель процесу функціонування системи відновлення ОВТ дозволяє вирішити також завдання щодо оцінювання економічної ефективності рекомендованих тактико-технічних завдань заходів. Відповідно включені в тактико-технічне завдання обмеження з матеріальних ресурсів можуть бути в повній мірі обґрунтовані.

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

Досвід застосування і вдосконалення системи відновлення в операції ООС (АТО) показує, що основними напрямками вдосконалення в більшості випадків були зміни структури системи і оснащення її ланок більш ефективними технічними засобами. Цей висновок підтверджується і численними дослідженнями на сучасному етапі, виконаними із застосуванням викладеної методики. Раціональний розподіл ремонтних бригад по ланках структури системи при незначному збільшенні їх чисельності дає різке підвищення функціональної ефективності. Оснащення ремонтно-відновлювальних військових частин (підрозділів) комплексами засобів ремонту, евакуації і транспортування, розробленими відповідно до обсягу ремонтних робіт, які виконуються в кожній ланці, також призводить до істотного зростання надійності системи відновлення ОВТ при підвищенні його економічної ефективності.

Удосконалення структури системи відновлення реалізується головним чином шляхом створення нових ремонтних ланок, організаційно-штатна структура яких розробляється на основі аналізу всієї системи як цілісного організму. Тому в подальшому необхідно розглянути питання проектування ремонтно-відновлювальних військових частин (підрозділів) та оснащення їх рухомими засобами ремонту, технічного обслуговування, евакуації, які задовольнятимуть положенням системного підходу.

Досвід застосування і вдосконалення системи відновлення в операції ООС (АТО) показує, що основними напрямками вдосконалення в більшості випадків були зміни структури системи і оснащення її ланок більш ефективними технічними засобами. Цей висновок підтверджується і численними дослідженнями на сучасному етапі, виконаними із застосуванням викладеної методики. Раціональний розподіл ремонтних бригад по ланках структури системи при незначному збільшенні їх чисельності дає різке підвищення функціональної ефективності. Оснащення ремонтно-відновлювальних військових частин (підрозділів) комплексами засобів ремонту, евакуації і транспортування, розробленими відповідно до обсягу ремонтних робіт, які

виконуються в кожній ланці, також призводить до істотного зростання надійності системи відновлення ОВТ при підвищенні його економічної ефективності.

Удосконалення структури системи відновлення реалізується головним чином шляхом створення нових ремонтних ланок, організаційно-штатна структура яких розробляється на основі аналізу всієї системи як цілісного організму. Тому в подальшому необхідно розглянути питання проектування ремонтно-відновлювальних військових частин (підрозділів) та оснащення їх рухомими засобами ремонту, технічного обслуговування, евакуації, які задовольнятимуть положенням системного підходу.

### Література

- Новиков Н. Н.** Российские Вооружённые силы в чеченском конфликте: анализ, итоги, выводы / Новиков Н. Н. – М.: ОВА ВС РФ, 1996. – 163 с. **2. Єремєєв І. В.** Уроки “локальних” війн ХХ-го століття / І. В. Єремєєв // Військо України. – 2001. – № 3. С. 30-31. **3. Сисоев О. О.** Проблеми, тенденції і перспективи розвитку системи технічного забезпечення військ (сил) у війнах і збройних конфліктах кінця ХХ – початку ХХІ століття / Сисоев О. О. – К.: НАОУ, 2004. – 104 с. **4. Сенічкин І. Е.** Танко-технічне обслуговування танкових (мотострелкових) подразделений в боевых условиях / І. Е. Сенічкин, В. А. Гречка, А. В. Тарасов. – М.: Воениздат, 1989. – 220 с. **5.** Восстановление вооружения: учебное пособие: в 2 ч. / В.Р.Стефанович [и др.]. – Минск: БНТУ, 2013–Ч.1. – 169 с. **6. Шишанов М.О.** Обґрунтування методу моделювання процесу функціонування системи відновлення озброєння та військової техніки угруповання військ / Шишанов М.О., Гуляєв А.В., Шевцов М.М. // Озброєння та військова техніка, 2017, №1(13), с. 75-77 **7. Запара Д.М.** Впровадження процедури прогнозування пошкоджень ОВТ від впливу осколкової дії засобів ураження в перспективну АСУ матеріально-технічним забезпеченням / Запара Д.М., Бровко М.Б., Старцев В.В., Кушпета Р.Ю., Дудко М.В. // Збірник наукових праць Харківського національного університету Повітряних Сил, 2018, №4(58) с. 50-56. **8. Куровська Т.Ю.** Метод оцінки надійності підприємств-виробників ОВТ / Куровська Т.Ю., Троцько Л.Г., Троцько Б.В. // Вісник Національного університету оборони України, 2015, №2(45), с. 317-320. **9. Люлін Д.О.** Удосконалення системи технічного забезпечення засобів зв'язку і автоматизації Збройних Сил України / Люлін Д.О. Михайлов О.В. Кайдаш І.Н. // Збірник наукових праць ВІПІ НТУУ“КПІ”, 2011, вип. 2, с. 68-75. **10. Павловський О.В.** Прогнозування величини втрат озброєння та військової техніки під час операцій (бойових дій) / Павловський О.В. // Системи озброєння і військова техніка, 2015, № 4(44), с. 116-118. **11. Радзівілов Г.Д.** Відновлення військової техніки зв'язку при диференційованому підході до кількісної оцінки ймовірності її пошкодження / Радзівілов Г.Д. Романенко В.П. // Збірник наукових праць ВІПІ НТУУ“КПІ”, 2011, вип. 2, с. 94-100. **12. Наумов А.В.** Совершенствование технологического процесса восстановления машин путем применения новых образцов подвижных средств технического обслуживания и ремонта / Наумов А.В., Тетенькин А.С., Перевертов А.А., Татарнов В.В. // [Электронный ресурс]: [http://www.science-bsea.bgita.ru/2012/mashin\\_2012\\_16/naumov\\_sov.ht](http://www.science-bsea.bgita.ru/2012/mashin_2012_16/naumov_sov.ht). **13. Пьянков А.А.** Математическая модель процесса восстановления вооружения и военной техники в ходе боевых действий тактического воинского формирования / Пьянков А.А. // Вооружение и экономика. 2014. № 2 (27), с. 53-64. **14. Гришина Н.С.** Оптимізація системи технічного забезпечення військ зв'язку ЗС України за досвідом проведення бойових дій / Гришина Н.С., Білий О.А., Побережець Т.В., Новак А.О., Ткач В.О. // Молодий вчений. 2018. № 12 (64), с. 563-565. **15. Каревик А.А.** Оценка эффективности применения новой метрологической техники для метрологического обеспечения радиотехнических систем / Каревик А.А., Котова М.А., Дзябенко А.Н. URL:[http://www.metrology.kharkov.ua/fileadmin/user\\_upload/data\\_gc/conference/M2012/pages/247.pdf](http://www.metrology.kharkov.ua/fileadmin/user_upload/data_gc/conference/M2012/pages/247.pdf). **16. Дюбанов О.О.** Системний підхід до врегулювання проблемних процесів автотехнічного забезпечення Сухопутних військ Збройних Сил України. / Дюбанов О.О. // [Електронний ресурс]: <http://znp-cvds.nuou.org.ua/article/download/124422/118948>. **17. Пальчук М. М.** Досвід бойового застосування військ, зброї і військової техніки в локальних війнах і збройних конфліктах / М. М. Пальчук, М. М. Лобко. – К.: НАОУ, 2001. – 119 с. **18. Королев Г. Е.** Исследование боевых повреждений образцов отечественных БТТ / Г. Е. Королев, Р. З. Мамлеев. – М.: Вестник БТТ, 1991. – № 8. – С. 36 – 39. **19. Барабаш Ю. Л.** Основи теорії оцінювання ефективності складних систем (Методологія наукових досліджень) / Барабаш Ю. Л. – К.: НАОУ, 1999. – 40 с. **20. Вентцель Е. С.** Прикладные задачи теории вероятностей / Е. С. Вентцель, Л. А. Овчаров. – М.: Радио и связь, 1983. – 416 с. **21. Борохвостов В. К.** Теоретические основы ремонта БТВТ / Борохвостов В. К. – К.: КВТИУ, 1992.– 84 с. **22. Соболев Е. Г.** Требования к восстанавливаемости ВГМ / Е. Г. Соболев // Вестник БТТ. – 1990. – № 3. – С. 3 –7. **23. Вентцель Е. С.** Теория

вероятностей / Вентцель Е. С. – М.: Физматлит, 1962. – 564 с. **24. Круглов В. В.** О тенденциях развития современной вооруженной борьбы / В. В. Круглов // Военная мысль. – 1998. – № 2. – С. 39 – 44. **25. V. Dachkovskiy** Methodical approach to evaluation of economic efficiency of repairing the weapons and military equipment / V. Dachkovskiy, O. Sampir Y. Horbachova //

Journal of Scientific Papers VUZF review. – 2020. – Vol. 5, No 1, p. 22-30. **26. Дачковський В.О.** Методика обґрунтування тактико-технічних вимог до рухомих засобів ремонту озброєння та військової техніки / В.О. Дачковський // Social development & Security. – 2019. – №9(6), 86 – 101.

## МЕТОДИКА ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ВОССТАНОВЛЕНИЯ ОРУЖИЯ И ВОЕННОЙ ТЕХНИКИ

*Владимир Александрович Дачковский (кандидат технических наук)  
Владимир Иванович Коцюруба (доктор технических наук, доцент)*

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

*Анализ применения подразделений и воинских частей в локальных войнах и вооруженных конфликтах позволяет утверждать, что одним из основных показателей, влияющих на успех в выполнении задач является наличие в воинских частях (подразделениях) трудоспособных образцов вооружения и военной техники. При этом, одним из основных источников поступления трудоспособных образцов вооружения и военной техники в воинские части (подразделения) в ходе ведения боевых действий является возвращение их из стационарных и подвижных ремонтно-восстановительных воинских частей (подразделений) после выполнения мероприятий по их восстановлению.*

*Поэтому для оценки эффективности восстановления вооружения и военной техники предложена методика оценки эффективности функционирования системы восстановления. Суть, которой заключается в получении сведения о надежности восстановления вооружения и военной техники по номенклатуре в каждом звене структуры системы восстановления, количества восстановленных образцов вооружения и военной техники на каждом уровне иерархии, количества неохваченных ремонтно-восстановительными работами образцов вооружения и военной техники в каждом звене, количества трудоспособных образцов вооружения и военной техники на каждые сутки операции (боевых действий). Методика позволяет варьировать количеством ремонтных бригад и их распределением по звеньям структуры. Введение переменных оперативно-тактических ситуаций реализуется главным образом через фонд рабочего времени.*

***Ключевые слова:** вооружение и военная техника; восстановление; моделирование; производственные возможности; ремонтно-восстановительные подразделения.*

## METHOD OF EVALUATION OF EFFICIENCY OF FUNCTIONING OF ARMS AND MILITARY ENGINEERING SYSTEM

*Volodymyr Dachkovskiy (Candidate of Technical Sciences)  
Volodymyr Kotsiuruba (Doctor of Technical Sciences, Associate Professor)*

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

*The analysis of the use of units and military units in local wars and armed conflicts suggests that one of the main indicators that influence the success of the task is the availability of military units (units) of working models of weapons and military equipment. At the same time, one of the main sources of receipt of able-bodied samples of weapons and military equipment in the military units (units) in the course of hostilities is the return of them from stationary and mobile repair and restoration military units (units) after the completion of measures for their restoration.*

*Therefore, a technique for assessing the effectiveness of a recovery system is proposed to evaluate the effectiveness of weapons and military equipment recovery. The essence of which is to obtain information about the reliability of the renewal of weapons and military equipment by nomenclature in each element of the structure of the system of reconstruction, the number of recovered weapons and military equipment at each level of the hierarchy, the number of non-covered weapons repair and restoration works, the number of weapons and equipment able-bodied samples of weapons and military equipment for each day of the operation (combat). The technique allows to vary the number of repair crews and their distribution in the links of the structure. Introduction of variable operational and tactical situations is realized mainly through the working time fund.*

***Keywords:** weapons and military equipment; restoration, modeling; production capabilities; repair and restoration units.*

## References

- 1. Novikov N.N.** The Russian Armed Forces in the Chechen Conflict: Analysis, Results, Conclusions / Novikov N.N. – M.: OVA RF Armed Forces, 1996. – 163 p. **2. Erimeev I.V.** Lessons of “local” wines of the XX-th table / I.V. Erimeev // Viysko Ukraine. – 2001. – No. 3. – p. 30-31. **3. Sisoiev O.O.** Problems, Trends and Prospects for Developing a System of Technical Care Vysk (Strength) in Viynakh and Zbroiny Conflicts Kintsya XX – Cob XXI stoltyta / Sisoiev O. O. – K.: NAOU, 2004. – 104 p. **4. Senichkin I.E.** Tank-technical support of tank (motorized rifle) units in combat conditions / I. E. Senichkin, V.A. Grechka, A.V. Tarasov. – M.: Military Publishing, 1989. – 220 p. **5. Arms restoration: a training manual: at 2 o'clock / VR Stefanovich [et al.].** – Minsk: BNTU, 2013– Part 1. – 169 p. **6. Shishanov M.O.** Exploring the method of modeling the process of the function of the system and the updated technology and technical technology / Shishanov M.O., Gulyaev A.V., Shevtsov M.M. // Ozbroyennya viiskova tekhnika, 2017, No. 1 (13), p. 75-77 **7. Zapara D.M.** In the process of forecasting the prognosis of the shipment of OVT, I'm pouring shrapnel and other ideas into perspective ACS with material and technical care / Zapara D.M., Brovko M.B., Startsev V.V., Kushpet R.Yu., Dudko M.V. // Zbirnik naukovskih prats of the Kharkiv National University of the Powers, 2018, No. 4 (58) p. 50-56.
- 8. Kurovska, T.Yu.** The method of estimation of overpriority-virobnik OVT / Kurovska T.Yu., Trotsko L.G., Trotsko B.V. // News of the National University of Defense of Ukraine, 2015, No. 2 (45), p. 317-320.
- 9. Lyulin D.O.** More comfortable system of technical care for the call and automation of the Ukrainian Forces of Ukraine / Lyulin D.O., Mikhailov O.V., Kaydash I.N. // Zbirnik naukovykh praz VITI NTUU “KPI”, 2011, VIP. 2, p. 68-75. **10. Pavlovsky O.V.** Prediction of the value of the costs of the production and operation technology (operational hours) / Pavlovsky O.V. // Systems of engineering and technology, 2015, No. 4 (44), p. 116-118.
- 11. Radzivilov G.D.** Vidnovlennya viyskovo technology zv'yazku at differentiation to the approach to kilkisno otsinki ymovirnosti її poshkozheniya / Radzivilov G.D., Romanenko V.P. // Zbirnik naukovykh praz VITI NTUU “KPI”, 2011, VIP. 2, p. 94-100. **12. Naumov A.V.** Improving the technological process of restoration of machines through the use of new samples of mobile tools for maintenance and repair / Naumov A.V., Tetenkin A.S., Perevertov A.A., Tatarov V.V. // [Electronic resource]: Access mode: [http://www.science-bea.bgita.ru/2012/mashin\\_2012\\_16/naumov\\_sov.htm](http://www.science-bea.bgita.ru/2012/mashin_2012_16/naumov_sov.htm). **13. Pyankov A.A.** A mathematical model of the process of restoring weapons and military equipment during the operations of a tactical military formation / Pyankov A.A. // Armament and economics. 2014. No. 2 (27), p. 53-64.
- 14. Grishina N.S.** Optimization of the system of technical support for the sound of the AP of Ukraine for the conduct of combat engagements / Grishina N.S., Bilyi O.A., Poberezhets T.V., Novak A.O., Tkach V.O. // Young introductory. 2018.No 12 (64), p. 563-565. **15. Karevik A.A.** Evaluation of the effectiveness of the use of new metrological equipment for metrological support of radio engineering systems / Karevik A.A., Kotova M.A., Dzyabenko A.N. // [Electronic resource]: Access mode: [http://www.metrology.kharkov.ua/fileadmin/user\\_upload/data\\_gc/conference/M2012/pages/247.pdf](http://www.metrology.kharkov.ua/fileadmin/user_upload/data_gc/conference/M2012/pages/247.pdf).
- 16. Dyubanov O.O.** The systematic piddid until the problematic processes of the automotive technical care of the Land forces of Ukraine. / Dyubanov O.O. // [Electronic resource]: Access mode: <http://znp-cvds.nuou.org.ua/article/download/124422/118948>.
- 17. Palchuk M.M.** Dosvid combat stagnation of the battlefield, local technology and local technology in local conflicts / M.M. Palchik, M.M. Lobko. – K.: NAOU, 2001. – 119 p. **18. Korolev G.E.** Research of combat damage to samples of domestic BTT / G.E. Korolev, R.Z. Mamleev. – M.: Vestnik BTT, 1991. – No. 8. – p. 36-39. **19. Barabash Yu.L.** Fundamentals of the theory of efficiency of folding systems (Methodology of scientific research) / Barabash Yu.L. – K.: NAOU, 1999. – 40 p. **20. Ventzel E.S.** Applied problems of probability theory / E. S. Ventzel, L.A. Ovcharov – M.: Radio and communications, 1983. – 416 p.
- 21. Borokhvostov V.K.** Theoretical foundations of repair of BTVT / Borokhvostov V.K. – K.: KVTIU, 1992. – 84 p. **22. Sobolev E.G.** Requirements for the recoverability of the HMW / E.G. Sobolev // Bulletin of BTT. – 1990. – No. 3. – p. 3 –7. **23. Wentzel E.S.** Probability Theory / Wentzel E.S. – M.: Fizmatlit, 1962. – 564 p. **24. Kruglov V.V.** On the development trends of modern warfare / V.V. Kruglov // Military Mysl. – 1998. – No. 2. – p. 39-44.
- 25. V. Dachkovskiyi** Methodical approach to evaluation of economic efficiency of repairing the weapons and military equipment / V. Dachkovskiyi, O. Sampir Y. Horbachova // Journal of Scientific Papers VUZF review. – 2020. – Vol. 5, No 1, p. 22-30. **26. Dachkovskiyi V.O.** Metodyka obgruntuvannia taktyko-tekhnichnykh vymoh do rukhomykh zasobiv remontu ozbroiennia ta viiskovoi tekhniki / V.O. Dachkovskiyi // Social development & Security. – 2019. – №9(6), 86 – 101.

*Олександр Михайлович Доска* (кандидат технічних наук)<sup>1</sup>

*Павло Вікторович Опенько* (кандидат технічних наук)<sup>2</sup>

*Анатолій Сергійович Дудуш* (кандидат технічних наук)<sup>1</sup>

*Максим Володимирович Сургай*<sup>1</sup>

<sup>1</sup>Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

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

## ВИЗНАЧЕННЯ ПОКАЗНИКА ЕФЕКТИВНОСТІ ВІДНОВЛЕННЯ ЗЕНІТНОГО РАКЕТНОГО ОЗБРОЄННЯ З УРАХУВАННЯМ РЕСУРСНИХ ОБМЕЖЕНЬ

Обґрунтовується підхід щодо визначення ймовірності своєчасного проведення відновлювального ремонту з урахуванням обмежених запасів запасних частин, матеріалів, інструментів і приладдя (ЗІП). Знайдено аналітичне співвідношення для розрахунку ймовірності своєчасного проведення відновлювального ремонту зразків зенітного ракетного озброєння (ЗРО). Запропоноване співвідношення дозволяє врахувати дані про номенклатуру та кількість складових частин, що визначають працездатність зразка озброєння, кількість запасних частин у відновлювальних та експлуатаційних комплектах ЗІП, номенклатуру та кількість працездатних складових частин у зразках озброєння, які підлягають списанню і розукомплектуванню, ймовірності бойових пошкоджень складових частин та час виконання відновлювального ремонту.

**Ключові слова:** зенітне ракетне озброєння, відновлювальний ремонт, ресурсні обмеження, показник ефективності.

### Вступ

**Постановка проблеми.** Існуючі методи [1-4] визначення показників ефективності відновлення ЗРО, яке отримало бойові пошкодження, ґрунтуються на припущенні того, що ремонтний орган забезпечений достатньою кількістю комплектів ЗІП, а процес відновлення зразка ЗРО носить масовий характер та характеризується потоком відмов та потоком відновлень.

Разом з тим, проведений аналіз свідчить, що на сьогоdnішній час існує дефіцит запасів запасних частин за окремою номенклатурою [5]. Підприємства оборонно-промислового комплексу спроможні частково задовольнити потреби Збройних Сил України в елементній компонентній базі зразків ЗРО. Питання імпортозаміщення гостродефіцитних складових частин вирішено не в повній мірі.

Крім того, виникнення потреби проведення відновлювального ремонту є випадковою подією, яка визначається ймовірністю бойового пошкодження складових частин зразка ЗРО [6, 7]. Відновлення зразка ЗРО проводиться агрегатним методом, шляхом заміни пошкоджених складових частин на працездатні зі складу комплектів ЗІП. При цьому кількість відновлювальних ремонтів складової частини обмежена. Тому припущення про багаторазове відновлення працездатності складової частини, або багаторазове проведення відновлювального ремонту, не відповідає реальному процесу відновлювального ремонту зразка ЗРО.

Таким чином, оцінювання показників ефективності відновлення ЗРО з урахування

обмежених запасів ЗІП є актуальною задачею.

**Аналіз останніх досліджень і публікацій.** В [1] у якості основного показника, який характеризує ефективність проведення ремонту, обрано середній час відновлення апаратури, який в свою чергу поділено на три складові: час активного ремонту, адміністративний час та час забезпечення ремонту. Зазначено, що закон розподілу активного часу ремонту в основному визначається методом відшукування несправностей та конструктивними особливостями апаратури. У якості закону розподілу часу активного ремонту запропоновано використовувати експоненціальний закон.

У [2] розглянутий підхід до моделювання системи відновлення озброєння та військової техніки (ОВТ) на основі моделей масового обслуговування, що дозволяє оцінити можливості сил та засобів військового та заводського ремонтів ОВТ. При визначенні цих можливостей використовуються методи, що враховують лише експлуатаційні відмови. Механізми виникнення бойових пошкоджень відрізняються від механізмів виникнення експлуатаційних відмов. Тому підходи до визначення показників ефективності відновлення зразків ЗРО повинні враховувати особливості процесів отримання і результати бойових пошкоджень.

У [3] розглянуто загальний підхід до створення математичної моделі процесу відновлення ОВТ, яка базується на математичній моделі технічного забезпечення, побудованій з використанням математичного методу “динаміки середніх”.

Особливістю запропонованої моделі є те, що в умовах бойових дій потік пошкоджень зразків ОВТ не є стаціонарним, а його функція інтенсивності представляє собою імпульсну функцію.

У [4] зазначено, що в якості показників, які характеризують можливості відновлення ЗРО, пошкодженого під час ведення бойових дій, використовуються кількісні показники – середній час відновлення зразка ЗРО та ймовірність відновлення зразка ЗРО за заданий час. Процес відновлення зразків ЗРО в [4] розглядається як масовий процес, тому для його описання використовують математичний апарат теорії систем масового обслуговування. Обслуговуючою системою є система ремонту, яка здійснює ремонт пошкоджених складових частин зразка ЗРО шляхом їх заміни на справні зі складу комплекту ЗІП. При цьому обслуговується потік заявок, який полягає в багаторазовому використанні запасних частин зі складу комплектів ЗІП для відновлення працездатності зразків озброєння, що не в достатній мірі відповідає реальним умовам відновлювального ремонту зразків ЗРО.

У [8,9] обґрунтовано необхідність забезпечення ремонту бойових засобів зенітного ракетного комплексу відновлювальними комплектами ЗІП (ЗІП-В). При цьому, на відміну від експлуатаційних комплектів ЗІП, ЗІП-В повинні забезпечувати усунення бойових пошкоджень, викликаних дією засобів протидії противника, з відновленням працездатності та ресурсу в обсязі, який забезпечує експлуатацію зразка ЗРО протягом встановленого терміну, або до чергового бойового пошкодження.

У [9] запропоновано метод розрахунку показника достатності комплекту ЗІП-В, який на відміну від відомих, ґрунтується на разових заявках на запасну частину та разовому їх відновленні, що дозволяє позбутися припущень про надходження інтенсивності потоку заявок на запасні частини та інтенсивності відновлення.

Питання визначення показників ефективності відновлення ЗРО у [8, 9] не розглядалося.

У [6,7] приведені співвідношення для визначення витрат часу на поточний ремонт радіоелектронних систем для експоненціального розподілу випадкової величини часу проведення ремонтних робіт. При цьому питання обмеженості запасів ЗІП в [6, 7] не розглядалося.

Таким чином, існуючі підходи [1-9] мають значні методичні погрішності, обумовлені невідповідністю математичних моделей процесу відновлення зразків ЗРО, не враховують ресурсні обмеження та не можуть в повній мірі використовуватися для визначення показників ефективності відновлення ЗРО.

**Метою статті** є розробка методу розрахунку показника ефективності відновлення ЗРО з урахуванням ресурсних обмежень.

### Виклад основного матеріалу дослідження

Відновлення працездатності пошкодженого зразка ЗРО потребує певного часу, значення якого може перевищувати наявний термін. Разом з тим, в

умовах бойових дій, існує необхідність виконання поставлених бойових завдань підрозділами та частинами зенітних ракетних військ, що в свою чергу потребує працездатного озброєння.

Можливим шляхом забезпечення проведення відновлення зразка ЗРО у встановлені терміни є проведення відповідного відновлювального ремонту в обсязі, який забезпечує функціонування зразка ЗРО з мінімально необхідною для виконання бойових завдань структурою.

Розглянемо зразок ЗРО, структура якого відома та може бути представлена вектором

$$A = \{a_\ell\}, \quad \ell = \overline{1, L},$$

де:  $a_\ell$  – кількість складових частин  $\ell$ -го типу;

$L$  – кількість типів складових частин зразка ЗРО.

Рівень розукрупнення зразка ЗРО встановлюється з розрахунку на агрегатний метод ремонту із врахуванням стійкості апаратури зразка до вогневого впливу повітряного противника і може включати функціональні вузли, блоки, шафи, контейнери і т.п.

Припустимо, що складові частини зразка ЗРО отримують бойові пошкодження незалежно одна від одної. Кожна  $j$ -та складова частина  $\ell$ -го типу, що входить до складу зразка ЗРО, може бути пошкоджена з імовірністю  $P_j^\ell$ , або не пошкоджена з імовірністю  $q_j^\ell = 1 - P_j^\ell$ ,  $j = \overline{1, a_\ell}$ .

З метою усунення бойових пошкоджень і відновлення працездатності зразка ЗРО проводиться його відновлювальний ремонт, який полягає в усуненні бойових пошкоджень та відновленні працездатності зразка шляхом заміни пошкоджених складових частин на працездатні зі складу експлуатаційних та відновлювальних комплектів ЗІП. У випадку відсутності необхідних складових частини в комплектах ЗІП, у якості запасних частин можуть використовуватися працездатні складові частини списаних зразків озброєння, які підлягають розукрупненню.

Крім того, при відновлювальному ремонті поновлюється цілісність обшивки кабін, каркасів стійок, шаф та блоків, усуваються обриви в кабельній мережі, тощо. Після ремонту проводиться налаштування і регулювання апаратури зразка ЗРО.

Можливості відновлення зразка ЗРО для конкретного ремонтного органу (підрозділу) визначаються його здатністю до відновлення бойових пошкоджень заданого типу за напрямками відновлення.

Напрямки відновлення в ремонтному органі (підрозділі) пов'язані з конструктивно-технологічними особливостями зразка ЗРО, які обумовлюють необхідність застосування відповідного обладнання та устаткування для усунення бойових пошкоджень.

До таких напрямків відновлення зразка ЗРО можна віднести:

- відновлення антенно-фідерних пристроїв;
- відновлення високочастотної апаратури;
- відновлення низькочастотної апаратури;
- відновлення засобів рухомості і т.п.



Для кожного напрямку відновлення в ремонтному органі (підрозділі) організується ремонтна ділянка  $\zeta$ , яка в свою чергу складається з  $\eta$  робочих місць. На кожному робочому місці може проводитися  $\xi$  ремонтних операцій.

Середній час виконання  $\xi$ -ї ремонтної операції  $\bar{t}_{p\xi}$  може бути визначено за статистичними даними. Якщо за статистичними даними можливо визначити тільки мінімальний  $\bar{t}_{p\xi \min}$  та максимальний  $\bar{t}_{p\xi \max}$  час виконання  $\xi$ -ї ремонтної операції, то  $\bar{t}_{p\xi}$  може визначатися за співвідношенням

$$\bar{t}_{p\xi} = \frac{3t_{p\xi \min} + 2t_{p\xi \max}}{5}; \quad (1)$$

$$\sigma(\bar{t}_{p\xi}) = \sqrt{\frac{t_{p\xi \max} - t_{p\xi \min}}{5}}, \quad (2)$$

де:  $\sigma(\bar{t}_{p\xi})$  – середньоквадратична помилка у визначенні часу  $\bar{t}_{p\xi}$ .

З метою скорочення термінів проведення відновлювального ремонту, в ремонтному органі (підрозділі) ремонтні операції намагаються виконувати на паралельних ділянках та робочих місцях. Для цього складається схема (модель) технологічного процесу відновлювального ремонту та визначається найкоротший шлях виконання робіт. Проведення відновлення за найкоротшим шляхом схеми технологічного процесу дозволяє забезпечити не тільки мінімальні витрати часу, а й залучити до проведення ремонту мінімальну кількість спеціалістів [1].

Тоді задача розрахунку показника ефективності відновлення ЗРО полягає у визначенні ймовірності відновлення зразка ЗРО за заданий час  $t_{вр}$  за умови наявності даних про:

кількість та номенклатуру складових частин зразка ЗРО різного рівня розукрупнення  $a_\ell, L$ ;

ймовірності бойових пошкоджень складових частин зразка ЗРО  $P_{\ell,j}$ ;

ймовірності бойових пошкоджень запасних частин у комплектах ЗІП  $P_{\ell,j}^{зип}, P_{\ell,j}^{зип-в}, P_{\ell,j}^p$ ;

кількість ремонтних ділянок в найкоротшому шляху схеми технологічного процесу відновлювального ремонту  $\Theta$ ;

кількість робочих місць на кожній ділянці в найкоротшому шляху схеми технологічного процесу відновлювального ремонту  $\Psi$ ;

кількість ремонтних операцій на кожному робочому місці ремонтної ділянки найкоротшого шляху схеми технологічного процесу відновлювального ремонту  $\Omega$ ;

середні значення часу виконання  $\xi$ -ї ремонтної операції на  $\eta$ -му робочому місці  $\zeta$ -ї ремонтної ділянки  $\bar{t}_{p\eta\xi}, \zeta \in \Theta, \eta \in \Psi, \xi \in \Omega$ .

Проведення відновлювального ремонту за заданий час не є гарантованим. Ймовірність такої події може бути знайдена як ймовірність складної

події

$$P(X, t_{вр}) = P_{зип}(X)P(t_{вр}/X), \quad (3)$$

де:  $P_{зип}(X)$  – ймовірність того, що запасних частин в комплектах ЗІП буде достатньо для проведення відновлювального ремонту;

$P(t_{вр}/X)$  – умовна ймовірність проведення відновлювального ремонту за час, який не перевищує задане значення  $t_{вр}$  за умови, що запасних частин в комплектах ЗІП буде достатньо.

Умовна ймовірність  $P(t_{вр}/X)$  залежить від часу  $t_{вр}$ , необхідного для проведення відновлювального ремонту, і може бути оцінена відомим співвідношенням [4]

$$P(t_{вр}/X) = \Phi\left[\frac{t_{вр} - t_{вроч}}{\sigma(t_{вроч})}\right], \quad (4)$$

де:  $\Phi[\ ]$  – таблиця функція нормального розподілу випадкової величини;

$t_{вроч}$  – очікуваний час виконання відновлювального ремонту

$$t_{вроч} = \sum_{\zeta=1}^{\Theta} \sum_{\eta=1}^{\Psi} \sum_{\xi=1}^{\Omega} \bar{t}_{p\eta\xi}; \quad (5)$$

$\sigma(t_{вроч})$  – середньоквадратична помилка у визначенні часу виконання відновлювального ремонту

$$\sigma(t_{вроч}) = \sqrt{\sum_{\zeta=1}^{\Theta} \sum_{\eta=1}^{\Psi} \sum_{\xi=1}^{\Omega} \sigma(\bar{t}_{p\eta\xi})^2}. \quad (6)$$

Для визначення  $P_{зип}(X)$  розглянемо випадок, коли до складу зразка ЗРО та комплектів ЗІП входять складові та запасні частини однієї номенклатури ( $\ell$ -го типу), а вже потім отримаємо розрахункове співвідношення з урахуванням того, що зразки ЗРО та комплекти ЗІП складаються зі складових та запасних частин різної номенклатури  $\ell = \overline{1, L}$ .

У відповідності до прийнятих припущень, представимо структуру складових частин  $\ell$ -го типу зразків ЗРО та відповідних запасних частин до них у вигляді структурної схеми надійності системи з ковзним резервуванням (рис. 1).

Розглянемо подію  $V_\ell$  яка полягає в тому, що система рис. 1 втратила свою працездатність з причин бойових пошкоджень складових та запасних частин  $\ell$ -го типу.

Згідно схеми рис. 1 подія  $V_\ell$  наступить тоді, коли резервні елементи не в змозі забезпечити потребу в заміні основних складових частин  $\ell$ -го типу, тобто – коли запасів запасних частин недостатньо.

При нанесенні повітряного удару противником по позиціям угруповання військ можуть бути пошкоджені як бойові, так і технічні засоби (в тому числі і машини ЗІП), тому виникнення події  $V_\ell$  пов'язано з виникненням різних комбінацій бойових пошкоджень як складових, так і запасних частин засобів ЗРО.

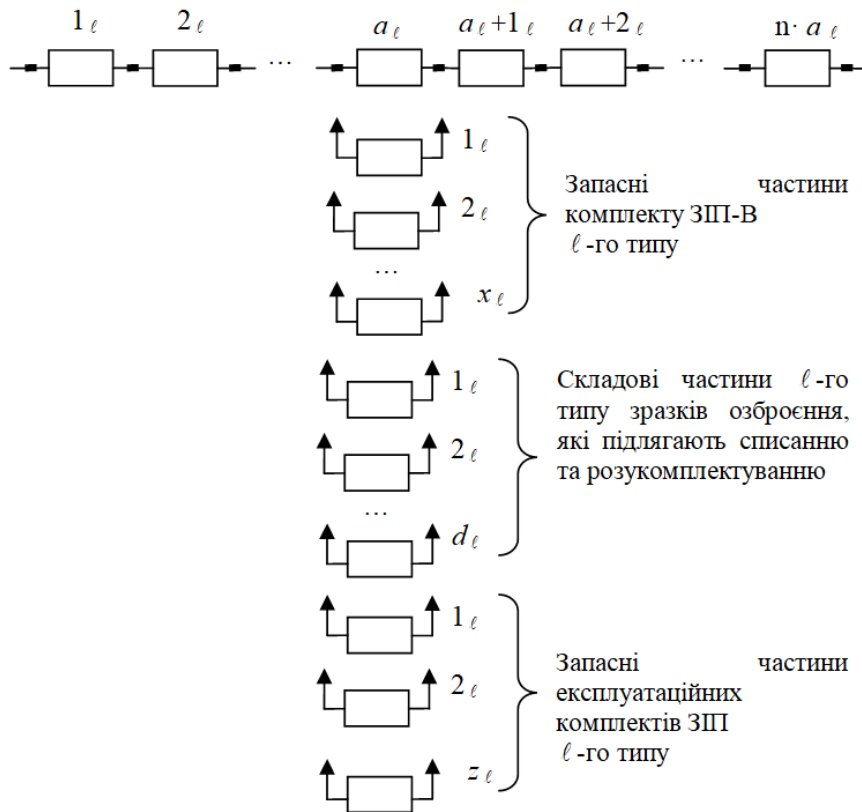


Рис. 1. Структура складових та запасних частин  $l$ -го типу  $n$  засобів ЗРО:

$a_l$  – кількість складових частин  $l$ -го типу в засобі ЗРО;  $x_l$  – кількість складових частин  $l$ -го типу в комплекті ЗПП-В;  $z_{f,l}$  – кількість складових частин  $l$ -го типу в експлуатаційних комплектах ЗПП;  $d_l$  – кількість складових частин  $l$ -го типу в зразках озброєння, які підлягають списанню та розукомплектуванню

У загальному випадку, коли ймовірності бойових пошкоджень складових та запасних частин  $l$ -го типу різні, доцільно для синтезу розрахункового співвідношення використовувати метод твірної функції [10].

Тоді технічний стан пари “виріб-ЗПП” (рис. 1) може бути описаний наступним чином

$$\varphi_l(z) = \left[ \prod_{j=1}^{na_l} (q_{l,j} + P_{l,j}z) \right] \cdot \left[ \prod_{j=na_{f,l}}^{na_l+x_l} (q_{f,l,j}^{зпп-в} + P_{f,l,j}^{зпп-в}z) \right] \times \left[ \prod_{j=na_l+x_l}^{na_l+x_l+z_l} (q_{l,j}^{зпп} + P_{l,j}^{зпп}z) \right] \cdot \left[ \prod_{j=na_l+x_l+z_l}^{na_l+x_l+z_l+d_l} (q_{l,j}^p + P_{l,j}^pz) \right],$$

де:  $\varphi_l(z)$  – твірна функція, що характеризує технічний стан складових та запасних частин  $l$ -го типу пари “виріб-ЗПП” (рис. 1);

$z$  – довільний параметр;

$q_{l,j}$  – ймовірність непошкодження  $j$ -ї складової частини  $l$ -го типу в зразку ЗРО;

$P_{l,j}$  – ймовірність бойового пошкодження  $j$ -ї складової частини  $l$ -го типу в зразку ЗРО;

$q_{l,j}^{зпп-в}$  – ймовірність непошкодження  $j$ -ї запасної частини  $l$ -го типу в комплекті ЗПП-В;

$P_{l,j}^{зпп-в}$  – ймовірність бойового пошкодження  $j$ -ї запасної частини  $l$ -го типу в комплекті ЗПП-В;

$q_{l,j}^{зпп}$  – ймовірність непошкодження  $j$ -ї

складової частини  $l$ -го типу в експлуатаційних комплектах ЗПП;

$P_{l,j}^{зпп}$  – ймовірність бойового пошкодження  $j$ -ї складової частини  $l$ -го типу в експлуатаційних комплектах ЗПП;

$q_{l,j}^p$  – ймовірність непошкодження  $j$ -ї складової частини  $l$ -го типу в зразках озброєння, які підлягають списанню та розукомплектуванню;

$P_{l,j}^p$  – ймовірність бойового пошкодження  $j$ -ї складової частини  $l$ -го типу в зразках озброєння, які підлягають списанню та розукомплектуванню.

Згідно теореми про повторення дослідів [10], ймовірність того, що пара “виріб-ЗПП” (рис. 1), до складу якої входить  $N_l$  складових та запасних частин  $l$ -го типу втратить свою працездатність з причини бойового пошкодження рівно  $k$  складових частин, дорівнює коефіцієнту при  $z^k$  у виразі твірної функції. Тоді

$$\left[ \prod_{j=1}^{na_l} (q_{l,j} + P_{l,j}z) \right] \cdot \left[ \prod_{j=na_{f,l}}^{na_l+x_l} (q_{f,l,j}^{зпп-в} + P_{f,l,j}^{зпп-в}z) \right] \times \left[ \prod_{j=na_l+x_l}^{na_l+x_l+z_l} (q_{l,j}^{зпп} + P_{l,j}^{зпп}z) \right] \cdot \left[ \prod_{j=na_l+x_l+z_l}^{na_l+x_l+z_l+d_l} (q_{l,j}^p + P_{l,j}^pz) \right] = \sum_{k=0}^{N_l} P_{l,k} z^k,$$

де:  $P_{\ell,k}$  – ймовірність втрати працездатності пари “виріб-ЗІП” з причини бойового пошкодження рівно  $k$  складових частин  $\ell$ -го типу.

У цьому випадку ймовірність виникнення події  $B_{\ell}$  може бути розрахована за співвідношенням

$$P(B_{\ell}) = \sum_{k=Z_{\ell}+1}^{N_{\ell}} P_{\ell,k}, \quad (7)$$

де:  $Z_{\ell}$  – загальна кількість запасних частин  $\ell$ -го типу в системі “виріб-ЗІП”.

Враховуючи (7) ймовірність того, що запасних частин  $\ell$ -го типу буде достатньо для проведення відновлювального ремонту  $P_{\text{зип}}(x_{\ell})$  для випадку різних ймовірностей бойових пошкоджень складових частин однієї номенклатури може розраховуватися за співвідношенням

$$P_{\text{зип}}(x_{\ell}) = 1 - \sum_{k=Z_{\ell}+1}^{N_{\ell}} P_{\ell,k}. \quad (8)$$

Враховуючи те, що до складу системи “виріб-ЗІП” входять складові та запасні частини різної номенклатури співвідношення для розрахунку

$P_{\text{зип}}(X)$  набуває такого вигляду

$$P_{\text{зип}}(X) = \prod_{\ell=1}^L P_{\text{зип}}(x_{\ell}). \quad (9)$$

Зробивши підстановку (9), (4) в (3), отримаємо:

$$P(X, t_{\text{вр}}) = \prod_{\ell=1}^L \left( 1 - \sum_{k=Z_{\ell}+1}^{N_{\ell}} P_{\ell,k} \right) \cdot \Phi \left[ \frac{t_{\text{вр}} - t_{\text{вроч}}}{\sigma(t_{\text{вроч}})} \right]. \quad (10)$$

Таким чином, знайдено аналітичне співвідношення для розрахунку ймовірності своєчасного проведення відновлювального ремонту зразків ЗРО.

На відміну від відомих [1-4], співвідношення (10) на основі даних про номенклатуру та кількість складових частин, що визначають працездатність зразка озброєння, кількість запасних частин у відновлювальних та експлуатаційних комплектах

### Література

**1. Буравлев А. И.** Марковская модель восстановления вооружения и военной техники в новой системе технического обслуживания и ремонта / А.И. Буравлев // Вооружения и экономика. – 2014. – №1(26). – С. 39-52.  
**2. Пьянков А.А.** Математическая модель процесса восстановления вооружения и военной техники в ходе боевых действий тактического воинского формирования / А.А. Пьянков // Вооружения и экономика. – 2014. – №2(27). – С. 53-64.  
**3. Быкадор А.К.** Основы эксплуатации радиоэлектронной аппаратуры / А.К. Быкадор, Л.И. Кульбак, В.Ю. Лавриненко и др.: Под ред. В.Ю. Лавриненко. – Высш. школа, 1978. – 320 с.  
**4. Боярников В. Б.** Восстановление военной и боевой техники ЗРВ ПВО страны / В. Б. Боярников ; под ред. Н. Д. Гребенникова. – Минск : МВИЗРУ ПВО, 1972. – 240 с.  
**5. Методика визначення та корегування складу запасів запасних частин комплектів ЗІП наземних бойових засобів зенітних ракетних комплексів / Б.М. Ланецький, В.В. Лук'янчук, О.М. Доска, В.В. Лісовенко // Проблеми координації воєнно-технічної та оборонно-промислової політики в Україні. Перспективи розвитку озброєння та військової техніки: матеріали V Міжнародної науково-**

ЗІП, номенклатуру та кількість працездатних складових частин в зразках озброєння, які підлягають списанню і розукомплектуванню, ймовірності їх бойових пошкоджень та оцінок математичного сподівання і дисперсії часу виконання відновлювального ремонту дозволяє провести розрахунки показника ефективності відновлювального ремонту.

Достовірність розрахунку показника ефективності визначається достовірністю визначення вихідних даних.

Достовірність існуючих підходів [1-4] визначається достовірністю визначення інтенсивності потоку відмов та інтенсивності відновлення, їх апроксимаціями і припущеннями, які вносяться при розрахунках, наприклад, про пуассонівський потік заявок.

Виходячи з цього, запропонований підхід характеризується більш високою достовірністю розрахунку.

### Висновки й перспективи подальших досліджень

Розроблено метод розрахунку показника ефективності відновлювального ремонту – ймовірності проведення відновлювального ремонту за час, який не перевищує задане значення.

На відміну від відомих, запропонований метод враховує: обмеженість запасів експлуатаційних та відновлювальних комплектів ЗІП; можливість бойових пошкоджень як складових, так і запасних частин засобів ЗРО; можливості використання в якості запасних частин при проведенні відновлювальних ремонтів складових частин зразків ЗРО, які підлягають списанню і розукомплектуванню; обмежень щодо часу проведення відновлювального ремонту, що дозволяє позбутися припущень про надходження інтенсивності потоку заявок та інтенсивності відновлення, тим самим підвищити достовірність отриманих результатів.

практичної конференції, 11–12 жовтня 2017 року.: тези доповіді. – К., 2017. – 272-273.  
**6. Ковтуненко А.П.** Основы теории восстановления эксплуатационных свойств технических систем / Ковтуненко А.П., Шишанов М.А., Зубарев В.В. – К.: НАУ, 2007. – 294 с.  
**7. Ковтуненко А. П.** Восстановление эксплуатационных свойств радиоэлектронных систем / А. П. Ковтуненко, В. Н. Козлов, Ю. М. Россинский. – М. : МО, 1980. – 257 с.  
**8. Флоров О.Д.** Розрахунок складу ремонтного комплекту ЗІП бойових засобів ЗРК / О.Д. Флоров, О.М. Доска // Наука і техніка Повітряних Сил ЗС України. Х.: ХУПС.– 2013. – Вип. 1(10) – С. 61-64.  
**9. Метод розрахунку показника достатності відновлювального комплекту ЗІП зразків зенітного ракетного озброєння, які отримують бойові пошкодження / Б.М. Ланецький, О.М. Доска, // Новітні технології для захисту повітряного простору: матеріали десятої наукової конференції Харківського університету Повітряних Сил ім. І. Кожедуба, 9-10 квіт. 2014 р.: Тези доповіді. – Х., 2014. – С. 111.  
**10. Ландо С.И.** Лекции о производящей функции / Ландо С.И. – М. МЦНМО, 2007. – 144 с.**

## ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЯ ЭФФЕКТИВНОСТИ ВОССТАНОВЛЕНИЯ ЗЕНИТНОГО РАКЕТНОГО ВООРУЖЕНИЯ С УЧЕТОМ РЕСУРСНЫХ ОГРАНИЧЕНИЙ

*Александр Михайлович Доска (кандидат технических наук)<sup>1</sup>  
Павел Викторович Опенько (кандидат технических наук)<sup>2</sup>  
Анатолий Сергеевич Дудуш (кандидат технических наук)<sup>1</sup>  
Максим Владимирович Сургай<sup>1</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

Обосновывается подход к определению вероятности своевременного проведения восстановительного ремонта с учетом ограниченных запасов запасных частей, материалов, инструментов и принадлежностей (ЗИП). Найдено аналитическое соотношение для расчета вероятности своевременного проведения восстановительного ремонта образцов зенитного ракетного вооружения (ЗРО). Предложенное соотношение позволяет учесть данные о номенклатуре и количестве составных частей, определяющих работоспособность образца вооружения, количество запасных частей в восстановительных и эксплуатационных комплектах ЗИП, номенклатуру и количество работоспособных составных частей в образцах вооружения, которые подлежат списанию и разуконплектованию, вероятности боевых повреждений составных частей и время выполнения восстановительного ремонта.

**Ключевые слова:** восстановительный ремонт; зенитное ракетное вооружение; ресурсные ограничения; показатели эффективности.

## DETERMINING THE RECOVERY EFFICIENCY INDEX OF ANTI-AIRCRAFT MISSILE ARMAMENT, TAKING INTO ACCOUNT RESOURCE CONSTRAINTS

*Alexander Doska (Candidate of Technical Sciences)<sup>1</sup>  
Pavlo Open'ko (Candidate of Technical Sciences)<sup>2</sup>  
Anatolii Dudush (Candidate of Technical Sciences)<sup>1</sup>  
Maksim Surgai<sup>1</sup>*

<sup>1</sup>Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

<sup>2</sup>National Defense University of Ukraine named by Ivan Cherniakhovsky, Kyiv, Ukraine

The approach to determining the probability of timely conduct the recovery repair taking into account limited stocks of spare parts, materials, tools and accessories (spare parts) is substantiated. An analytical expression is found to calculate the probability of timely conduct the recovery repair of anti-aircraft missile armament (AMA). The proposed expression allows to take into account data on the nomenclature and number of components that determine the operability of an AMA, the number of spare parts in recovery and operational spare parts kits, the nomenclature and the number of operable components in AMAs that are subject to decommissioning and understaffing, the probability of combat damage of AMA's components and recovery repair time.

**Key words:** recovery repair, anti-aircraft missile armament, resource limitations, efficiency indexes.

### References

1. Buravlev A. I. Markovskaya model vosstanovleniya vooruzheniya i voennoj tehniky v novej sisteme tehničeskogo obslužhivaniya i remonta / A.I. Buravlev // Vooruzheniya i ekonomika. – 2014. – №1(26). – S. 39-52.  
2. Pyankov A.A. Matematicheskaya model processa vosstanovleniya vooruzheniya i voennoj tehniky v hode boevyh dejstvij taktičeskogo vojnogo formirovaniya / A.A. Pyankov // Vooruzheniya i ekonomika. – 2014. – №2(27). – S. 53-64.  
3. Bykador A.K. Osnovy ekspluatcii radioelektronnoj apparatury / A.K. Bykador, L.I. Kulbak, V.Yu. Lavrinenko i dr.: Pod red. V.Yu. Lavrinenko. – Vyssh. shkola, 1978. – 320 s.  
4. Boyarnikov V. B. Vosstanovlenie voennoj i boevoj tehniky ZRV PVO strany / V. B. Boyarnikov ; pod red. N. D. Grebennikova. – Minsk : MVIZRU PVO, 1972. – 240 s.  
5. Metodika viznachennya ta koreguvannya skladu zapasiv zapasnih chastin kompleksiv ZIP nazemnih bojovih zasobiv zenitnih raketnih kompleksiv / B.M. Laneckij, V.V. Luk'yančuk, O.M. Doska, V.V. Lisovenko // Problemi koordinaciyi voyenno-tehničnoy ta oboronno-promislovovyi politiki v Ukraini. Perspektivi rozvitku ozbrojenya ta vijskovoyi tehniky: materiali V

Mizhnarodnoy naukovo-praktičnoy konferenciyi, 11–12 zhovtnya 2017 roku.: tezi dopovidi. – K., 2017. – 272-273.  
6. Kovtunenکو A.P. Osnovy teorii vosstanovleniya ekspluatacionnyh svojstv tehničeskijh sistem / Kovtunenکو A.P., Shishanov M.A., Zubarev V.V. – K.: NAU, 2007. – 294 s.  
7. Kovtunenکو A. P. Vosstanovlenie ekspluatacionnyh svojstv radioelektronnyh sistem / A. P. Kovtunenکو, V. N. Kozlov, Yu. M. Rossinskij. – M. : MO, 1980. – 257 s.  
8. Florov O.D. Rozrahunok skladu remontnogo komplektu ZIP bojovih zasobiv ZRK / O.D. Florov, O.M. Doska // Nauka i tehnika Povitryanij Sil ZS Ukrayini. H.: HUPS.– 2013. – Vip. 1(10) – S. 61-64.  
9. Metod rozrahunku pokaznika dostatnosti vidnovlyvalnogo komplektu ZIP zrazkiv zenitnogo raketnogo ozbrojenya, yaki otrimuyut bojovi poskodzhennya / B.M. Laneckij, O.M. Doska, // Novitni tehnologiyi dlya zahistu povitryanogo prostoru: materiali desyatoyi naukovoyi konferenciyi Harkivskogo universitetu Povitryanij Sil im. I. Kozheduba, 9-10 kvit. 2014 r.: Tezi dopovidi. – H., 2014. – S. 111.  
10. Lando S.I. Lekcii o proizvodyashej funkcii / Lando S.I. – M. MCNMO, 2007. – 144 s.

Олег Александрович Білобородов (кандидат технічних наук)

Центральний науково-дослідний інститут озброєння та військової техніки ЗС України, Україна

## УПРАВЛІННЯ ШИРИНОЮ ДІАГРАМИ НАПРАВЛЕНОСТІ І ПОТУЖНІСТЮ ВИПРОМІНЮВАННЯ АНТЕННОЇ СИСТЕМИ

Для боротьби з групами безпілотних літальних апаратів, а також для інших завдань ефективним є застосування засобів електромагнітного впливу. При зміні відстані до групової цілі її кутовий розмір змінюється, тому актуальним є завдання ефективного регулювання ширини діаграми направленості антенної системи випромінювального радіотехнічного засобу і потужності, що випромінюється. У статті наведені основні співвідношення для забезпечення заданої густини потоку потужності випромінювання у заданій області з урахуванням поглинання енергії в атмосфері. Представлені результати аналізу методів синтезу антен та обґрунтовані основні методи регулювання ширини діаграми направленості: використання апертури змінного розміру, а також варіювання параметрів для параметричних амплітудних розподілів збуджуючих струмів вздовж апертури антени. Проведено аналіз впливу зазначених параметрів на показники поля випромінювання антен. Представлено розроблені алгоритми варіювання параметрів і потужності випромінювання для забезпечення заданого рівня впливу густини потоку потужності випромінювання на ціль. Отримані результати дозволяють обґрунтовувати вимоги до радіотехнічних засобів електромагнітного впливу (боротьби з безпілотним літальними апаратами, системами управління противника тощо). Результати можна застосовувати у складі алгоритмів систем управління спеціальних радіотехнічних засобів.

**Ключові слова:** радіотехнічний засіб; антенна система; діаграма направленості; потужність випромінювання; густина потоку потужності.

### Вступ

В останні роки стрімко поширюється обсяг застосування безпілотних літальних апаратів [1]. Групи БпЛА застосовуються для атаки як військових об'єктів, так і важливих об'єктів інфраструктури. Для боротьби з такого роду викликами, а також для інших завдань можливо застосування засобів електромагнітного впливу [2]. При цьому засоби електромагнітного впливу мають переваги перед іншими саме для протидії групам БпЛА [3].

**Постановка проблеми.** У випадку зміни відстані між складною (груповою) ціллю і засобом електромагнітного впливу її кутовий розмір також змінюється (рис. 1).

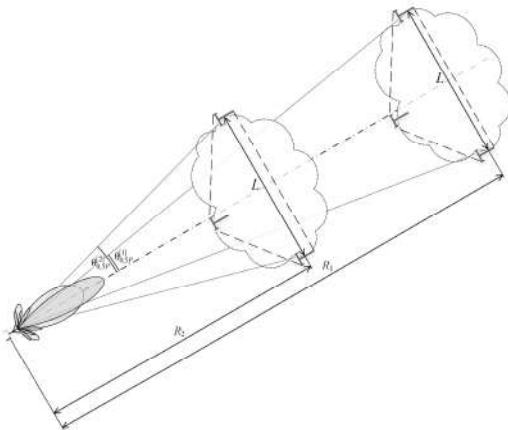


Рис. 1. Зміна необхідної ширини ДН

Для забезпечення необхідної напруженості поля (густини потоку потужності випромінювання) постає проблема ефективного регулювання ширини діаграми направленості (ДН) антенної системи випромінювального радіотехнічного засобу і потужності, що випромінюється.

**Аналіз останніх досліджень і публікацій.** Аналіз методів синтезу антен свідчить, що управління шириною ДН для заданої антени можна здійснювати зміною амплітудно-фазового розподілу струмів збудження [4]: більш швидке спадання амплітуди збуджуючих струмів від центру до краю апертури призводить до розширення ДН. Але для такого способу необхідно розроблювати систему управління необхідного розподілу струмів збудження [5], що може значно ускладнити антенну систему [6]. Крім того, ширина ДН, при інших рівних умовах, залежить від розміру випромінювальної апертури: зі збільшенням розмірів антени ДН звужується. Дискретний варіант зазначеного способу можна просто реалізувати у фазованій антенній решітці [7, 8] шляхом регулювання кількості рядків випромінювання і кількості активних елементів випромінювання у рядку.

Враховуючи зазначене метою статті є запропонування антенної системи та синтез алгоритму управління нею для забезпечення опромінювання області заданого розміру із інтенсивністю, не менше заданої.

У ході дослідження використовувались такі методи: аналіз теоретичних джерел з проблем синтезу антен, синтез випромінювальних систем, синтез ДН, математичне моделювання.

**Виклад основного матеріалу дослідження**

1. *Енергетичні співвідношення.* Поверхнева густина потоку потужності електромагнітного випромінювання у дальній зоні  $R$  без урахування затухань визначається формулою [9]:

$$S_0 = \frac{PD\eta_A}{4\pi R^2}, \quad (1)$$

де  $P$  – середня потужність, що підводиться до антени,  $D$  – коефіцієнт направленої дії,  $\eta_A$  – коефіцієнт корисної дії антени.

При наявності затухань густина потоку зменшується [9]:

$$S = \frac{S_0}{10^{0,1\gamma R}} = \frac{PD\eta_A}{4\pi R^2 \cdot 10^{0,1\gamma R}}, \quad (2)$$

де  $\gamma$ , [дБ/км] – коефіцієнт затухання (табл. 1) за напрямком поширення хвиль електромагнітного випромінювання ( $R$ , [км]).

Таблиця 1

Значення коефіцієнтів затухання для нормального стану атмосфери [10; 11]

$\lambda$ , [см]	0,1	0,2	0,3	0,4	0,46	0,6	0,7	0,8	1
$\gamma$ , [дБ/км]	6	2	0,5	0,35	2	0,4	0,2	0,12	0,1
$\lambda$ , [см]	2	3	5	10	21	24	25	65	150
$\gamma$ , [дБ/км]	$4 \cdot 10^{-2}$	$1,4 \cdot 10^{-2}$	$9,5 \cdot 10^{-3}$	$7,0 \cdot 10^{-3}$	$6 \cdot 10^{-3}$	$5,7 \cdot 10^{-3}$	$5,6 \cdot 10^{-3}$	$5 \cdot 10^{-3}$	$4,8 \cdot 10^{-3}$

Якщо у заданій області необхідно забезпечити  $S \geq S_{\min}$ , то з (2) необхідна потужність, що підводиться до антени:

$$P \geq \frac{4\pi S_{\min} R^2}{D\eta_A} \cdot 10^{0,1\gamma R}. \quad (3)$$

2. *Просторово-енергетичні характеристики випромінювання антен.* Результати аналізу методів синтезу антен дозволили, у якості основних методів регулювання ширини ДН, визначити наступні: використання апертур з можливістю зміни розміру, а також використання параметричних амплітудних розподілів. У якості апертури перемінного розміру розглядається антенна решітка (АР) із зміною кількості випромінювачів. Збільшення кількості випромінювачів, при інших незмінних умовах, дозволяє таким чином впливати на множник АР, що головний максимум результуючої ДН звужується. Управління шириною ДН пропонується здійснювати шляхом увімкнення/вимкнення рядків випромінювання і елементів у рядках таким чином, щоб забезпечити попадання заданого району у перетин головної пелюстки ДН антенної системи. У такій постановці можна сказати, що в якості варійованого параметру виступає кількість рядків (випромінювачів у рядку)  $N$ .

Серед параметричних амплітудних розподілів було обрано такі, у яких просто організовується регулювання параметра амплітудного розподілу, а саме: розподіл типу “косинус на п’єдесталі” (регульований параметр – величина п’єдесталу  $\Delta$ ) і розподіл типу  $\cos^n$  (регульований параметр – ступінь  $n$ ).

Результати попереднього моделювання показали, що для розширення можливостей доцільно поєднувати методи, що базуються на використанні параметричних амплітудних розподілів за методом варіювання кількості

випромінювачів. У якості базової антенної системи була обрана АР з ізотропними випромінювачами, а параметричні розподіли реалізовані у їх симетричному дискретному варіанті.

2.1. *Варіювання кількості рядків (елементів) випромінювання  $N$ .* Аналіз характеристик поля випромінювання АР у дальній зоні за відомими співвідношеннями, як зазначалось, показує, що варійованим параметром для регулювання ширини ДН може виступати кількість активних рядків випромінювання і елементів у рядках при рівномірному розподілі збуджуючих струмів вздовж апертури антени. Результати моделювання можливостей зміни ширини ДН для різної кількості випромінювачів наведені на рис. 2.

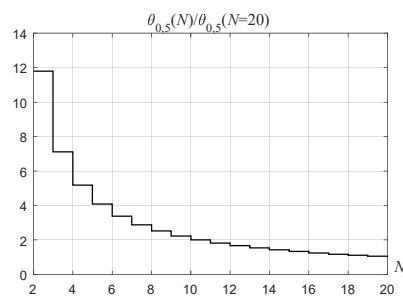


Рис. 2. Варіювання ширини ДН АР з рівномірним розподілом залежно від кількості рядків (елементів) випромінювання  $N$

Аналіз результатів моделювання свідчить, що метод варіювання кількості активних елементів випромінювання АР дозволяє досягти зміни ширини ДН до  $\sim 12$  разів для АР  $20 \times 20$  випромінювачів.

Для реалізації методу регулювання ширини головної пелюстки випромінювання АР шляхом варіювання кількості активних елементів випромінювання розроблено блок-схему алгоритму обчислень, що наведена на рис. 3.

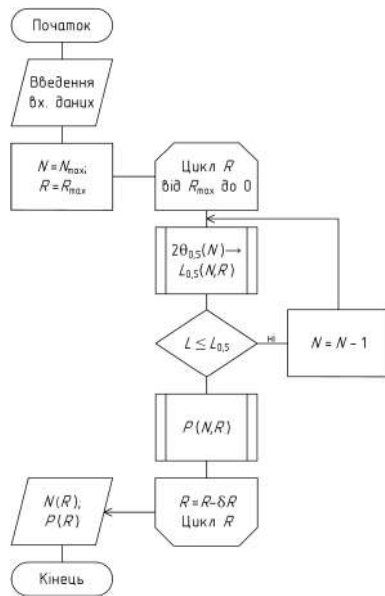


Рис. 3. Блок-схема алгоритму обчислень варіювання рядків (елементів) і потужності випромінювання АР з рівномірним розподілом струмів збудження

Далі розглянемо можливість регулювання ширини ДН зміною параметрів амплітудного розподілу збуджуючих струмів в апертурі антени.

2.2. Амплітудний розподіл типу “косинус на п’єдесталі”. Розглянемо найбільш поширений варіант амплітудного розподілу, а саме – розподіл типу “косинус на п’єдесталі”. Аналіз виразу для ДН у дальній зоні, як зазначалось, свідчить, що регулювання ширини ДН можна здійснювати шляхом варіювання параметра розподілу  $\Delta$  ( $\Delta = 1$  відповідає рівномірному розподілу,  $\Delta = 0$  відповідає зниженню амплітуд збуджуючих струмів на краях апертури до нуля). Результати моделювання можливостей зміни ширини ДН методом варіювання параметра  $\Delta$  наведені на рис. 4.

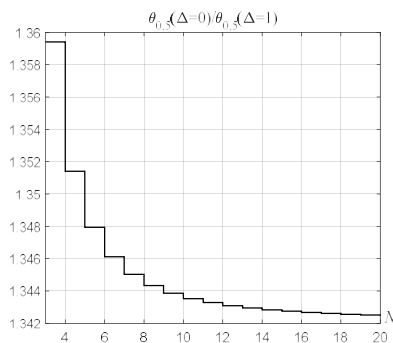


Рис. 4. Варіювання ширини ДН залежно від параметра  $\Delta$

Аналіз результатів моделювання свідчить, що метод варіювання параметру  $\Delta$  розподілу типу “косинус на п’єдесталі” дозволяє досягти варіювання шириною ДН АР від  $\sim 1,34$  разів для багатоеlementних АР до  $\sim 1,36$  для малорозмірних АР.

Для реалізації методу регулювання ширини головної пелюстки ДН АР шляхом варіювання параметру  $\Delta$  розподілу типу “косинус на п’єдесталі” розроблено блок-схему алгоритму обчислень, що наведена на рис. 5.

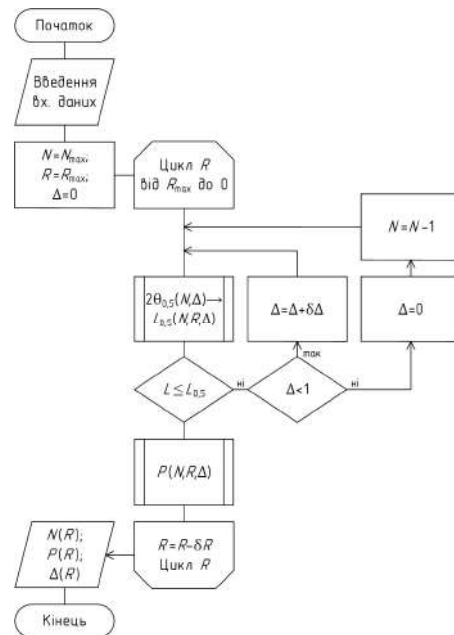


Рис. 5. Блок-схема алгоритму обчислень варіювання параметра  $\Delta$  і потужності випромінювання для розподілу типу “косинус на п’єдесталі”

2.3. Амплітудний розподіл типу  $\cos^n$ . Іншим видом розподілу, який дозволяє регулювати ширину ДН є розподіл типу  $\cos^n$ . Аналіз виразу для ДН антени у дальній зоні свідчить, що регулювання ширини ДН можна здійснювати, як зазначалось, шляхом варіювання параметра  $n$ . Результати моделювання можливостей зміни ширини ДН методом варіювання параметра  $n$  наведені на рис. 6.

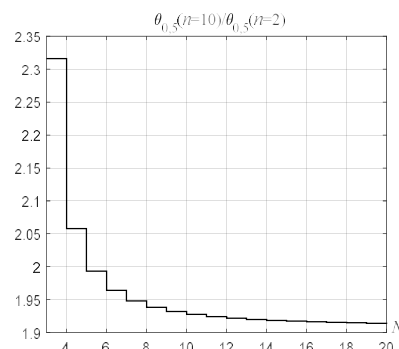


Рис. 6. Варіювання ширини ДН залежно від параметра  $n$

Таким чином, регулювання параметру  $n$  для розподілу  $\cos^n$  дозволяє досягти зміни ширини ДН від  $\sim 1,9$  разів для багатоеlementних АР до  $\sim 2,35$  для малорозмірних АР.

Для реалізації методу регулювання ширини головної пелюстки ДН АР шляхом варіювання параметру  $n$  розподілу типу  $\cos^n$  розроблено блок-схему алгоритму обчислень, що наведена на рис. 7.

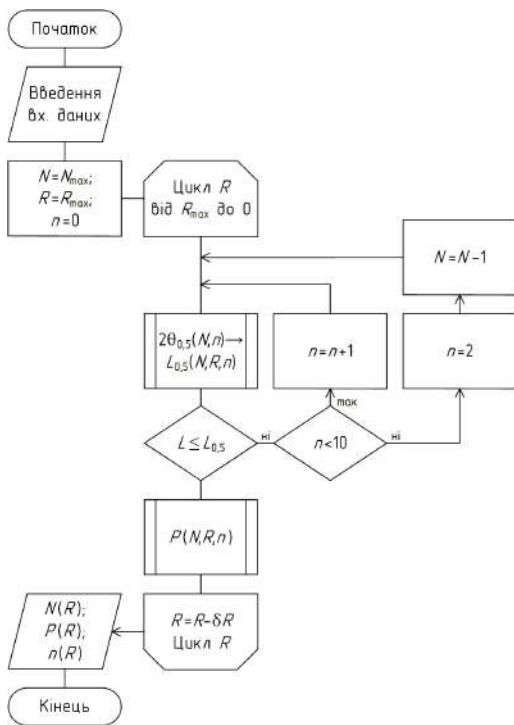


Рис. 7. Блок-схема алгоритму обчислень варіювання параметра  $n$  і потужності випромінювання для розподілу типу  $\cos^n$

2.4. *Моделювання і перевірка отриманих результатів.* Відповідно до розроблених алгоритмів було проведено програмне моделювання. Для обчислень було обрано наступні вхідні дані: максимальна кількість рядків АР та елементів у рядках  $N_{\max}=20$ ; довжина хвилі  $\lambda=3$  см, що відповідає  $\gamma=0,014$  Дб/км; відношення  $d/\lambda=0,5$ ; максимальна дальність до цілі  $R_{\max}=1,2$  км. Для вироблення управляючих команд було синтезовано програмний комплекс формування команд управління радіотехнічним засобом при зміні відстані до району опромінення та перевірено його працездатність (рис. 8).

Для різних типів розподілу було проведено порівняння енергетичних показників (рис. 9).

2.5. *Обговорення результатів.* Отримані залежності і результати моделювання підтверджують основні положення теорії антен, зокрема щодо:

характеру залежності ширини головної пелюстки ДН залежно від розміру апертури і розподілу збуджуваних струмів вздовж апертури антени;

зменшення впливу розподілу збуджуваних струмів на показники направленості із збільшенням розміру АР.

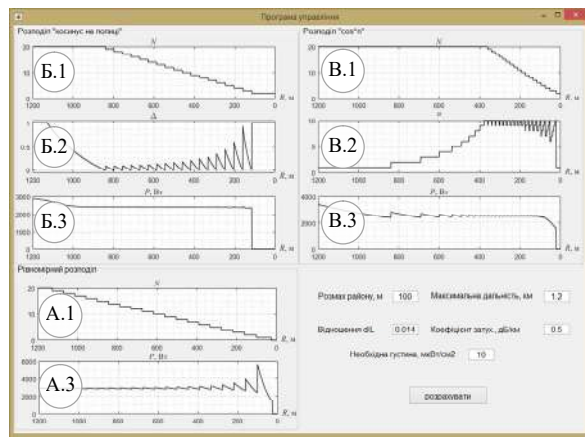


Рис. 8. Послідовність формування команд управління залежно від дальності до цілі у програмному модулі: необхідна кількість рядків (елементів) випромінювання (1), необхідне значення варіюваного параметра (2), необхідна потужність (3) для рівномірного розподілу (А), розподілу типу “косинус на п’єдесталі” (Б) та типу  $\cos^n$  (В)

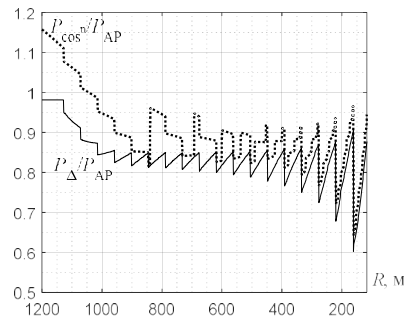


Рис. 9. Порівняння енергетичних показників

Для впливу на великі дистанції показники направленості антени необхідно збільшувати, а єдиним шляхом для цього є збільшення розмірів апертури. Отже, запропонований метод варіювання як розмірів апертури, так і розподілу збуджуваних струмів виявився виправданим.

Аналіз отриманих результатів моделювання стосовно енергетичних показників свідчить: для рівномірний розподіл більш ефективний лише на великих відстанях, коли розмір області опромінення менше розміру перерізу головної пелюстки ДН антени.

Розроблені алгоритми і програмний модуль дозволяють обґрунтовувати вимоги до радіотехнічних засобів електромагнітного впливу (боротьби з БпЛА, системами управління противника тощо).

Типові операції з обґрунтування вимог до зразка:

у залежності від максимальної потужності генераторного пристрою, обґрунтовуються вимоги до зразка стосовно дальності дії (рис. 10);

у залежності від ширини ДН і відповідної дальності застосування обґрунтовуються вимоги стосовно фазових неоднорідностей, точності наведення і стабілізації антенної системи;



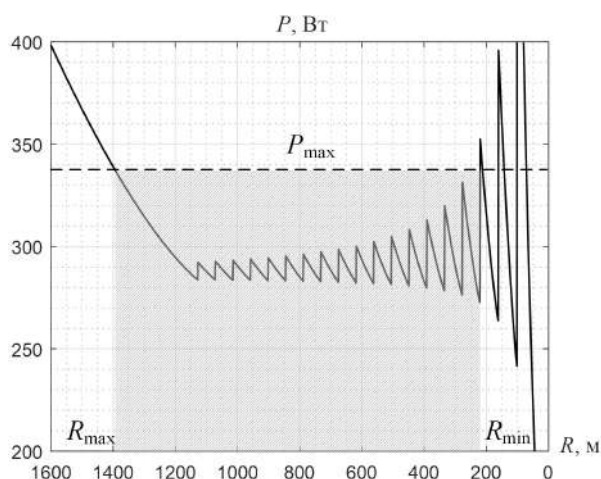


Рис. 10. Використання отриманих результатів для обґрунтування пропозицій щодо побудови засобів впливу

у залежності від необхідної дальності визначаються вимоги до потужності або до розмірності АР (рис. 10);

у випадку високої динаміки роботи радіотехнічного засобу, відсутності регулювання у реальному часі параметрів розподілу збуджуючих струмів, або відсутності оперативних даних про

відстань до області впливу, у якості параметрів управління можна обирати усереднені (або граничні) вимоги до енергетичних параметрів і параметрів розподілу збуджуючих струмів для певного інтервалу дії.

### Висновки й перспективи подальших досліджень

У результаті проведених досліджень розроблено алгоритми і програмний модуль синтезу сигналів управління параметрами розподілу збуджуючих струмів і потужністю випромінювання для регулювання ширини ДН і забезпечення у заданій області необхідного потоку потужності електромагнітного випромінювання для функціонального ураження цілей. Отримані результати можна застосовувати при обґрунтуванні тактико-технічних вимог до зразків спеціальних радіотехнічних засобів, а також у складі систем управління ними. Напрямок подальших досліджень можна визначити обґрунтування вимог щодо точності наведення і стабілізації розглянутих засобів, а також синтез системи управління для сканувальних антенних систем.

### Література

1. James DeShaw Rae. Analyzing the Drone Debates: Targeted Killing, Remote Warfare, and Military Technology. Springer, 2014. 147 p. DOI: 10.1057/9781137381576.
2. Семенец В. О., Трухин М. П. Способы противодействия беспилотным летательным аппаратам. *Наукоёмкие технологии в космических исследованиях Земли*. 2018. Т. 10. № 3. С. 4-12. DOI: 10.24411/2409-5419-2018-10070.
3. Теодорович Н. Н., Строганова С. М., Абрамов П. С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами. *Интернет-журнал "Науковедение"*. 2017. Т. 9, № 1. URL: <http://naukovedenie.ru/PDF/13TVN117.pdf>. (дата звернення: 19.11.2019).
4. Сахацкий В. Д., Щеглов А. Ю. Антенный излучатель для систем диагностики подповерхностных объектов. *Scientific Journal «ScienceRise»* № 5/2 (4). 2014. С. 60-63.
5. Белоусов О. А., Рязанов Е. В., Колмыкова А. С., Дякин А. И. Применение алгоритмов нечеткой логики в системе управления диаграммообразующим устройством гибридной зеркальной антенны. *Программные продукты и системы*. 2018. № 4 (31). С. 757-762. DOI: 10.15827/0236-235X.031.4.757-762.
6. Митрохин В. Н., Пропастин А. А. Синтез излучающей системы, формирующей секторную диаграмму направленности с минимизацией эффекта Гиббса. *Радиооптика*. МГТУ им. Н. Э. Баумана, 2016. № 6. с. 1-13. DOI: 10.7463/rdopt.0616.0852509.
7. Устройства СВЧ и антенны. Проектирование фазированных антенных решеток : Учеб. пособие для вузов / Под ред. Д.И. Воскресенского. М. : Радиотехника, 2012. 744 с.
8. Robert C. Hansen. Phased array antennas. 2009. 547 p.
9. Черный Ф. Б. Распространение радиоволн. М. : Сов. Радио, 1972. 464 с.
10. Рекомендация МСЭ-R Р.676-6. Затухание в атмосферных газах (Вопрос МСЭ-R 201/3). 2005. URL: [https://www.itu.int/dms\\_pubrec/itu-r/rec/p/R-REC-P.676-6-200503-S!!PDF-R.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.676-6-200503-S!!PDF-R.pdf). (дата звернення: 20.11.2019).
11. Захаров А. И., Кувалкин Е. С. Программная реализация методики расчета затухания радиосигнала в атмосферных газах для спутниковой связи. *Вестник Балтийского федерального университета им. И. Канта*. Серия: Физико-математические и технические науки. 2019. № 1. С. 18-27.

## УПРАВЛЕНИЯ ШИРИНОЙ ДИАГРАММЫ НАПРАВЛЕННОСТИ И МОЩНОСТЬЮ ИЗЛУЧЕНИЯ АНТЕННОЙ СИСТЕМЫ

Олег Александрович Белобородов (кандидат технических наук)

Центральный научно-исследовательский институт вооружения и военной техники ВС Украины, Украина

Для борьбы с группами беспилотных летательных аппаратов, а также для других задач эффективно применение средств электромагнитного воздействия. При изменении расстояния до групповой цели ее угловой размер изменяется, поэтому актуальной является задача эффективного регулирования ширины диаграммы направленности антенной системы излучающего радиотехнического средства и излучаемой мощности. В статье приведены основные соотношения для обеспечения заданной плотности потока мощности излучения в заданной области с учетом поглощения энергии в атмосфере. Представлены результаты анализа методов синтеза антенн и обоснованы основные методы регулирования ширины диаграммы направленности: использование апертуры переменного размера, а также варьирования параметров для параметрических амплитудных распределений возбуждающих токов вдоль апертуры антенны. Проведен анализ влияния указанных параметров на пространственно-энергетические показатели поля излучения антенн. Представлены разработанные

алгоритмы варьирования параметров и мощности излучения для обеспечения заданного уровня воздействия плотности потока мощности излучения на цель. Полученные результаты позволяют обосновывать требования к радиотехническим средствам электромагнитного воздействия (борьбы с беспилотными летательными аппаратами, системами управления противника и т.д.). Результаты можно применять в составе алгоритмов систем управления специальных радиотехнических средств.

**Ключевые слова:** радиотехническое средство; антенная система; диаграмма направленности; мощность излучения; плотность потока мощности.

## CONTROL BEAMWIDTH AND RADIATION POWER OF ANTENNA SYSTEM

*Oleh Biloborodov (Candidate of Technical Sciences)*

*Central Research Institute of Armament and Military Equipment of the Armed Forces of Ukraine, Ukraine*

To combat groups of unmanned aerial vehicles, as well as for other tasks, the use of electromagnetic means is effective. When the distance to the group target changes, its angular size changes, therefore, the urgent task is to effectively control the radiation pattern width of the antenna system of the radiating radio equipment and the radiation power. The article describes the basic relationships for ensuring a given radiation power flux density in a given region, taking into account energy absorption in the atmosphere. The results of the analysis of antenna synthesis methods are presented and the main methods for controlling the width of the radiation pattern are substantiated: the use of aperture of variable size, as well as variation of parameters for the parametric amplitude distributions of exciting currents along the antenna aperture. The analysis of the influence of parameters on the spatial and energy parameters of the radiation field of the antennas is carried out. The developed algorithms for varying the parameters and radiation power to provide a given level of impact on the target are presented. The results obtained allow us to justify the requirements for radio equipment of electromagnetic effects (combat unmanned aerial vehicles, enemy control systems, etc.). The results can be used as part of control systems algorithms for special radio equipment.

**Keywords:** radio engineering tool; antenna system; radiation pattern; radiation power; power flux density.

### References

1. James DeShaw Rae (2014), Analyzing the Drone Debates: Targeted Killing, Remote Warfare, and Military Technology. Springer, 147 p. DOI: 10.1057/9781137381576.
2. Semenets V. O., Truhin M. P. (2018), Ways to counter unmanned aerial vehicles [Sposoby protivodeystviya bespilotnyim letatelnyim apparatam]. Naukoemkie tehnologii v kosmicheskikh issledovaniyakh Zemli, Vol.10. No.3. pp. 4-12. DOI: 10.24411/2409-5419-2018-10070.
3. Teodorovich N. N., Stroganova S. M., Abramov P. S. (2017), Methods for detecting and combating small-sized unmanned aerial vehicles [Sposoby obnaruzheniya i borby s malogabaritnyimi bespilotnyimi letatelnyimi apparatami]. Internet-zhurnal "Naukovedenie", Vol. 9, No. 1, available at: <http://naukovedenie.ru/PDF/13TVN117.pdf>.
4. Sahatskiy V. D., Scheglov A. Yu. (2014), Antenna emitter for diagnostic systems of subsurface objects [Antennyiy izluchatel dlya sistem diagnostiki podpoverhnostnykh ob'ektov]. Scientific Journal «ScienceRise», No. 5/2 (4), pp. 60-63.
5. Belousov O. A., Ryazanov E. V., Kolmyikova A. S., Dyakin A. I. (2018) The use of fuzzy logic algorithms in the control system of a beam-forming device of a hybrid mirror antenna. [Primenenie algoritmov nechetkoy logiki v sisteme upravleniya diagrammoobrazuyuschim ustroystvom gibridnoy zerkalnoy anteny], Programmnye produkty i sistemy, No. 4 (31). pp. 757-762. DOI: 10.15827/0236-235X.031.4.757-762.
6. Mitrohin V. N., Propastin A. A. (2016), Synthesis of a radiating system forming a sector radiation pattern with minimization of the Gibbs effect [Sintez izluchayushey sistemy, formiruyushey sektornuyu diagrammu napravlenosti s minimizatsiey efekta Gibbsa], Radiooptika, MGTU im. N. E. Bauman, No. 6. pp. 1-13. DOI: 10.7463/rdopt.0616.0852509.
7. Microwave devices and antennas. Designing Phased Antenna Arms: Textbook for High Schools [Ustroystva SVCh i anteny. Proektirovanie fazirovannykh antenykh reshetok : Ucheb, posobie dlya vuzov], Ed. Voskresensky D. I., Radiotekhnika, Moscow (2012), 744 p.
8. Robert C. Hansen (2009), Phased array antennas, 547 p.
9. Chernyy F. B. (1972), Radiowave propagation [Rasprostranenie radiovoln], M. : Sov. Radio, 464 p.
10. Recommendation ITU-R P.676-10. (09/2013). Attenuation by atmospheric gases, available at: [https://www.itu.int/dms\\_pubrec/itu-r/rec/p/R-REC-P.676-10-201309-S!!PDF-E.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.676-10-201309-S!!PDF-E.pdf).
11. Zaharov A. I., Kuvalkin E. S. (2019), Software implementation of the method for calculating the attenuation of a radio signal in atmospheric gases for satellite communications [Programmnyaya realizatsiya metodiki rascheta zatuhaniya radiosignala v atmosferynykh gazakh dlya sputnikovoy svyazi], Vestnik Baltiyskogo federalnogo universiteta im. I. Kanta. Seriya: Fiziko-matematicheskie i tehnicheskie nauki, No. 1, pp. 18-27.

## ЕЛЕМЕНТИ ІМІТАЦІЇ У РІВНЯННЯХ МОДЕЛЕЙ ЛАНЧЕСТЕРСЬКОГО ТИПУ

У статті приведений короткий огляд можливої сфери застосування модифікацій моделей ланчестерського типу, а також розглянуті деякі особливості використання елементів імітації та чисельного вирішення диференціальних рівнянь таких моделей у стохастичній постановці. Стохастична постановка дозволяє певним чином імітувати вплив випадкових факторів та урахувати елементи невизначеності, які впливатимуть на динаміку змін чисельності протиборчих угруповань, і які у тій чи іншій мірі присутні у будь-яких бойових діях. На відміну від детермінованих моделей, стохастичні моделі потребують використання спеціальних чисельних методів, вибір конкретного з яких може ґрунтуватися на вимогах до ступеню їх збіжності на інтервалі інтегрування. Оцінка збіжності може слугувати також для перевірки правильності програмної реалізації обраного методу.

**Ключові слова:** імітація у ланчестерських моделях; стохастичні диференціальні рівняння; методи чисельного вирішення; збіжність методу.

### Вступ

**Постановка проблеми.** Інтерес до моделей ланчестерського типу, який простежується за регулярними публікаціями у тематичних періодичних виданнях, зокрема [1-5], свідчить про дієвість такого апарату для питань оперативного прогнозування змін у чисельності протиборчих угруповань в ході бойових дій. Так, у [1, 2] зазначено, що навіть у складі потужних комплексів математичних моделей операцій (бойових дій) є необхідними та практично завжди використовуються так звані експрес-моделі. Основним призначенням таких моделей є проведення швидких оціночних розрахунків (без необхідності використання значного обсягу вихідних даних та обчислювального ресурсу) початкового співвідношення сил протиборчих сторін, а також прогнозування ймовірного ходу та результатів дій, що плануються. Є зрозумілим, що для таких задач використовується переважно арсенал аналітичного моделювання. Особливе місце у цьому класі займають моделі ланчестерського типу, до переваг яких можна віднести ясний фізичний зміст складових, які можуть входити у різні модифікації рівнянь (наслідком чого є можливість зрозумілим чином інтерпретувати отримані результати), оперативність отримання результатів та контрольованість проведення розрахунків. Достатньо перспективним напрямком модифікації моделей зазначеного типу (для підвищення адекватності моделей шляхом наближення опису за їх допомогою реалій бойових дій), слід вважати використання елементів імітації для урахування невизначеностей різного характеру у динамічних коефіцієнтах бойової ефективності, інтенсивності поповнення (зменшення) чисельності угруповань, а також у вигляді стохастичних складових у диференціальних рівняннях. Оскільки відомості щодо ймовірних намірів противника носитимуть, здебільшого, лише прогнозний характер, урахування

динамічних коефіцієнтів у відповідних диференціальних рівняннях можливе у вигляді розподілів величин, вигляд яких обиратиметься виходячи з наявних даних про противника або виходячи з інших, суто практичних міркувань. Є очевидним, що оперативність вирішення навіть лінійних диференціальних рівнянь у складі ланчестерських моделей досягається лише при використанні чисельних методів, урахування динамічних коефіцієнтів переводить такі рівняння до розряду нелінійних, що робить використання чисельного інтегрування єдиним шляхом отримання результатів за такими моделями. Однак, імітація впливу різного роду випадкових чинників на хід бойових дій шляхом введення стохастичних складових у рівняння ланчестерських моделей обумовлює необхідність представлення їх у формі стохастичних диференціальних рівнянь (СДР), для вирішення яких відомі та апробовані чисельні методи (типу методів Рунге-Кутти різних порядків точності, або модифікацій методу Ейлера) неефективні. Методи вирішення СДР та їх систем відрізняються від згаданих методів чисельного інтегрування, вони мають ряд особливостей, урахування яких для отримання прийнятних результатів за моделями ланчестерського типу у стохастичній постановці представляється достатньо актуальним науково-практичним завданням.

**Аналіз останніх досліджень і публікацій.** Незважаючи на те, що хрестоматійний вигляд рівнянь був запропонований (незалежно один від одного) Осіповим та Ланчестером ще на початку 20-го сторіччя, такі моделі знаходять подальший теоретичний розвиток і сьогодні, що відзначається, зокрема, у [3]. Дослідження у сфері складних військових систем, результати яких узагальнюються у приведених джерелах, показують, що модифікації ланчестерських моделей представляються достатньо ефективним інструментом їх якісного аналізу та виявлення нових закономірностей їх розвитку при урахуванні нелінійних співвідношень між параметрами

систем. Проте, хоча у роботі [1] деталізовані способи імітації випадкових процесів у диференційних рівняннях, а у [3] відзначена перспективність такого напрямку розвитку ланчестерських моделей, як перевід їх у вигляд СДР, розгляд питань вирішення СДР та їх систем залишений поза увагою. Такі питання набувають ще більшої актуальності зважаючи на те, що, на відміну від відомих методів чисельного інтегрування, методи вирішення СДР у більшості середовищ моделювання не реалізовані, тобто вони потребуватимуть програмної реалізації з одночасною перевіркою отриманих характеристик відповідним теоретичним положенням. Зважаючи на викладене, **метою статті** є розгляд доцільності введення елементів імітації у рівняння ланчестерських моделей для урахування впливу випадкових факторів на динаміку змін чисельності сторін в ході бойових дій.

### Виклад основного матеріалу дослідження

Детальний аналіз та класифікація моделей ланчестерського типу приведений у [4]. Розглянувши та проаналізувавши більшість існуючих класичних постановок, автор [4] приходить до справедливого висновку, що такі моделі можна вважати певною мірою “ідеальними”, пристосованими для ідеальних умов. Реальні конфлікти відрізнятимуться, насамперед, за часом, тривалістю їх буде визначатися надходженням різного роду ресурсів (людських, матеріальних) та впливом інших, зокрема й випадкових чинників. Тому, фактично, у рівняннях повинен знаходитися член, впливом на який можна “регулювати” тривалість збройного конфлікту та перевагу тієї чи іншої сторони. Таке твердження знайшло відображення у наступному узагальненому запису системи рівнянь у так званій “м’якій”, нелінійній постановці:

$$\begin{cases} \frac{dx}{dt} = -c(x, y)y(t) - d(t) \\ \frac{dy}{dt} = -g(x, y)x(t) - h(t) \end{cases}, \quad (1)$$

де  $x, y$  – чисельності протиборчих угруповань;

$c, g$  – змінні коефіцієнти, що відображають інтенсивність втрат від впливу противника;

$d, h$  – вільні члени рівнянь, які відображають надходження різного роду резервів та вплив інших чинників.

Необхідно відзначити, що вільні члени рівнянь вигляду (1)  $d(t)$  та  $h(t)$  можуть відігравати роль не тільки відображення надходження (збитку) різного роду ресурсів, а і взагалі впливу зовнішнього середовища, що часто використовується у моделях популяційної динаміки. У стохастичній постановці вільні члени рівнянь ланчестерського типу, що використовуватимуться в якості експрес-моделей прогнозування ходу бойових дій, також можуть відображати важкопрогнозовані випадкові чинники, які природним чином присутні протягом їх ведення. Як відомо [6], у загальному випадку під стохастичним диференціальним рівнянням розуміється диференціальне рівняння, у якому один член або більше відображають стохастичний процес. Найбільш відомий та достатньо поширений у практиці приклад СДР – це рівняння

з членом, що описує так званий вінерівський випадковий процес (форма Ланжевена у інтерпретації Іто або Стратоновича):

$$dx = a(x)dt + b(x)dW. \quad (2)$$

Як видно з форми рівняння (2), воно складається зі звичайного (не стохастичного) диференційного рівняння та додаткової частини, що описує вінерівський шум  $(dW)$  [6].

Зазвичай вінерівський шум реалізується як  $dW = \varepsilon\sqrt{dt}$ , де  $\varepsilon = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$  та  $\varepsilon_i \sim N(0, 1)$  – нормальний розподіл з нульовим середнім та одиничною дисперсією. Хоча, взагалі, у якості випадкового процесу можна використовувати будь-який напівмартингал, практичне застосування знайшли саме вінерівський та пуассонівський процеси.

Приведення рівнянь моделей ланчестерського типу (з метою імітації впливу випадкових факторів) до стохастичної форми у приведеній вище постановці не викликає труднощів, параметри розподілів випадкових процесів (нормального або пуассонівського) при цьому обираються, як зазначалося, виходячи з наявних даних про умови ведення бойових дій. Але методи їх чисельного вирішення будуть відрізнятися від загальновідомих методів чисельного інтегрування, при цьому необхідно зазначити, що вони (у своїй більшості) є своєрідними стохастичними аналогами розкладання у ряд Тейлора. Серед таких методів порівняно простою для програмної реалізації та необхідних подальших перевірок відрізняються наступні: метод Ейлера-Мураями, методи Мільштейна та Тейлора. Їх відмінність полягає, насамперед, у збіжності, поняття якої полягає у наступному. Припустимо, що  $X(t)$  – рішення СДР на ділянці  $[0; T]$ , така ділянка розбита рівними кроками розмірності  $h$ . Нехай  $Y(t)$  – деяка дискретна апроксимація  $X(t)$ , що розрахована за допомогою модифікованого чисельного методу у певних точках розбиття ділянки  $[0; T]$ . У такому випадку вважається, що чисельний метод сильно сходиться до  $X(t)$  у момент часу  $T$ , якщо  $\lim_{h \rightarrow 0} E\{|X(t) - Y(t)\} = 0$ , де  $E$  – математичне очікування. Вважається також, що чисельний метод збігається сильно до  $X(t)$  у момент часу  $T$  з порядком  $\gamma > 0$ , якщо існує деяка константа  $C > 0$ , що не залежить від  $h$ , а також число  $\delta > 0$  таке, що  $\lim_{h \rightarrow 0} E\{|X(t) - Y(t)\} \leq Ch^\gamma$ , для усіх  $h \in (0; \delta)$ . Змістовно, поняття сильної збіжності означає, що при усіх достатньо малих значеннях кроку інтегрування  $h$  середнє значення похибки у кінцевій точці  $t=T$  буде обмежуватись величиною кроку у ступеню  $\gamma$ , множеній на деяку константу, яка не залежить від  $h$ . Чим більше значення  $\gamma$ , тим шорше збігається метод при зменшенні кроку  $h$ . Так, якщо метод матиме порядок збіжності 1, це означатиме, що при зменшенні кроку інтегрування вдвічі слід очікувати не менше ніж двократного зменшення похибки у точці  $t=T$ . Необхідно також відзначити, що у теорії СДР існує також поняття слабкої збіжності, яке у даному випадку не розглядається. Перелічені вище методи мають наступні порядки збіжності: метод Ейлера-Мураями – 1/2; метод Мільштейна – 1; метод Тейлора – 1,5.

Для наочності та в якості прикладу припустимо, що для програмної реалізації обраний метод Мільштейна, для перевірки правильності його реалізації можна використати тестове модельне рівняння вигляду:

$$dS_t = S_t (rdt + \sigma dW_t), S_0 > 0 \quad (3)$$

з аналітичним рішенням виду:

$$S_t = S_0 e^{\left(r - \frac{\sigma^2}{2}\right)t + \sigma W_t}, \quad (4)$$

де  $r, \sigma$  – постійні коефіцієнти, що ураховують випадковий характер функції виду  $S_t$ .

Тоді чисельний метод Мільштейна для вирішення СДР можна записати у вигляді:

$$S_{i+1} = S_i + S_i (rh + \sigma \Delta W_i) + \frac{1}{2} \sigma^2 S_i ((\Delta W_i)^2 - h), \quad (5)$$

$$S_0 = s_0$$

де  $\Delta W_i = N(0,1) h^{1/2}$  – приріст випадкового вінерівського процесу.

Наявність точного аналітичного рішення  $X(t)$  за (4) тестового рівняння виду (3) дає змогу перевірити програмну реалізацію обраного методу чисельного інтегрування СДР. Практична організація перевірки реалізації методу Мільштейна полягає у отриманні оцінки ( $\varepsilon$ ) математичного очікування  $E\{|X(t) - Y(t)|\}$  як:

$$\varepsilon = \frac{1}{nPaths} \sum_{k=1}^{nPaths} \{|X^k(T) - Y^k(T)|\} \quad (6)$$

де  $nPaths$  – кількість траєкторій, отриманих для точного  $X^k(t)$  та приблизного чисельного  $Y^k(t)$  рішення відповідно (зазвичай, величина  $nPaths$  обирається достатньо великою, не меншою за 100 траєкторій).

Після упевнення у правильності реалізації обраного методу вирішення СДР та його відповідності теоретичним характеристикам збіжності, отриману реалізацію можна використати для вирішення, наприклад, такого вигляду ланчестерської моделі з урахуванням поповнення чисельності сторін в ході бойових дій:

$$\begin{aligned} \frac{dx}{dt} &= -\lambda_2 y + \mu_1 (N_1 - x), \quad x(0) = N_1 \\ \frac{dy}{dt} &= -\lambda_1 x + \mu_2 (N_2 - y), \quad y(0) = N_2 \end{aligned} \quad (7)$$

де  $N_{1,2}$  – початкові чисельності протидіючих угруповань;

$\lambda_{1,2}$  – інтенсивності вражаючої дії бойових одиниць сторін;

$\mu_{1,2}$  – інтенсивності відновлення чисельності угруповань.

При цьому доцільно спочатку привести вигляд динаміки системи (7), що вирішується як детермінована методом Рунге-Кутти 4 порядку точності. Припустимо також, що параметр  $\mu_1$  змінюється ступінчастим чином на протязі 2,5 одиниць часу (імітується введення в бій резервів у визначені моменти часу, рис. 1), сторона  $y$  свою чисельність протягом бою не поповнює ( $\mu_2 = 0$ ). Відносно доволіно взятих початкових умов, за яких сторона  $y$  втричі перевищує сторону  $x$  за початковою чисельністю, значення параметрів та динаміка системи (7) за детермінованою моделлю графічно відображається так, як показано на рис. 2.

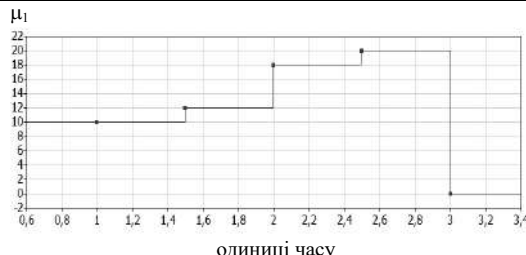


Рис. 1. Характер змін параметру  $\mu_1$

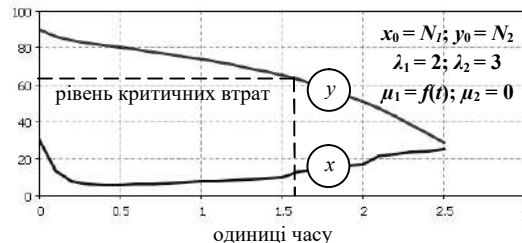


Рис. 2. Динаміка змін чисельності сторін, розрахована за детермінованою моделлю

На рис. 3 показана аналогічна динаміка змін чисельності сторін, але розрахована вже за стохастичною моделлю (для ідентичних умов).

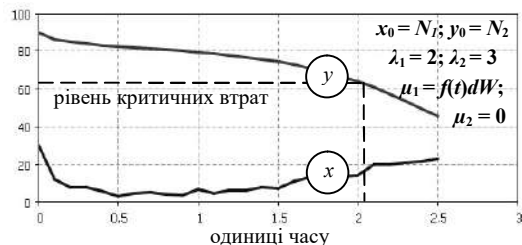


Рис. 3. Динаміка змін чисельності сторін, розрахована за стохастичною моделлю

Як видно з рис. 2 та 3, негативний вплив випадкових чинників може суттєво відзначитися на динаміці змін чисельності сторін в ході бойових дій. Припускаючи (для прикладу) що мова йде про моделювання дій тактичного рівня на протязі 2,5 годин бою (сторона  $y$ , маючи трикратну перевагу, наступає, сторона  $x$  обороняється;  $N_1=30, N_2=90$ ), а також вважаючи, що критичними для противника втратами, після яких він відмовляється від продовження дій, є втрати 30 % початкової чисельності, можна відзначити наступне. При використанні детермінованої ланчестерської моделі за заданих умов вважатиметься, що противник відмовиться від продовження дій після приблизно 1,5 годин бою. При використанні стохастичної моделі, що імітує вплив важкоформалізуємих чинників (якими можуть бути умови місцевості, пора року або погодні умови, морально-психологічний стан військ тощо), інтенсивність надходження резервів до сторони  $x$  відрізнятиметься від такої ж інтенсивності у детермінованій (дещо ідеалізованій) моделі. Це відповідним чином відображається на втратах сторони  $y$  та, як наслідок, критичній рівень втрат цієї стороною досягатиметься лише після 2 годин бою. Тобто, при коректному описі значених вище чинників для імітації їх впливу стохастичний вигляд рівнянь ланчестерських моделей можна вважати більш наближеним до реалій бойових дій. Інакше кажучи, представлення рівнянь ланчестерських моделей у стохастичній формі та

урахування всіх особливостей їх чисельного вирішення має на меті розширення можливостей моделей зазначеного типу щодо опису бойових дій, та, у кінцевому випадку, підвищення їх адекватності.

### Висновки й перспективи подальших досліджень

Моделі ланчестерського типу та їх численні модифікації залишаються достатньо ефективним інструментом якісного аналізу та виявлення нових закономірностей динамічних військових систем при урахуванні нелінійних співвідношень між їх параметрами. Одним з напрямків розвитку моделей зазначеного типу є урахування (імітація) впливу важкопрогнозованих випадкових факторів на динаміку змін чисельності протиборчих сторін. Це дозволить наблизити такі моделі до реалій

бойових дій та сприятиме підвищенню їх адекватності, але потребуватиме приведення диференціальних рівнянь моделей до стохастичного виду. Такий вид рівнянь визначає необхідність залучення для їх вирішення спеціальних чисельних методів, кожен з яких відрізняється за своїми характеристиками, насамперед – за збіжністю результатів чисельного інтегрування.

Важливим питанням при використанні рівнянь ланчестерського типу з імітацією впливу випадкових факторів на динаміку бойових дій залишається питання обґрунтованого вибору виду та параметрів розподілу випадкових величин, суттєвих для урахування в моделі. Таке питання потребуватиме детальнішого розгляду і складає перспективу подальших досліджень у окресленому в статті напрямку.

### Література

1. Горевич Б.Н. Применение элементов имитации в дифференциальных моделях военных действий / Б.Н. Горевич // Вооружение и экономика. – М., 2010. – № 2(10). – С. 31-41.  
2. Буравлев А.И. Дифференциальное уравнение для количественного соотношения численностей противоборствующих сторон / А.И. Буравлев // Вооружение и экономика. – М., 2009. – № 4(8). – С. 4-8.  
3. Новиков Д.А. Иерархические модели военных действий / Д.А. Новиков // Управление большими системами: сб. трудов. – М., 2012. –

Вып. 37. – С. 25-62.  
4. Митюков Н.В. К вопросу о типологии ланчестерских моделей / Н.В. Митюков // Круг идей: междисциплинарные подходы в исторической информатике. – М., 2008. – С. 375-399.  
5. Чуев В.Ю. Модели двусторонних боевых действий многочисленных группировок / В.Ю. Чуев, И.В. Дубоград // Математическое моделирование и численные методы. 2016. № 9. С. 89-104.  
6. Кузнецов Д.Ф. Стохастические дифференциальные уравнения: теория и практика численного решения / Д.Ф. Кузнецов. СПб, 2010.

## ЭЛЕМЕНТЫ ИМИТАЦИИ В УРАВНЕНИЯХ МОДЕЛЕЙ ЛАНЧЕСТЕРСКОГО ТИПА

*Александр Александрович Машкин (кандидат технических наук, старший научный сотрудник)*

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

*В статье приведен краткий обзор возможной сферы применения модификаций моделей ланчестерского типа, а также рассмотрены некоторые особенности использования элементов имитации и численного решения дифференциальных уравнений таких моделей в стохастической постановке. Интерес к моделям ланчестерского типа, который прослеживается по публикациям в тематических периодических изданиях, свидетельствует о действенности подобного аппарата для решения вопросов оперативного прогнозирования изменений в численности противостоящих группировок в ходе боевых действий. Стохастическая постановка позволяет определенным образом имитировать влияние случайных факторов и учитывать элементы неопределенности, которые оказывают влияние на динамику изменения численности противостоящих группировок, и которые в той или иной степени присутствуют в любых боевых действиях. В отличие от детерминированных моделей, стохастические модели требуют использования специальных численных методов, выбор конкретного из них может быть обоснован на требованиях к степени их сходимости на интервале интегрирования. Оценка сходимости может служить также для проверки правильности программной реализации выбранного метода. В статье рассмотрен сравнительный пример использования метода Мильштейна для численного решения дифференциальных уравнений ланчестерской модели в стохастической постановке.*

*Ключевые слова:* имитация в ланчестерских моделях; стохастические дифференциальные уравнения; методы численного решения; сходимость метода.

## IMITATION ELEMENTS IN THE LANCHESTER MODEL EQUATIONS

*Olexander Mashkin (Candidate of Technical Sciences, Senior Researcher)*

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

*The article gives a brief overview of the possible scope of application of modifications of the Lanchester type models, and also considers some features of the use of simulation elements and numerical solution of differential equations of such models in stochastic formulation. The interest to the models of the Lanchester type, which is traced by the publications in the thematic periodicals, testifies to the effectiveness of such apparatus for solving the problems of operational forecasting of changes in the number of opposing groups during the combat operations. Stochastic formulation allows to simulate in a certain way the influence of random factors and to take into account the elements of uncertainty that influence the dynamics of changes in the number of opposing factions, and which to some extent are present in any combat operations. In contrast to deterministic models, stochastic models require the use of special numerical methods, the choice of a particular model can be justified by the requirements for the degree of their convergence on the integration interval. Evaluation of the convergence can also serve to verify the correctness of the software implementation of the selected method. The article considers a comparative example of using the Milstein method for numerical solution of the Lanchester model differential equations in stochastic formulation.*

*Keywords:* simulations in Lanchester models; stochastic differential equations; numerical solution methods; convergence of the method.

*Сергій Григорович Вдовенко**Юрій Григорович Даник (доктор технічних наук, професор)**Олександр Юрійович Пермяков (доктор технічних наук, професор)**Національний університет оборони України імені Івана Черняхівського, Київ, Україна*

## ДОСВІД РОЗВИТКУ СИСТЕМ КІБЕРБЕЗПЕКИ ТА КІБЕРОБОРОНИ ПРОВІДНИХ КРАЇН СВІТУ

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

*Більше 60 країн світу, міжнародні (СЄ) та військово-політичні союзи (НАТО), міжнародні безпекові організації (ОБСЄ) зосереджують значні зусилля щодо забезпечення спроможностей зі своєчасного виявлення, запобігання, нейтралізації і ліквідації загроз в кіберпросторі, зокрема у сфері оборони.*

*В статті представлені результати: здійснення аналізу існуючих систем кібербезпеки і кібероборони провідних країн світу в контексті можливості та доцільності впровадження їх досвіду в Україні; здійснення аналізу передумов, існуючого стану та проблемних питань формування систем кібербезпеки та кібероборони в Україні, а також потрібного рівня їх всебічного забезпечення; здійснення розробки основних теоретичних та прикладних положень формування систем кібербезпеки та кібероборони в Україні.*

***Ключові слова:** кібербезпека; кібероборона; кіберпростір; система кібербезпеки; система кібероборони; кіберзагроза; кіберзахист; суб'єкти кібербезпеки; суб'єкти кібероборони; об'єкти критичної інфраструктури.*

### Вступ

**Постановка проблеми.** В сучасному світі питання кібербезпеки та кібероборони стали найбільш актуальними й разом з тим найбільш проблемними в забезпеченні національної безпеки і оборони практично для всіх держав світу. На даний час інформаційні та кібер-фактори стають системоутворюючими у сучасних воєнних (гібридних, проксі- та інших) конфліктах та збройній боротьбі у всіх її проявах. Але, комплексних та системних досліджень з цих питань проведено недостатньо. І це особливо проявляється в умовах криз (як, наприклад, при проведенні АТО (ООС), сьогодишньої пандемії COVID-19 тощо), коли кількість кібератак та кіберінцидентів значно зростає.

**Аналіз останніх досліджень і публікацій.** Концептуальні проблемні питання щодо загроз національній безпеці, зокрема у сфері інформаційної та кібербезпеки, окремі засади протидії кіберзлочинності та боротьби з кібертероризмом, управління кібербезпекою, а також загальної теорії кібербезпеки досліджували О.Баранов, В.Бурячок, Ю.Грицюк, Р.Гришук, Ю.Даник, Д.Дубов, Р.Лук'янчук, С.Мельник, В.Шеломенцев, В.Шпачук, М.Яцишин та інші. У

вітчизняних фахових виданнях проблемам кібероборони, порівняно з провідними країнами світу, приділяється вкрай незначна увага та лише окремими дослідниками [1-3].

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

### Виклад основного матеріалу дослідження

Поняття “кібернетика” (κυβερνητική – грец.) з'явилося в стародавній Греції, як похідне від слова “κυβερнетес” (κυβερνήτης – грец.), що означає “керманіч”. З цим словом пов'язана етимологія інших слів, що широко вживаються у багатьох мовах світу. Так, давні римляни перетворили його на “губернатор” (*gubernator*), англійці – на “уряд” (*government*), в сучасній українській мові це – “керівник”.

В давнину під кібернетикою розуміли “мистецтво управління”. Древньогрецький

філософ Платон у своїх творах кібернетику визначає, як мистецтво управління кораблем, або колісницею, а також як мистецтво правити людьми. Відомий французький вчений-фізик А.Ампер (André-Marie Ampère) в першій частині своєї праці “Досвід про філософію наук, або Аналітичний виклад природної класифікації всіх людських знань” у 1834 р. зазначив кібернетику як політичну науку про управління державою (народом), яка допомагає урядові вирішувати конкретні завдання з управління державою і забезпечує досягнення при цьому миру для держави та процвітання для народу. У другій частині роботи, опублікованої після його смерті в 1843 р., він визначив кібернетику як мистецтво управління взагалі, управління відносинами між народами зокрема. Роль кібернетики в політиці порівняна ним зі значенням стратегії в військовому мистецтві, з тією відмінністю, що перша націлена на збереження миру між народами.

Початок розвитку сучасної кібернетики, як самостійного наукового напрямку, відносять до 1948 р., коли Норберт Вінер (Norbert Wiener) опублікував роботу “Кібернетика, або управління і зв'язок у тварині і машині”, в якій узагальнив закономірності, притаманні системам управління різної природи (біологічних, технічних, соціальних) та визначив, що кібернетика це наука про загальні закономірності процесів управління і передачі інформації в живих організмах, суспільстві та машинах. Пізніше, у 1954 р., у книзі “Кібернетика й суспільство” питання управління в соціальних системах ним були розглянуті більш докладно.

У цей же період, у 1945 р., Клод Шеннон (Claude Elwood Shannon) виступає в Конгресі США із секретною доповіддю “Теорія зв'язку в секретних системах”, яка стала точкою відліку для самостійної науки – криптологія. Доповідь була розсекречена у 1949 р. та видана у вигляді монографії разом з роботою “Математична теорія зв'язку”, в якій була доведена теорема відліків, або теорема Віттакера – Найквіста – Шеннона – Котельникова. Теорема незалежно була доведена ще у 1933 р. радянським вченим В.Котельниковим у роботі “Щодо перепускної спроможності етеру та дроту в електровз'язку”, яка тоді ж була представлена Генеральному штабу РСЧА у вигляді секретної доповіді.

У грудні 1949 р. Джон фон Нейман (John von Neumann) читає в Іллінойському університеті серію лекцій “Теорія і організація складних автоматів”, матеріали яких та ряду інших лекцій стали основою теорії самовідтворення автоматів.

У 1955 р. опублікована стаття С.Соболева, А.Кітова, О.Ляпунова “Основні риси кібернетики”. В той же час публікуються дослідження В.Глушкова, які разом склали основи методології сучасної кібернетики, а надалі й кібербезпеки, як галузі знань про забезпечення захищеності процесів управління в усіх сферах (технічній, соціальній, соціотехнічній, економічній тощо) від

різноманітних кіберзагроз різної природи та для забезпечення їх ефективності.

Опублікована у 1975 р. робота У.Діффі, (W. Diffie) та Э. Хеллмена (A.Hellman) “Захищеність та імітостійкість. Введення у криптографію” відкрила еру відкритої криптографії та змінило інформаційну структуру суспільства. З'явилася реальна можливість перенести у кіберпростір ряд соціально значущих, в тому числі і соціоуправлінських функцій, заощаджуючи час та кошти, а також мінімізуючи корупційну складову.

У 2016 р. українськими вченими І.Горбенко, О.Замулою та Є.Семенко запропоновано визначення криптографічного дискретного сигналу (КДС), сформульовано в загальному вигляді і вирішено задачу синтезу й аналізу КДС [4,5]. Це значною мірою може вплинути на забезпечення захисту військових кіберфізичних систем (КФС).

Питання та передумови виникнення напрямів кібербезпеки та кібероборони в тому чи іншому контексті пов'язані із появою та розвитком радіотехніки і радіоелектроніки, електронної техніки і технічних засобів шифрування та криптоаналізу, обчислювальної техніки і інформатики, кібернетики, теорії зв'язку та інформації, стрімким розвитком кібернетичних, інформаційно-телекомунікаційних систем та їх впровадженням в усі галузі й сфери людської діяльності [6,7].

Однією з перших країн, яка на державному рівні означила кібернетичну безпеку як окремий вид безпеки, були США. У лютому 2003 р. у США була оприлюднена “Національна стратегія щодо забезпечення безпеки кіберпростору” (National Strategy to Secure Cyberspace), в якій були визначені об'єкти критичної кібернетичної інфраструктури, що підлягають кіберзахисту, а саме: державні та приватні установи різних галузей господарства, промисловості, уряду, оборонного комплексу, телекомунікацій, енергетики, транспорту, банківської справи та фінансового сектору, хімічної промисловості та виробництва небезпечних речовин, судноплавства тощо (рис. 1).

Зокрема, у стратегії було відмічено, що усі вони об'єднані у рамках одного простору - кібернетичного, якій складається із сотень тисяч об'єднаних між собою комп'ютерів, серверів, маршрутизаторів, комутаторів, волоконно-оптичних кабелів, інших електронних систем і пристроїв, які забезпечують роботу об'єктів критичної кібернетичної інфраструктури. Задачею кібербезпеки у рамках цієї стратегії було визначено забезпечення безпеки кіберпростору за рахунок координації цілеспрямованих зусиль уряду та громадян.

Вперше у міжнародний обіг термін кібербезпека офіційно було введено на засіданні підготовчого комітету Всесвітньої зустрічі на вищому рівні з питань побудови інформаційного



суспільства у лютому 2003 р. у Женеві. У першому наближенні під кібербезпекою розумілися питання, пов'язані з проблемами забезпечення безпеки даних та захисту інформації в інформаційному суспільстві, а також проблема недоторканості приватного життя. Але, до того часу вже стали реаліями життя дії в електромагнітному спектрі випромінювання з метою передачі та отримання інформації і протидії цим процесам, соціокібернетичні дії в кіберпросторі та через кіберпростір.



Рис.1. Сфери життєдіяльності що підлягають кіберзахисту та кіберобороні.

Для формування науково обґрунтованого підходу щодо визначення напрямків розвитку воєнної, воєнно-технічної, воєнно-наукової, воєнно-економічної, воєнно-дипломатичної політики держави у сфері кібероборони, стратегії кібероборони тощо, слід згадати декілька етапів розвитку окремих питань управління у воєнній сфері, та деяких інших аспектів, що з точки зору воєнно-історичного аналізу впливають на досягнення мети статті.

В усіх без виключення війнах та військових конфліктах була, є і буде присутньою інформаційна складова. З метою приховування своїх намірів та дій, а також для взяття під контроль процесів управління населенням та силами протидіючої сторони використовувалися притаманні для свого часу методи, комунікації та засоби. Питання досягнення успіху за рахунок інформаційних дій свого часу розглядалися на теоретичному рівні Сунь-Цзи, Карлом фон Клаузевіцем (Carl Philipp Gottlieb von Clausewitz), Лідделлом Гарттом (Sir Basil Henry Liddell Hart), який в своїй роботі [8] аналізує досвід попередніх поколінь в досягненні мети війни та робить висновок, що дійсною метою війни є створення вигідної стратегічної обстановки яка забезпечить

перемогу. У 1996 р. у військовій доктрині США “Concept Force XXI” вперше в світі на законодавчому рівні було визнано необхідність захисту кіберпростору. До цього моменту де-юре мова йшла лише щодо інформаційної безпеки. Але, де-факто, на практиці такі питання фрагментарно та ситуативно вирішувалися від початку практичного застосування радіохвиль, а щодо криптографії – значно раніше.

Історію розвитку та еволюції поглядів людства на кіберінформаційні аспекти управління військами, бойовими діями та війною умовно можна поділити на декілька етапів.

**I етап:** Початок – перша третина ХХ сторіччя. Використання електронних засобів для передачі інформації та здійснення інформаційних впливів на широкі маси населення стало можливим з винаходом радіо (1896, 1897 р.р., Олександр Попов, Гульєльмо Марконі (Guglielmo Marconi)). Початок застосування електронних засобів для порушення роботи засобів зв'язку та отримання інформації про противника, зафіксовано невдовзі після винаходу радіо (1904-1905. Російсько-Японська війна), що надало поштовх розвитку напрямків радіорозвідки, радіоподавлення (РЕР, РЕБ) та заборони застосування засобів радіовипромінювання без кріптозахисту інформації, якою обмінювалися. Необхідність дотримання скритності управління військами при масовому використанні засобів зв'язку (1914-18-ий роки, I світова війна та 1920-30-ті роки), призвела до стрімкого розвитку криптографії та криптоаналізу, що згодом поєдналися в єдину науку – криптологія.

З врахуванням висновків з теорії Джуліо Дуе (Giulio Douhet), щодо панування в повітрі, та розвитку засобів повітряного, нападу, формуються військово-повітряні та протиповітряні сили держав, як окремі види збройних сил, військово-повітряні та протиповітряні компоненти видів збройних сил, як роди військ, з відповідними командуваннями, системами управління та забезпечення бойового функціонування. Для їх ефективних дій формуються системи повітряного спостереження, оповіщення та зв'язку – прообраз сучасних систем С<sup>N</sup>X...X (наприклад, C4ISR – Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance).

**II етап:** Друга третина ХХ сторіччя. В ході та після II Світової війни, що мала характер “війни моторів”, на озброєння приймаються атомна зброя, засоби масового ураження, високотехнологічні засоби їх доставки (літаки, гелікоптери, ракети, атомні підводні човни). З'являється можливість масового застосування радіо та телебачення для пропаганди (масовий вплив) А для розвідувальних операцій й управління військами держав та коаліцій – радіозасобів, засобів радіолокації, радіорозвідки, дезінформації, електромеханічних та електронних пристроїв для криптографічного захисту інформації та криптоаналізу (прообраз сучасних комп'ютерів). Виникли та отримали

розвиток нові напрямки науки: теорія зв'язку та інформації, криптологія, кібернетика.

Для боротьби з засобами військово-повітряного, а далі і ракетно-ядерного нападу, які набули стратегічного значення, формується протиповітряна оборона держав, як окремий вид збройних сил, або складова частина ВПС (в деяких державах), компоненти ППО інших видів збройних сил, а далі і війська ракетно-космічної оборони (РКО) з компонентами попередження про ракетний напад та протиракетної оборони, контролю космічного простору та протикосмічної оборони з відповідними командуваннями, системами управління військами і зброєю та забезпечення їх бойового функціонування системами з високим рівнем автоматизації. В них вперше в збройних силах комплексно впроваджуються складні системи автоматизації (автоматизовані системи управління - АСУ), технічні (електронні) системи і комплекси розвідки, наземного, повітряного та космічного базування, об'єднані в єдину систему, системи передачі даних та обміну інформацією, кіберінформаційні (кібернетичні) системи та системи підтримки прийняття рішень. Утворюються та розвиваються стратегічні ядерні сили, у вигляді ядерної тріади з відповідними командуваннями, системами управління та забезпечення бойового функціонування. Ступень автоматизації та інтеграції автоматизованих систем управління ядерними силами РВСП, ВПС, ВМС, РКО на наступному III етапі буде досягнута рівня майже 100%.

**III етап:** кінець 60-их середина 90-тих років XX сторіччя. Стрімкий розвиток електроніки, комп'ютеризація, інтеграція систем управління до моделей C2 та C3I (Command, Control, Communication, Intelligence), виконання космічних програм призвели до:

появи космічних систем суто воєнного призначення та застосування їх з метою моніторингу земної поверхні, ведення розвідки, телекомунікації, геоінформаційного та навігаційного забезпечення, управління високоточною зброєю;

формування концепції мережецентричних війн (дій), проксі та "заколот" війн, так званих 4GW війн (за західною класифікацією, 1989 рік);

визнання можливості застосування інформаційної, психологічної та когнітивної зброї.

Особливістю цього етапу стало масове використання реалізованих передових військових технологій для забезпечення потреб суспільства. Як приклад, можна привести Інтернет, мобільний зв'язок, космічні та інформаційні технології. В свою чергу, це підвищило можливості розвідки (OSINT) за рахунок багатократного збільшення відкритих джерел та засобів їх аналізу.

Космос де-факто визнано четвертою сферою ведення бойових дій, хоча міжнародна правова заборона на мілітаризацію космосу продовжує діяти. В окремих державах (США, колишньому

СРСР), вже де-юре формуються та розвиваються військово-космічні сили з відповідними командуваннями, системами управління та забезпечення бойового функціонування з повною інтеграцією їх систем управління. В інших державах світу, наприклад КНР, це відбулося пізніше, умовно на IV етапі.

**IV етап:** Кінець XX сторіччя. Потужності і можливості кіберінформаційних (кібер-) систем стрімко зросли, відбувся якісний стрибок у швидкодії і продуктивності електронних засобів та обсягів інформації, що обробляється, зберігається та передається. Що, одночасно створило безліч нових вразливостей в системах управління (в тому числі і в оборонній сфері), тобто, кібервразливостей, і дозволило практично розглядати перехід до принципу функціонального ураження, як безпекової і оборонної складових держави так і їх окремих елементів. В той же час, технічні засоби отримання (розвідки), обробки та передачі інформації, управління і наведення засобів впливу, забезпечили ефективне застосування сил та засобів збройної боротьби відповідно до задачі не лише на стратегічному та оперативному рівнях, але й на тактичному [9].

Можливості таких систем, в наслідок посилення науково-технічних, виробничо-технологічних та фінансових спроможностей держав дозволяють створювати бойові підрозділи нового типу, які призначені для нанесення ураження противнику не лише в кінетичний (вогневого ураження) спосіб, але й в енергетичний (електронний) та інформаційно-когнітивний та широкого застосування, в тому числі групового і комплексного, робототехнічних засобів повітряного, наземного та морського (надводного і підводного) базування.

Проникнення інформаційних технологій в усі сфери життя людини та суспільства дозволило розглядати інформаційну зброю, як зброю першого удару. Згідно концепції Уордена-Бойда (John Ashley Warden III, John Boyd) в "операціях на основі ефектів" (ЕВО – Effect-based-Operations), що ставили за мету системні порушення управління та функціонування держав противника до кризового рівня (рис.2), в якості цілей для ураження або взяття під контроль стали розглядатися не лише збройні сили, їх системи управління, інфраструктура та комунікації, але й об'єкти економіки, населення і керівництво держав протиборчої сторони (рис.1) [10,11]. Формується функціональна модель бойового управління силами та засобами, що мають нові бойові спроможності. Це обумовило необхідність захисту вищезазначених об'єктів (рис.1) на новому рівні, складність та масштабність завдань якого дозволить розпочати його виконання лише на наступному V етапі.

**V етап.** Початок XXI сторіччя. Нове неймовірно стрімке зростання у розвитку можливостей ІТ-технологій в цілому та особливо кіберсистем щодо обробки великих обсягів даних

та швидкодії, глобальна комп'ютеризація всіх областей існування та функціонування людини та суспільства призвели до створення інтернету речей (IoT), теле та кібермедицини, а у війсьній сфері високо інтегрованих мережецентричних систем управління війсьними діями (Network-centric Warfare, NCW), або C5ISR (Command, Control, Communication, Computers, Combat System, Intelligence, Surveillance, Reconnaissance) [12,13], кіберзброї, когнітивної та консцієнтальної (руйнуючої свідомість) зброї.

Відбулося визнання кіберпростору п'ятою сферою ведення бойових дій [14,15].

У більш ніж 60 країнах світу формуються кібервійська (кіберсили) з відповідними командуваннями, системами управління та забезпечення бойового функціонування. Базою та технічною основою цих систем є безпосередньо кіберсистеми. Сфера їх бойового застосування – кіберпростір. Подальший розвиток кіберсистем

пов'язаний із технологіями збору і обробки великих масивів даних та обміну ними, IoT, глобальною роботизацією та штучним інтелектом.

Суттєво розширюється комплексне застосування різноманітної кіберзброї проти кіберфізичних та інших вразливих до неї систем, сферою діяльності яких є кіберпростір, поєднаний з іншими чотирма природними фізичними просторами.

Кіберфізична система (КФС – Cyber Physical system, CPS) – система, яка інтегрує обчислювальні, комунікаційні та керуючі технології для регулювання діяльності фізичних об'єктів під контролем фізичних осіб. До КФС відносять, наприклад, системи управління різного призначення, зокрема енергетикою, транспортом, робототехнічні системи, самокеровані літальні апарати, безпілотні автомобільні системи, бойові кораблі та підводні човни, Інтернет речей тощо [16].

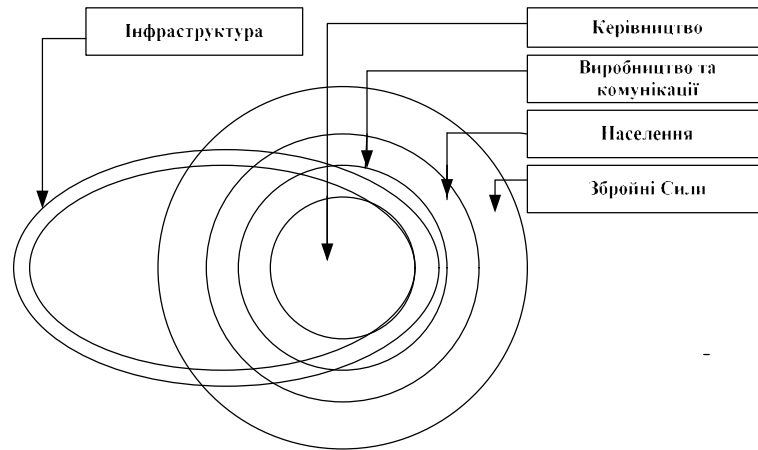


Рис. 2. Модифіковані кільця Уордена (Цілі ЕВО – атак)

Нездатність захистити ці системи від деструктивних впливів, зокрема кібератак, може мати катастрофічні наслідки [17,18]. З метою підвищення рівня захищеності своїх кіберфізичних систем, а також збільшення рівня ефективності впливу на кіберфізичні системи противника, провідні країни світу створюють науково-дослідні установи, як то Лабораторія кіберфізичних систем Академії ВМС США [19].

Особливістю кібероборони є необхідність захисту кіберсистем об'єктів критичної інфраструктури свого сектору національної безпеки та оборони, військового управління, комплексів озброєння та військової техніки, а також досягнення необхідних спроможностей деструктивного впливу на кіберфізичні та кіберсистеми противника (порушення функціонування, взяття під свій контроль та управління, фізичне знищення тощо). Особливого значення в цьому контексті набувають питання застосування робототехнічних комплексів. Можливість порушення функціонування кіберсистем робототехнічних комплексів (РТК) потребує розвитку засобів і способів їх надійного

захисту від подібних впливів, а також засобів і способів моніторингу та впливу на РТК противника та боротьби з ними шляхом некінетичного (ЕМ, енергетичного, програмного тощо) впливу на Hard and Soft Wear їх кіберсистем.

Нижченаведені приклади свідчать про об'єктивність, перспективність та незворотність зазначеного.

У кінці березня 2020 р. Космічні сили США прийняли на озброєння систему спостереження за супутниками Space Fence («Космічний паркан»). Для боротьби з ворожими безпілотниками США розміщують на закордонних базах лазерні системи боротьби з БПЛА HELWS (High-Energy Laser Weapon System) з багато спектральними системами наведення, електромагнітні системи THOR та імпульсні системи PHASER. HELWS може робити кілька десятків пострілів на одному заряді та відрізняється підвищеною точністю. PHASER здатна виводити з ладу дрони за одну мікросекунду та дозволяє атакувати кілька цілей одночасно. Завдання електромагнітної системи THOR — знищення груп безпілотників. Системи

пройдуть випробування в бойових умовах на базах в Іраку і Сирії, після чого будуть розміщені на базах у США [19].

В США ведуться роботи над створенням технології виробництва великих безпілотників-носіїв, які зможуть запускати групу невеликих розвідувальних або бойових дронів. У 2017 р. успішно відбулися випробування прообразу такої системи, в ході яких з літака-носія F-18 було випущено рій зі 103 нано-дронів "Perdix" [35, 36]. В цьому ж році, на фестивалі в Гуанчжоу Китайська компанія "Ehang" продемонструвала управління з одного пульта роєм з 1000 дронів та виконання ним 6 різних тактичних завдань [19].

Для підвищення бойової ефективності піхотних підрозділів на тактичному рівні Збройні сили Великої Британії формують роботизовані взводи. На озброєнні взводу перебувають чотири вантажні роботизовані машини Mission Master-Cargo, які можуть бути як вантажними, так і бойовими й легко адаптуються під різні завдання (захист, розвідка, спостереження, вогнева підтримка, медична евакуація, зв'язок) [19].

Міністерство оборони Франції для потреб сухопутних військ закуповує багатоцільові мікророботи NERVA, які мають три модифікації. Вони здатні в будь-яких умовах вести розвідку та приховане стеження в автономному режимі, а також можуть бути використані для розмінування. Керуються за допомогою будь-якого стандартного комп'ютера, планшета чи смартфона [19].

У 2014 р. Управління військово-морських досліджень США продемонструвало можливість супроводження бойового корабля невеликим роєм безпілотних човнів. А вже у 2019 р. Військово-морський флот США замовив чотири роботизованих кораблі. В Корпусі морської піхоти будуть розформовані ряд частин авіації та вертолітних ескадрилій, зняті з озброєння танки M1 "Abrams" та більшість ствольної артилерії. Натомість на озброєння надійдуть робототехнічні засоби і реактивні системи залпового вогню [19].

Поява результатів фундаментальних та прикладних досліджень у галузях нанотехнологій, насамперед матеріалознавства, прогнозує закінчення дієвості закону Мура (Moore's law) щодо експоненціального зростання обсягів виробництва та якісних змін електронних пристроїв й систем внаслідок розвитку технологій та здешевлення виробництва. Цей емпіричний закон був сформульований Гордоном Муром (Moore, Gordon) ще у 1965 р., та їм же ж, виходячи з атомарної природи речовин та постійної величини швидкості світла у вакуумі, у 2003-2007 р.р. спростований та уточнений [20-22]. У 2016 р. дослідники Массачусетського технологічного інституту (Massachusetts Institute of Technology), під керівництвом Джеффри Біча (Beach, Geoffrey), зробили відкриття щодо існування скірміонів (skyrmions) [23], віртуальних часток, електромагнітні властивості яких, дозволили створити та призведуть до масового

використання в найближчому майбутньому квантових комп'ютерів, роботизованих систем нового покоління, подальшого розвитку штучного інтелекту та постквантової криптографії. Це вже впливає та й надалі все більше буде впливати на формування політики держав у сферах кібербезпеки та кібероборони.

Основними світовими трендами розвитку інформаційних, електронних та кібер-технологій, що безпосередньо здійснюють вплив на розвиток суспільства, суспільно-політичних та суспільно-економічних відносин, можуть бути наступні:

лавиноподібне зростання кількості інформації, що обробляється, зберігається і передається;

зміна форм представлення інформації, необхідної для прийняття управлінських рішень;

ускладнення систем управління та нелінійних зв'язків і процесуальної взаємодії між складовими різнорідних процесів управління та задіяних елементів.

Сучасні високі технології змінюють процеси організації бойових дій (операцій) та методи управління ними, і тому вимагають розробки та впровадження нових концепцій та стратегій оборони, розвитку існуючих та розробки нових, які враховують досягнення інноваційних технологій, форм, способів, методів і технологій збройної боротьби в сучасних і особливо перспективних умовах, а також підготовки та перепідготовки фахівців сектору безпеки та оборони, здатних їх впроваджувати та ефективно використовувати. У сфері оборони відбувається глобальний перехід на інтегровані системи управління військами та зброєю від стратегічного до тактичного рівня, та інноваційні системи озброєння, які до 80% побудовані з високотехнологічних складових [7,24].

Це швидко веде до набуття передовими арміями світу можливості ведення мережових війн, в тому числі на тактичному рівні. В США реалізують нову версію платформи NCW у версії C6ISR, до якої додається ще одна компонента – Cyber [25]. Для ведення кібердій платформа NCW може бути розгорнута до моделі C5IEWS&IM (Command, Control, Communications, Computers, Cyber, Intelligence, Electronic Warfare, Sensors and Information Management) [7, 26].

З іншого боку інноваційний розвиток інформаційних та кібер-технологій та їх доступність у рази посилює можливість ведення не лише військовими або розвідувальними службами, але й незаконними формуваннями, злочинними та терористичними організаціями шпигунських й терористичних дій через інформаційний та кібер-простори та безпосередньо в них. Кібератаки стали більш організованими та руйнівними для державних установ, підприємств, економіки, транспорту, електроенергетики, об'єктів критичної інфраструктури. Вони можуть досягти критичного рівня, який загрожує національному і євроатлантичному процвітання, безпеці і стабільності [6,18,27]. Нові вразливості

національної критичної інфраструктури, які проявляються паралельно з бурхливим розвитком технологій, породжують нові небезпеки, загрози й ризики в інформаційному та кібер- просторах та вимагають вирішення питань щодо їх запобігання, стримування та нейтралізації. Це питання існування і майбутнього держав у сучасному світі, що перебуває напередодні нового етапу розвитку суспільства – постінформаційного.

Виходячи з цього, у держав виникає необхідність утворення ефективної системи кібербезпеки та кібероборони з функціональною спроможністю не нижче гранично необхідного рівня, не залежно від рівня їх економічного розвитку і стану та науково-технічного прогресу країни, але адекватно до рівня загроз, що притаманні світові у першій чверті ХХІ століття, а у стратегічній перспективі – до середини століття [6,28].

Аналіз теорії, практики й досвіду побудови систем і забезпечення кібербезпеки та кібероборони провідних країн світу свідчить про їх адекватність загрозам, як відомим так і прогнозованим. Кіберсили розглядаються в якості сил стримування. Державне та військове керівництво армій розвинених країн світу у відповідності до нових підходів щодо будівництва збройних сил особливу увагу приділяє формуванню та розвитку систем кібербезпеки та кібероборони, як головного фактору у досягненні воєнно-стратегічної переваги в забезпеченні національної безпеки і оборони у сучасних умовах та у перспективі.

Концепція колективної оборони НАТО передбачає розвиток та застосування всіх політичних та військових можливостей щодо запобігання, виявлення, захисту і відновлення порушень внаслідок кібератак. Йде вдосконалення процесу планування НАТО та формування Кіберкомандування Альянсу, завданням якого будуть: охоплення усіх органів НАТО централізованим кіберзахистом; вдосконалення та координація національних можливостей з кіберзахисту; інтеграція національних систем в єдину систему попередження і реагування НАТО на кіберзагрози. Це стосується також країн - партнерів [14].

Світовий досвід свідчить, що ефективне вирішення будь-якими військами задач за призначенням та забезпечення максимально повного використання потенціалу озброєння та військової техніки можливе лише за умов їх об'єднання у єдиній військово-організаційній структурі (відповідно до фізичного простору де вони діють, або озброєння, яке вони застосовують) та наявності раціональної системи управління на усіх рівнях від стратегічного до тактичного. Як приклад – на початку ХХ століття масова поява авіації, танків та засобів протиповітряної оборони гостро поставила питання щодо створення відповідних органів управління підрозділами, з'єднаннями, об'єднаннями, оснащеними цими

засобами, а також їх підготовки і всебічного забезпечення. Відомо, що до того, доки не були створені раціональні системи управління, ефективність застосування зазначених сил та засобів була вкрай низькою.

Кіберсили створюються й розвиваються в залежності від розвитку сучасної науки та технологій під впливом процесу розвитку і трансформації кіберпростору, який на відміну від природних просторів (сухопутного, морського, повітряного, космічного) не є незмінним у своїй фізичній суті. Це відбувається за рахунок поєднання в єдиній структурі, яка відповідає за кібероборону, всіх необхідних складових, відповідно до мети, завдань, доцільних форм та способів їх застосування для забезпечення кібербезпеки у воєнній сфері та реалізації різних функцій та напрямів діяльності поєднаних їх відношенням до кіберпростору. Створені в провідних країнах світу системи кібероборони включають та об'єднують військово-організаційні структури, які відповідають за: дії в комп'ютерних мережах, електромагнітному спектрі випромінювання, інформаційні та психологічні операції, організацію та застосування технічних видів розвідки, забезпечують зв'язок та криптографічний захист інформації, приймають участь у заходах введення в оману, здійснюють наукові дослідження і випробування в цих сферах та підготовку кадрів. (Рис. 3) [6,7].

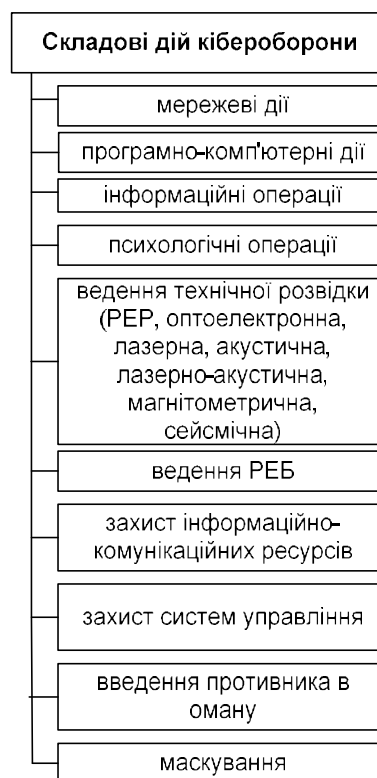


Рис. 3. Складові дії кібероборони

**США.** Система кібербезпеки США є трирівневою та ґрунтується на функціональній взаємодії державних інституцій та суб'єктів

національної економіки та приватно-державному партнерстві.

Перший, стратегічний рівень, включає:

Міністерство оборони, з підпорядкованим йому Агентством Національної Безпеки (АНБ – National Security Agency, NSA). Останнє виконує завдання в інтересах оборони, відповідає за збір та аналіз розвідувальної інформації та за захист інформаційних систем і комп'ютерних мереж, налічує близько 120000 співробітників та має річний бюджет за різними оцінками \$3,5 – 13 млрд. [19];

Міністерство внутрішньої безпеки, до складу якого входить Національне управління кібербезпеки США з річним бюджетом \$400 млн., виконує завдання із захисту національної критичної інфраструктури;

Міністерство юстиції, до складу якого входить ФБР, що займається розслідуванням кіберзлочинів в США.

На другому рівні, серед інших інституцій, Кіберкомандування США (United States Cyber Command – USCYBERCOM) та розвідувальне співтовариство.

На третьому – регіональні та локальні підрозділи кіберзахисту.

З 2018 р. в Законі про національну оборону (“National Defense Authorization Act”) для міністерства оборони США визначено завдання централізації керівництва всіма силами та засобами, які відповідають за кіберзахист, активні заходи дій в кіберпросторі та інші операції в комп'ютерних мережах, електромагнітному спектрі випромінювання, інформаційні та психологічні операції, дії в космічному просторі, дії відповідних технічних видів розвідки тощо. З 2019 р. кібербезпека (безпека кіберпростору) у США розглядається як дії, вжиті в захищеному кіберпросторі для запобігання несанкціонованому доступу, експлуатації або пошкодженню комп'ютерів, електронних систем зв'язку та інших інформаційних технологій, включаючи інформаційні технологічні платформи, а також інформацію, що міститься у них [29].

Кіберстратегія МО США визначає наступні пріоритети: підготовка простору операцій; висока готовність; ресурсне забезпечення; підготовка; партнерство. Кібервійська повинні бути спроможними контролювати ескалацію конфліктів і впливати на розвиток подій на всіх етапах конфліктів. Їх фінансування складає до \$7 млрд. на рік. [19, 30, 31].

США з 2009 р. для захисту від кіберзагроз військової інфраструктури, реалізації програм та засобів, що спроможні контролювати ескалацію конфліктів та впливати на розвиток подій на всіх етапах конфліктів, першими у світі почали формування сил кібероборони, як окремого виду збройних сил [32,33]. Кіберкомандування США було утворено на базі та фондах АНБ й управління інформаційної безпеки Повітряних Сил (Air Force Information Security Agency), шляхом об'єднання

сил і засобів (підрозділів) за ознакою їх віднесення до кіберпростору (електромагнітного спектру), перепрофілювання або створення установ (підрозділів) науки та підготовки персоналу, створення системи кіберрозвідки з підсистемою управління, силами та засобами. У 2015 р. його повноваження були значно розширені Кіберстратегією 2.0, яка з метою підвищення рівня кіберзахисту та кібероборони США передбачала створення кіберсил, підпорядкованих окремому командуванню [34]. На сьогодні Кіберкомандування та АНБ одночасно очолює одна особа. З 2018 р. Кіберкомандування виведено з підпорядкування Стратегічного командування (STRATCOM) в самостійне бойове командування з наступним його відділенням від АНБ.

Причина майбутнього розділення полягає в тому, що відповідно до законодавства США, АНБ, як розвідувальний орган спеціального призначення, має право проводити за межами держави лише розвідувальні операції, право ведення бойових (воєнних) дій, в тому числі поза межами США – належить тільки військовим. Для забезпечення автономності ведення бойових дій проводяться заходи щодо створення спеціального Розвідувального центру кібероперацій (Cyber Warfare Intelligence Center) [19, 35,36].

Станом на кінець 2019 р. в підпорядкуванні Кіберкомандування США перебувають та виконують завдання кібероборони органи управління та військові підрозділи трьох видів Збройних Сил та одного роду військ, що налічують майже 50000 військовослужбовців та працівників (2,5% від загальної чисельності ЗС США). Діяльність Кіберкомандування США забезпечується потужною освітньо-науковою базою. Дослідження з питань кібербезпеки та кібероборони та підготовка персоналу здійснюються в 5 науково-дослідних установах та 2 навчально-тренувальних центрах [19].

**Кіберкомандування Армії США** (Army Cyber Units), або Командування 2 Армії – 19000 осіб. Йому підпорядковані військово-організаційні структури із завданнями:

1) Командування технологічних мереж Армії США (United States Army Network Enterprise Technology Command - NETCOM), або 9 командування зв'язку Армії США (командувань зв'язку територіальних – 3, бригад зв'язку територіальних - 7; бригада кіберзахисту) – веде глобальні операції в кіберпросторі та здійснює активну кібероборону від дій противника. Розгортає Центр управління інформаційних операцій Армії (AIOC), який забезпечує єдину оперативну підтримку планування інформаційних операцій Армії, розвідувальний аналіз та технічну допомогу розгорнутим командам інформаційних операцій (Information Operations Command, IO CMD), іншим військово-організаційним структурам, установам та відомствам, які потребують підтримки. Жодна інша структура

Армії не здійснює подібних завдань в кібер-інформаційному середовищі.

2) 1-ше Командування інформаційних операцій (1st Information Operations Command (Land) - 1st IO CMD) (штаб, штабні елементи, бригада військової розвідки (кібер) – 1, бригада кіберзахсту – 1, 1-й та 2-й окремі батальйони) – здійснює спеціальну підготовку фахівців та підрозділів кібербезпеки, розгортає різноманітні команди для виконання визначених завдань при підготовці та проведенні інформаційних операцій та операцій у кіберпросторі, зокрема:

команди польової підтримки інформаційних операцій (IO Field Support Teams – FST), які забезпечують узгодження та досягнення максимальної ефективності завдань інформаційних операцій та операцій в кіберпросторі при плануванні та проведенні операцій угрупованнями Армії або спільними угрупованнями;

команди оцінки вразливості (IO Vulnerability Assessment Teams – VAT), які допомагають підрозділам визначити уразливості військ та систем від впливу противника в повному спектрі інформаційних операцій та надають командуванню пропозиції щодо покращення захисту включно операційну безпеку (OPSEC), фізичну безпеку, соціальну інженерію, безпеку радіозв'язку і захищених телефонного зв'язку та електронної пошти (COMSEC), а також безпеки операцій у кіберпросторі;

елемент підтримки операційної безпеки (Operations Security Support Element - OSSE), який здійснює підготовку керівників програм та посадових осіб до управління підрозділами системи підтримки операційної безпеки, надає допомогу керівництву та командирам підрозділів системи з усіх напрямків діяльності, несе відповідальність за планування, навчання, проведення оцінок та інтеграцію системи підтримки операційної безпеки в усій Армії;

навчально-тренувальні імітаційні центри інформаційних та кібер-операцій (Information Warfare/Cyber Opposing Force – IW/Cyber OPFOR) - призначені для забезпечення імітації реалістичних, реальних, віртуальних рутинних та деструктивних масованих дій кіберсил збройних сил інших держав, насильницьких екстремістських та кримінальних кібератак та кібервпливів під час навчань й тренувань підрозділів кібербезпеки в пунктах постійної дислокації, центрах бойової підготовки та під час командно-штабних навчань;

3) Центр управління інформаційних операцій Армії (The Army Information Operations Center – AIOC) – забезпечує єдину оперативну підтримку планування інформаційних операцій Армії, розвідувальний аналіз та технічну допомогу розгорнутим командам IO CMD та іншим військовим частинам, підрозділам, установам та відомствам, які вимагають підтримки. Жодна інша організація в Армії не надає цього критичного,

унікального способу, орієнтованого на інформаційне середовище.

4) система навчальних курсів інформаційних операцій (Specialized IO training – SIOT) – курси у Форт Бельвоар, штат Вірджинія, і мобільні навчальні команди (МТТ) по всьому світу. Кожен з курсів фокусується на інтеграції інформаційних можливостей (IRCs). Навчальні курси включають: Навчальний курс IO, програми та планування (IOCAP); Фундаментальний курс інформаційних операцій (IOFC); Військовий курс підготовки планувальників введення противника в оману (MDPC); Інтегрований курс радіоелектронної боротьби (EWIC); та курс інтеграції операцій з військової інформаційної підтримки (MISOIC);

підрозділи підготовки (Mission Readiness Exercise - MRX) активної та резервної компоненти команд системи польової підтримки інформаційних операцій (IO FST), зокрема:

1 батальйон 1-го Командування IO відповідає за підготовку активної та резервної компонент бойових команд та розгортання декількох глобальних експедиційних інформаційних операцій (IO), синхронізацію інформаційних можливостей для підтримки Армії, спільних оперативних сил і окремих бойових підрозділів й команд. Він здійснює аналіз соціальних мереж та планування залучення їх можливостей для потреб Армії та об'єднаних сил, використовуючи загальнодоступну інформацію забезпечує операційну безпеку розгорнутого угруповання;

2-й батальйон 1-го Командування IO розгортає багатофункціональні команди інформаційних операцій (IO) у всьому світі, зберігаючи при цьому безпосередній і віддалений доступ до мережі та використовуючи всі можливості IO для підвищення готовності та здатності військових сил США щодо дій в інформаційному середовищі [19].

Кіберкомандування Повітряних Сил США (Air Forces Cyber), або 24 Повітряна Армія – понад 14000 військовослужбовців та працівників, що розміщені на 6 авіабазах в США та ФРН, здійснює кіберзахист мереж управління ПК, забезпечує підтримку бойових операцій ПК, приймає участь в об'єднаних (спільних) кіберопераціях. Складається з 11 органів управління (Центра операцій – 1, оперативної групи дій в кіберпросторі – 1, бойових груп мережевих операцій – 2, груп бойових комунікацій – 2, групи операцій у кіберпросторі – 1, інженерної групи забезпечення кіберпростору – 1, крила інформаційних операцій в комп'ютерних мережах – 1, крила бойового застосування кіберсистем – 1, крила зв'язку (бойових комунікацій) – 1) та 36 ескадрилей (мережевих операцій – 10, бойового зв'язку - 10, операцій в кіберпросторі – 2, інформаційних операцій – 2, розвідувальної підтримки – 1, оперативної підтримки – 1, підтримки операцій – 1, операційної підтримки - 2, підтримки бойового зв'язку – 2, інженерних – 2, підрядників – 1, випробувальної – 1, підготовки до дій в

кіберпросторі – 1), назви яких відображають сутність їх завдань [19].

Кіберкомандування ВМС (U.S. Fleet Cyber), або 10 Флот США – понад 16000 військовослужбовців і працівників дійсної служби та резерву, організованих у 27 активних та 27 резервних командувань, розміщених на 11 військово-морських базах (аеродромах) США, що формують 40 кіберкоманд, діючих по всьому світу (зокрема, Бахрейн – 2, Італія – 2, Японія – 3, Маріанські острови, Великобританія – по одній). Здійснює кіберзахист мереж управління ВМС, забезпечує підтримку бойових операцій ВМС, приймає участь в об'єднаних (спільних) кіберопераціях. Складається з:

Командування комп'ютерних мереж ВМС (Naval Network Warfare Command – NNWC) - 1, тактичних кібергруп (Cyber tactic group, CTG) – 3;

Командування кіберзахисту ВМС (Navy Cyber Defense Operations Command – NCDOC) - 1, CTG – 2;

Командування інформаційних операцій ВМС на ТВД (Navy Information Operations Command, NIOC) – 5;

6-та бойова група криптологічного забезпечення (Cryptologic Warfare Group – CWG6) у складі: 61 морський підрозділ криптологічних дій (Cryptologic Warfare Maritime Activity – CWMA); 63 підрозділ криптологічного забезпечення кіберударів (Cyber Strike Activity – CSA); 64 підрозділ криптографічного забезпечення кіберзахисту (Cyber Defense Activity – CDA). Група розгортає бойові підрозділи криптологічної підтримки операції по всьому світові – 10;

Група розробок інформаційних операцій, досліджень, розробок, випробувань та оцінок (Research and development).

Об'єднані спеціальні підрозділи (Joint Base San Antonio) [19].

Кіберкомандування Корпусу Морської Піхоти (U.S. Marine Corps Forces Cyberspace Command – MARFORCYBER) - біля 800 осіб особового складу, здійснює кіберзахист мереж управління МП, забезпечує підтримку бойових операцій МП, приймає участь в об'єднаних (спільних) кіберопераціях. Складається з Командного центру комп'ютерної безпеки корпусу МП (Network Operations Security Center) та батальйону криптографічної служби (Marine Corps Cryptologic Support Battalion). Розгортає:

оперативну кібергрупу корпусу МП (The Marine Corps Cyber Operations Group), яка здійснює збір та аналіз розвідувальної інформації, необхідної для планування виконання завдань за призначенням, збір та обмін інформацією щодо стану інцидентів в мережах, керівництво захистом мереж, реагування на загрози, вразливості та інциденти, технічне керівництво та втілення нових технологій;

бойову кібергрупу корпусу МП (The Marine Corps Cyber Warfare Group) [19].

Завданням USCYBERCOM є планування, координація, об'єднання, синхронізація і проведення заходів щодо керівництва операціями і захисту комп'ютерних мереж міністерства оборони; підготовка і здійснення повного спектру військових операцій в кіберпросторі, забезпечення свободи дій США та їх союзників в кіберпросторі та перешкоджання аналогічних дій противника. Спектр операцій Кіберкомандування США показаний на рис. 4.



Рис. 4. Операції Кіберкомандування США.

У 2019 р. США провели ряд бойових кібероперацій, зокрема проти Ірану та Росії. [19]. Активні сили складаються з майже 6200 осіб військового й цивільного персоналу (включно персонал запасних компонентів), організованих в 133 бойові команди, які досягли оперативної спроможності та активно проводять операції [19], а саме:

команди національної місії (National Mission Teams) захисту США та критичної інфраструктури від кібератак – 13 (використовують цивільних фахівців);

команди захисту пріоритетних мереж та систем (Cyber Protection Teams) - 68;

команди створення інтегрованих ефектів кіберпростору (Combat Mission Teams) для підтримки оперативних планів, операцій та бойових дій на випадок непередбачених обставин – 27;

команди (Support Teams) аналітичної та планової підтримки команд національної місії та бойової місії – 25.

Таким чином, США мають раціональну систему управління та необхідні сили і засоби об'єднані в єдину структуру відповідно до цілей, завдань і функцій для ведення всіх видів кібердій в кіберпросторі та через кіберпростір.

**ФРН.** Командування кібер- та інформаційного простору (далі ККІП), створено у 2017 році, має статус окремого виду збройних сил (ЗС). Чисельність 13700 військовослужбовців і 1500 тисячі цивільних осіб (6% від загальної



чисельності ЗС ФРН). Повна операційна готовність ККІП буде досягнута до кінця 2021 року.

ККІП організаційно складається з двох командувань ланки дивізії, кожне з яких має у своєму розпорядженні близько десяти структурних підрозділів нижчого рівня, та Центру геоінформації. Перше – реорганізоване Командування сил розвідки (КСР) відповідає за ведення РЕР і РЕБ та здійснення інформаційного і радіоелектронного впливу на противника. Друге – Командування інформаційно-технічних засобів (реорганізоване командування управління та зв'язку) відповідає за утримання і функціонування системи бойового управління та зв'язку, а також за захист інформаційних мереж від кібернетичних атак противника. Центр геоінформації бундесверу призначений для забезпечення всіх користувачів актуальними даними широкого спектру, включно: матеріали фотограмметрії, дистанційного

зондування Землі, геофізичні, геодезичні, гідрологічні, гідрографічні, океанографічні, метеорологічні, та картографічні матеріали тощо.

Створення ККІП здійснено за рахунок передачі в його розпорядження існуючих структурних підрозділів інших видів ЗС і не призвело до збільшення загальної чисельності Бундесверу. Зокрема, із Командування базових сил Бундесверу до складу ККІП передані у повному обсязі Командування стратегічної розвідки (близько 5500 осіб), Командування управління і зв'язку (понад 6000 осіб) та Центр інформаційно-психологічних операцій (близько 1000). Крім того, до складу ККІП включено частину підрозділів Федерального агентства озброєння, інформаційної техніки та експлуатації Бундесверу. Найменший підрозділ, якій відповідає за атаки, налічує лише 60 військовослужбовців. Структура ККІП ФРН показана на рис. 5.

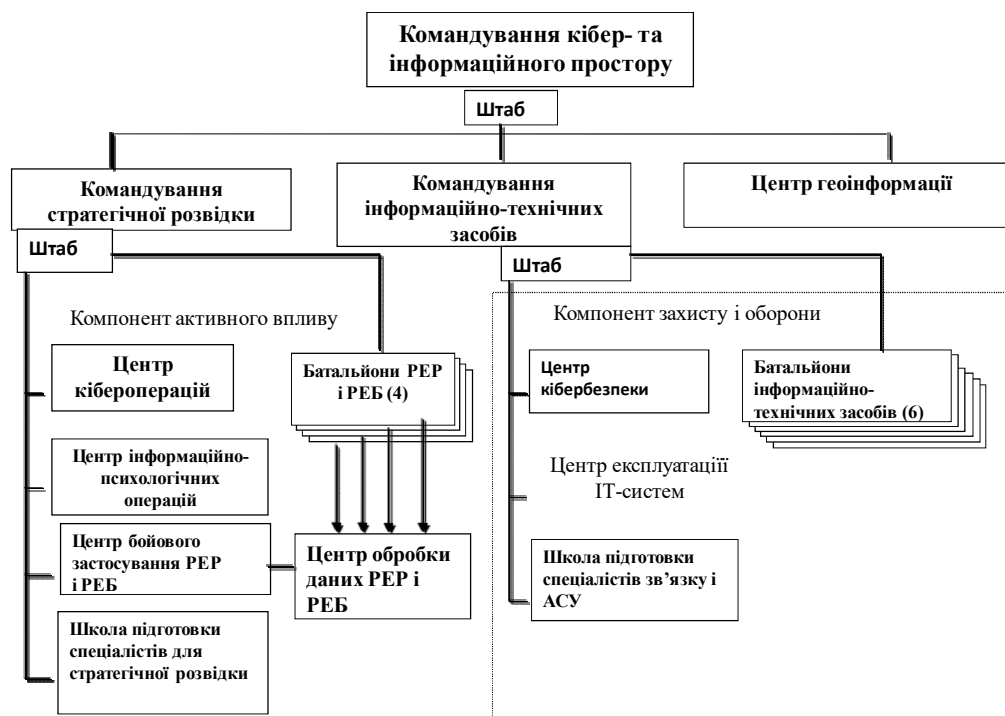


Рис. 5. Структура Командування кібер- та інформаційного простору ФРН

В університеті бундесверу в Мюнхені 11 кафедр пов'язані з обороною кіберпростору. Бюджет Дослідницького центру університету на 2019-2021 р.р. двадцять мільйонів євро [37].

**Великобританія.** Розгортання британських кібервійськ проходить згідно з ініціативи Міністерства оборони Великої Британії і Центру урядового зв'язку (GCHQ). Великобританія спланувала на розвиток кібербезпеки у 2016–2021 роках витрати у розмірі понад 3 мільярди фунтів. З них 22 млн. фунтів стерлінгів (\$27,8 млн.) - на створення Центру активних кібероперацій, який буде спільно використовуватися МО та GCHQ й забезпечувати та посилювати діяльність 77-ої бригади кібероперацій. До 2021 року кібервійська нараховуватимуть 2000 осіб, а фінансування,

становитиме понад 250 мільйонів фунтів на рік. Національний центр кібербезпеки Великої Британії щороку проводить найбільші у світі кібернавчання Locked Shields для експертів у сфері кіберзахисту [38].

**Республіка Польща.** Гарантоване безпечне функціонування в кіберпросторі визнано однією з основних стратегічних цілей безпеки держави. Військова контррозвідка (Sluzba Kontrwywiadu Wojskowego, SKW), яка підпорядкована Міністру національної оборони здійснює не тільки контррозвідувальні заходи, але й забезпечує кібербезпеку для Збройних Сил Республіки Польща. Військова розвідка (Sluzba wywiadu Wojskowego, SWW) здійснює в інтересах оборони електронну розвідку та криптоаналіз. Активно

здійснюються заходи правового, організаційного та технічного характеру щодо вдосконалення національної системи кібербезпеки та кібероборони, розробки нормативно-правової бази активної оборони в кіберпросторі.

На створення кіберсил Польща виділила 2 млрд. злотих (близько 465 млн євро). З 2019 р. розпочато формування Військ оборони кіберпростору, які у продовж кількох років мають нараховувати 1000 військовослужбовців. На основі Національного центру криптології (військово-організаційна структура підпорядкована Генеральному штабу) та Командування ІТ-мереж (структура МО) сформовано безпосередньо підпорядкований Міністерству Національної оборони РП Національний Центр кіберзахисту, до складу якого включений Інспекторат інформатики. Йому підпорядковані: Центр інформаційної підтримки Збройних Сил, Регіональні центри інформаційної підтримки – 4, до складу яких входять відділи кібербезпеки та захисту інформації; Центр інформаційної підтримки Повітряних Сил, райони інформаційної підтримки ПС – 4; Центр управління інформаційними мережами; Центр проектування інформаційних систем; група реагування інфраструктури – 4; військове бюро з регулювання й вимірювання радіочастот [39,40].

**Угорщина** створює у складі Збройних Сил Центр (Командування) кібербезпеки з підпорядкуванням йому існуючих підрозділів: Центру кібербезпеки Служби національної безпеки Угорщини, Головного центру кібербезпеки Будапештської гарнізонної бригади, Центру забезпечення захисту інформації та підтримки управління 43 полку зв'язку, а також створює для підготовки військових та цивільних фахівців силових структур країни Академію кіберзахисту, яка складається з 5 кафедр та 3 лабораторій. Центр кібербезпеки підпорядкований директорату технологій, кібер- та ІТ-захисту. В свою чергу, Директорат є військово-організаційною структурою, що входить до складу Воєнної служби національної безпеки. Чисельність Центру кібербезпеки може нараховувати до 1000 військовослужбовців [41,42].

**Естонія** відіграє провідну роль у зміцненні європейського кіберзахисту. З 2008 року у Таллінні діє Об'єднаний центр передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence), який сьогодні є флагманом європейської кібербезпеки. Центр має акредитацію НАТО. Центр налічує 20 учасників – 17 членів НАТО та 3 країни-партнери. Унікальність центру полягає в тому, що там разом працюють військові, цивільні, представники уряду. Робота центру сфокусована на трьох основних напрямках: дослідження, тренування та навчання. З 2018 р. Естонія розпочала формування кібервійськ, кількість яких складатиме 300 осіб. Набуття спроможностей

визначено на 2023 р. [43].

**РФ.** Воєнна доктрина (2014) та Доктрина інформаційної безпеки (2016) визначають можливість застосування сил інформаційних операцій (дії в кіберпросторі не відокремлюються) в інформаційній війні з метою створення системи неядерного стримування та запобігання конфліктам, для оборони, а також з метою нападу. Основну частину активних дій покладено на “добровольців”, “хактивістів” та інші “підконтрольні” умовно невійськові сили та засоби.

Війська інформаційних операцій МО РФ створені на підставі указу президента РФ у лютому 2014 року та налічують близько 1000 військовослужбовців, їх фінансування – на рівні 18 млрд руб. (\$300 млн.). Кіберкомандування ГШ ЗС РФ створено у січні 2014 року на підставі наказу МО РФ. Його основними завданням є: управління та захист воєнних комп'ютерних мереж та систем управління і зв'язку від кібертероризму та дій імовірного противника [44]. Крім військових закладів вищої освіти, підготовка висококваліфікованого військового та науково-технічного персоналу для кібер командування та військ ІО здійснюється в наукових ротах, зокрема: 6 нр Восьмого управління ГШ ЗС РФ (м. Краснодар), 3 нр Військ повітряно-космічної оборони (м. Красногорськ), нр Військово-повітряної академії ім. Жуковського та Гагаріна (м. Воронеж). Особливістю останніх є те що до них відбираються найбільш талановиті випускники, або студенти останнього року навчання профільних цивільних закладів вищої освіти, які після призову, протягом 2 років проходять дійсну строкову військову службу та одночасно здійснюють наукову діяльність. З присвоєнням першого офіцерського звання, випускники наукових рот отримують призначення у військові або оборонні науково-дослідні установи, або в конструкторські бюро оборонного призначення [45].

**Ізраїль.** На виконання п'ятирічного Плану розвитку сил оборони Ізраїлю, прийнятого у 2015 році, якій передбачає активізацію діяльності щодо відбиття кібератак та інших асиметричних загроз від недержавних та терористичних організацій регіону, для захисту життєво важливих об'єктів інфраструктури Ізраїлю створена Національна цільова кібернетична група (НЦКГ) рівня дивізії, яка є відповідальною за кібероборону. НЦКГ була утворена шляхом об'єднання в єдину організаційну структуру Національного кібернетичного штабу, що існував з 2012 р. та Національного управління з кібернетики, що діяло з 2015 р. НЦКГ очолив колишній керівник Центру шифрування та захисту інформації, що забезпечує криптографічний захист мереж ЦАХАЛу, служби внутрішньої безпеки ШАБАК, розвідки МОССАД, а також національних корпорацій. Розглядається можливість розгортання в подальшому НЦКГ у

Кіберкорпус, який стане відповідальним за оборону країни, як і інші існуючі Армійській, Військово-морській та Військово-повітряній корпуси. У 2019 р. на це реформування було виділено \$150 млн. У разі створення, Кіберкорпус має виконувати інтегровані функції електронної розвідки, протидії та захисту, які наразі виконуються органами військової розвідки трьох існуючих корпусів та командою 8200 військової розвідки, а також Управлінням командування, управління, зв'язку, інформаційних систем та розвідки (С4І) в частині, що стосується захисту від кібератак та криптографічного захисту інформації мереж воєнного призначення, а також мереж стратегічних військових концернів, таких як Ізраїльська електрична компанія, національна водна монополія "Мекорот" і телефонна компанія "Безек". Кібервійська будуть відповідати за забезпечення належного рівня оброну Ізраїлю та координацію розробок нового програмного забезпечення для Збройних Сил та ізраїльських компаній сектору високих технологій. Чисельність, яка планується – 1000 осіб [46].

**Аналіз стану кібероборони в Україні.** В Україні питання формування системи кібероборони знаходиться у стадії вирішення. Відповідно до чинного законодавства та окремих нормативно-правових актів підготовка держави до відбиття агресії у кіберпросторі (кібероборона) є одним із головних завдань, які покладаються на Міністерство оборони та Збройні Сили України. За виконання пов'язаних за змістом та простором завдань кібероборони на цей час відповідають різноманітні, різнопідпорядковані структурні підрозділи, що призводить до зростання витратності та зниження ефективності виконання цих задач. (рис. 5, 6) [47-54]. Щоб правильно визначити цілі і задачі стратегії кібероборони, необхідно спираючись на визначені функції та завдання, на основі структурно-системного підходу, здійснити чітку структурування та визначення зон відповідальності кожній складовій сектору безпеки і оборони стосовно кібербезпеки та кібероборони.

"Індекс кібер-готовності 2.0", опублікований у 2015 р. Потомакським Інститутом політичних досліджень [36] рекомендує для оцінки дієвості системи кібероборони держави та здатності Національного органу кібероборони та Збройних Сил держави щодо захисту від загроз, що йдуть від кіберпростору, використовувати наступну модель перевірки, що складається з 7 груп:

1. Наявність національної стратегії кібербезпеки.
2. Наявність структур відповідальних за інциденти, здатність їх до реагування на них.
3. Наявність правоохоронної кібер-структури та стан правоохоронної практики
4. Наявність системи обміну інформацією.
5. Наявність системи підготовки персоналу, досліджень та випробовувань.

6. Дипломатія та торгівля.

7. Оборона та наявність структур, що реагують на кризові ситуації.

Країни, зацікавлені у функціонуванні дієвої системи кібероборони, здійснюють заходи щодо створення в рамках Збройних Сил профільних кіберкомандувань, та кібервійськ (сил) з підрозділами кібербезпеки та активної кібероборони, а також забезпечення високого рівня їх забезпеченості та готовності.

У разі невідповідності вимогам, плануються та виконуються заходи щодо утворення інституцій та систем, які б відповідали цим вимогам. Зокрема, в рамках 7-ї групи, мають бути здійснені заходи щодо:

утворення Національного органу у складі Збройних Сил, на який покладено основне завдання щодо кібероборони;

формування його політичних та функціональних повноважень та стратегій реагування на кіберзагрози;

оприлюднення в рамках національного законодавства його пріоритетів та повноважень щодо кібероборони, як на території суверенної держави, так й поза її межами.

Національним центральним органом виконавчої влади у сфері кібероборони, в окремих суверенних державах може бути також Національна поліція або органи безпеки, чи розвідки. Але, обов'язковою умовою також є відповідність сучасним вимогам та готовність Збройних Сил до дій в кіберпросторі у разі збройного конфлікту. Законодавство України [101 - 104] однозначно покладає це завдання на Міністерство оборони та Збройні Сили України.

Для забезпечення створення та функціонування цілісної системи кібероборони (СКО) з урахуванням національних вимог [47-56] та рекомендацій провідних науково-дослідних центрів та країн-партнерів щодо уніфікації бойових командувань і процедур [36] необхідно здійснити низку взаємопов'язаних політичних, правових, організаційних, науково-технічних, безпосередньо військових та інших заходів спрямованих на формування такої системи кібербезпеки та кібероборони, яка забезпечить скоординоване управління всіма її складовими.

Така система потребує наявності відповідного єдиного органу управління, подібного за структурою, завданнями і функціями до аналогічних органів управління в цій сфері країн-членів НАТО, призначеного для реалізації єдиної політики та стратегії дій Міністерства оборони України та Збройних Сил України в інформаційному та кіберпросторі; організації та координації заходів щодо кібербезпеки та захисту критичної інформаційної інфраструктури держави; управління силами кібербезпеки та кібероборони під час кризових ситуацій, в умовах особливого періоду та правового режиму воєнного стану (рис. 6, 7) [6,7].

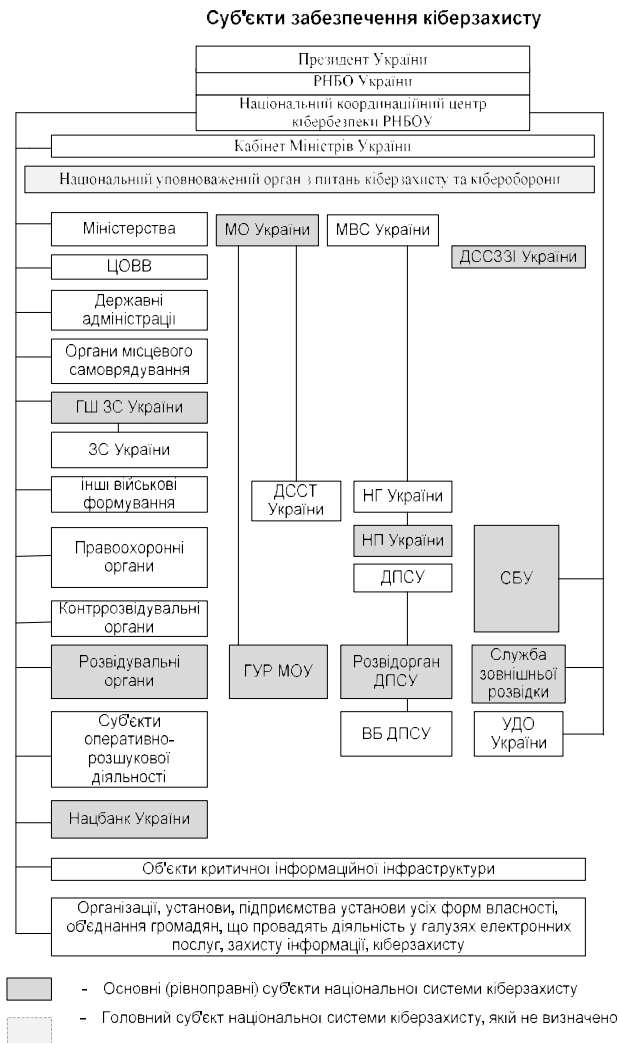


Рис.6. Суб'єкти забезпечення кіберзахисту

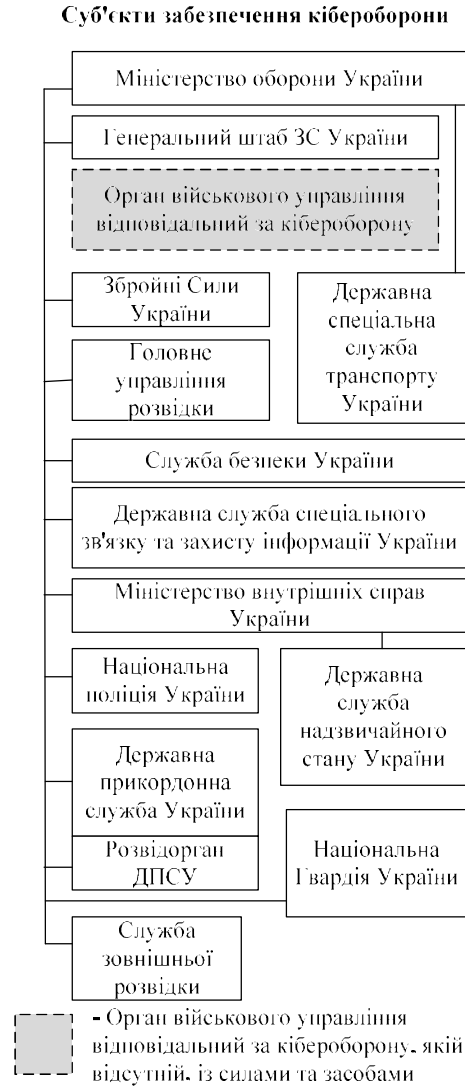


Рис.7. Суб'єкти забезпечення кібероборони

### Висновки й перспективи подальших досліджень

На думку авторів, утворення та розгортання системи кібероборони держави доцільно здійснювати шляхом комплексного узгодження напрямів діяльності складових сектору безпеки та оборони, які задіяні в вирішенні питань кібербезпеки з чітким розподілом функцій за їх належністю до вирішення питань кібероборони. Далі, повинна бути здійснена інтеграція всіх сил та засобів, які на цей час вирішують питання, що мають відношення до кібероборони, за досвідом країн НАТО, в єдину структуру, подібну до кіберсил (кібервійськ) країн НАТО. Для них повинні бути чітко визначені цілі, функції і завдання, які вони повинні вирішувати в інтересах забезпечення кібероборони держави та здійснене відповідне кадрове, наукове і ресурсне забезпечення. Необхідно спланувати та провести заходи щодо утворення дієздатної національної системи кібероборони з урахуванням вимог

законів та нормативно-правових актів України [47-49,51,52,54,55] та досвіду провідних країн світу, особливо країн-членів НАТО.

Створення, з урахуванням досвіду країн-членів НАТО та наявність ефективної системи управління силами і засобами які діють в кіберпросторі забезпечить їх найбільш раціональне функціонування та застосування, інформаційну і кібер перевагу над противником та буде сприяти практичній реалізації прийнятої в країнах членах НАТО концепції “смарт-оборони”, ключовими елементами якої є високотехнологічна підготовка персоналу та збалансоване поєднання найбільш ефективних аспектів стратегій “жорсткої сили” та “м’якої сили”, шляхом зваженого і узгодженого використання інструментарію стратегічних комунікацій, інформаційних та кібердій, санкцій, переконання і раціональне застосування сили та інших впливів способом, який є найбільш рентабельним та має політичну і соціальну легітимність

## Література

1. В.Бурачок, Г.Гулак, В.Хорошко, Завдання, форми та способи ведення війн у кібернетичному просторі – К.: Наука і оборона №3 - 2011, с.35-42. 2. Є.Живило О., О.Черноног. Стратегія кібероборони України – К.: ВІТІ № 4 – 2017, с. 30-37 3. В. Ліпкан, І. Діордіца. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України – К.: Підприємництво, господарство і право №5– 2017, с. 174-180. 4. I.Gorbenko, A.Zamula, Ye.Semenko. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications – Kharkiv/ Telecommunications and Radio Engineering. – 2016. – Vol. 75. – Issue 2. – P. 169–178. 5. I.Горбенко, О.Замула. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності – Харків - Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки - 2017. Випуск 15. с.43-49 - [Електронний ресурс]. Режим доступу:[http://nbuv.gov.ua/UJRN/Mtkm\\_fiz\\_mat\\_2017\\_15\\_10](http://nbuv.gov.ua/UJRN/Mtkm_fiz_mat_2017_15_10) 6. Ю.Даник, С.Вдовенко. Проблеми та перспективи забезпечення кібероборони держави К.:ВІКНУ, випуск 66, 2020 - С. 56-72. 7. Ю.Даник. Високотехнологічні аспекти забезпечення національної безпеки й оборони. К.: Военная связь. Телеком. Жовтень 2018. с. 58-69 8. Г. Лиддел. Стратегия непрямых действий — М.: ИЛ - 1957. 9. DoD C4ISR Cooperative Research Program Assistant Secretary of Defense (C3I) Mr. Arthur L. Money Special Assistant to the ASD (C3I). [Електронний ресурс]. Режим доступу: [http://dodccrp.org/files/Alberts\\_NCW.pdf](http://dodccrp.org/files/Alberts_NCW.pdf) 10. Warden, John A. III (September 1995), Chapter 4: Air theory for the 21st century, Battlefield of the Future: 21st Century Warfare Issues. 11. Bryant D.J. Critique, Explore, Compare and Adapt (CECA): A New Model for Command Decisionmaking. Defence R&D Toronto Technical Report, DFDC, Toronto TR, 2003. 63 p. 12. DoD C4ISR Cooperative Research Program Assistant Secretary of Defense (C3I) Mr. Arthur L. Money Special Assistant to the ASD(C3I). [Електронний ресурс]. Режим доступу [http://dodccrp.org/files/Alberts\\_NCW.pdf](http://dodccrp.org/files/Alberts_NCW.pdf) 13. Л.Поліщук, С.Богуцький М. Сучасні тенденції розвитку систем управління збройних сил провідних країн світу - ВІТІ - 2014, с.42-46 14. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 – 2016, 100 15. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015. 16. S.Neema. Symbiotic Design for Cyber Physical Systems. Defense Advanced Research Projects Agency Program Information. [Електронний ресурс]. Режим доступу: <https://www.darpa.mil/program/symbiotic-design-for-cyber-physical-systems>. 17. С.Вдовенко, Ю.Даник. Концептуальні напрямки комплексного вирішення проблеми захисту від несанкціонованого доступу в складних системах спеціального призначення. Вінниця, ВНПУ - 2017, с. 61 – 64. 18. Ю.Даник, С.Вдовенко. Ланцюгові ефекти в кібердіях. Збірник наукових праць військового інституту Київського Національного університету імені Тараса Шевченка, випуск 64 - 2019 - С. 56-71. 19. [Електронний ресурс]. Режим доступу: <https://www.usna.edu/wrc/cpsl/index.php>, <https://thebabel.com.ua/news/41889-ssha-rozhortayut-protidronovi-lazerni-sistemi-na-zarubizhnih-bazah>, <https://defence-ua.com/index.php/statti/2245-vyprovuvannya-bpla-6-ho-pokolinnya-ssha-pokazaly-mistse-rosiyi>, <http://www.nanonewsnet.ru/news/2017/kitaitsy-obedinili-v-stayu-tysyachu-dronov>, [https://lb.ua/world/2015/11/17/321192\\_britaniya\\_sozdast\\_speetsialnie.html](https://lb.ua/world/2015/11/17/321192_britaniya_sozdast_speetsialnie.html), <http://www.lefigaro.fr/international/l-armee-se-dote-de-56-microrobots-de-reconnaissance>, [https://www.linkedin.com/company/national-security-agency?trk=similar-pages\\_result-card\\_full-click](https://www.linkedin.com/company/national-security-agency?trk=similar-pages_result-card_full-click), <https://www.cybercom.mil/About/Mission-and-Vision/> <https://www.cybercom.mil/>, <https://www.cybercom.mil/About/Leadership/Bio-Display/Article/1512978/commander-uscycbercom/>, [https://en.wikipedia.org/wiki/United\\_States\\_Cyber\\_Command](https://en.wikipedia.org/wiki/United_States_Cyber_Command), [https://military.wikia.org/wiki/Second\\_United\\_States\\_Army](https://military.wikia.org/wiki/Second_United_States_Army) <https://www.globalsecurity.org/military/agency/usaf/afcyber.htm>, <https://www.public.navy.mil/fcc-c10f/Pages/home.aspx>, [https://www.navy.mil/local/fccc10f/https://www.armed-services.senate.gov/imo/media/doc/Gilday\\_05-23-17.pdf](https://www.navy.mil/local/fccc10f/https://www.armed-services.senate.gov/imo/media/doc/Gilday_05-23-17.pdf), <https://www.candp.marines.mil/Organization/Operating-Forces/US-Marine-Corps-Forces-Cyberspace-Command/> <https://www.epravda.com.ua/news/2018/10/23/641908/> <https://www.rbc.ua/rus/news/ssha-proveli-kiberataku-iranskie-raketnye-1561260168.html> <https://lexinform.com.ua/v-sviti/ssha-pochaly-kiberoperatsiyu-proty-rosiyi/> <https://www.arcyber.army.mil/>, <https://www.fifthdomain.com/dod/cybercom/2019/07/25/wh-at-the-future-holds-for-cyber-command/> 20. Moore, Gordon E. (1965). Cramming more components onto integrated circuits, Electronics Magazine. с. 4 [Електронний ресурс]. Режим доступу: <https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf> 21. Moore, Gordon E. No Exponential is Forever: But “Forever” Can Be Delayed!, International Solid-State Circuits Conference 2003 / SESSION 1 / PLENARY / 1.1 -2003. [Електронний ресурс]. Режим доступу: <https://ieeexplore.ieee.org/document/1234194> 22. Kurzweil, Ray -2005. The Singularity Is Near. When Humans Transcend Biology. Penguin Books [Електронний ресурс]. Режим доступу: [http://stargate.inf.elte.hu/~seci/fun/Kurzweil/Ray\\_Singularity\\_Near\\_The\\_hardbac\\_ed\\_Bv1\\_D.pdf](http://stargate.inf.elte.hu/~seci/fun/Kurzweil/Ray_Singularity_Near_The_hardbac_ed_Bv1_D.pdf) 23. Recently discovered phenomenon could provide a way to bypass the limits to Moore's Law. [Електронний ресурс]. Режим доступу: <https://phys.org/news/2017-10-phenomenon-bypass-limits-law.html> 24. В. Берма, В. Шемяев. Розвиток технологій у провідних країнах світу. Уроки для України. [Електронний ресурс]. Режим доступу: <https://defence-ua.com/index.php/statti/publikatsiji-partneriv/8982-rozvytok-tekhnologiy-u-providnykh-krayinakh-svitu-uroky-dlya-ukrayiny> 25. Network Centric Warfare Market by Platform (Land, Air, Naval, Unmanned), Application (ISR, Communication, Computer, Cyber, Combat, Control & Command), Mission Type, Communication Network, Architecture, and Region - Global Forecast to 2021. [Електронний ресурс]. Режим доступу: <https://www.marketresearch.com/MarketsandMarkets-v3719/Network-Centric-Warfare-Platform-Land-10188278/> 26. BMC4ISR means Battle Management/Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. [Електронний ресурс]. Режим доступу: <http://acronymsandslang.com/definition/24656/BMC4ISR-meaning.html> 27. Summit Meeting of NATO Heads of State and Government - Lisbon, Portugal, 19-20 Nov 2010. [Електронний ресурс]. Режим доступу: [https://www.nato.int/cps/en/natolive/events\\_66529.htm](https://www.nato.int/cps/en/natolive/events_66529.htm) 28. С.Вдовенко, Ю.Даник, С.Фараон. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. – Харків: ХНУ ім. В.Н.Каразіна – 2019, №1(12). [Електронний ресурс]. Режим доступу: <https://doi.org/10.26565/2519-2310-2019-1-02> 29. DOD Dictionary of Military and Associated Terms As of January 2020. Електронний ресурс. Режим доступу: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> 30. DOD. Joint Publication 3-12, Cyberspace Operations, 8 June 2018/. Електронний ресурс. Режим доступу: [https://fas.org/irp/doddir/dod/jp3\\_12.pdf](https://fas.org/irp/doddir/dod/jp3_12.pdf) 31. Statement by lieutenant general Paul M. Nakasone Commander, United States Army Cyber Command before the Subcommittee on Cybersecurity Committee on Armed Services United States Senate second session, 115th congress May 23, 2017. Електронний ресурс. Режим доступу: [Modern Information Technologies in the Sphere of Security and Defence № 3\(36\)/2019 ISSN 2311-7249 \(Print\)/ISSN 2410-7336 \(Online\) 45](https://www.armed-</a></p>
</div>
<div data-bbox=)

- services.senate.gov/imo/media/doc/Nakasone\_05-23-17.pdf.
32. International Strategy For Cyberspace: Prosperity, Security and Openness in a Networked World. Washington DC: The White House, May 2011. [Електронний ресурс]. Режим доступу: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/internationalstrategy\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf)
33. Secretary of State Hillary Rodham Clinton On the Release of President Obama Administration's International Strategy for Cyberspace. May 16, 2011. [Електронний ресурс]. Режим доступу: <http://www.state.gov/secretary/rm/2011/05/163523.htm>
34. Department of Defense. The Department of Defense Cyber Strategy - April 2015 National Cyber Strategy of the United States of America. September 2018. [Електронний ресурс]. Режим доступу: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
35. Summary Department of Defense Cyber Strategy - 2018. [Електронний ресурс]. Режим доступу: [https://media.defense.gov/2018/sep/18/2002041658/-1-1/cyber\\_strategy\\_summary\\_final.pdf](https://media.defense.gov/2018/sep/18/2002041658/-1-1/cyber_strategy_summary_final.pdf)
36. Cyber Readiness Index 2.0 A Plan for Cyber Readiness: a baseline and an index. Potomac Institute for Policy Studies 901 N. Stuart St, Suite 1200 Arlington, VA, 22203, [Електронний ресурс]. Режим доступу: <https://www.potomacinstitute.org/images/CRIndex2.0.pdf>
37. [Електронний ресурс] – Режим доступу: [https://www.dw.com/uk/ukr-rss-MetaUA-ukr-V\\_Mire-3051-xml-mrss](https://www.dw.com/uk/ukr-rss-MetaUA-ukr-V_Mire-3051-xml-mrss), [https://espreso.tv/news/2015/03/23/u\\_nimechchyni\\_vyrishyl\\_u\\_vstanovyty\\_pravyla\\_dlya\\_kiberviyn](https://espreso.tv/news/2015/03/23/u_nimechchyni_vyrishyl_u_vstanovyty_pravyla_dlya_kiberviyn)
38. [Електронний ресурс] – Режим доступу: <https://intvua.com/news/society/1537605491-velikobritaniya-priynyala-rishennya-pro-stvorennya-kiberviysk.html>, <https://dt.ua/WORLD/britaniya-pochalazbilshuvati-svoiy-kiberviyska-zmi-289016.html>, <https://www.unian.ua/world/1112130-velikobritaniya-zbilshue-finansuvannya-kiberviyn-u-10-raziv.html>
39. White book on National Security of the Republic of Poland. Published by National Security Bureau, Warsaw Poland, 2013. P.263. [Електронний ресурс] – Режим доступу: <https://www.unn.com.ua/uk/news/1766148-polscha-stvorit-viyska-kiberoboroni>
40. Disinformation as a Cyber Threat in the V4: Capabilities and Reactions to Russian Campaigns. [Електронний ресурс] – Режим доступу: <https://stratpol.sk/wp-content/uploads/2018/08/Infographic-Cyber-V4-STRATPOL.pdf>
41. Cyber defense academy in Budapest. [Електронний ресурс] – Режим доступу: <https://dailynewshungary.com/cyber-defense-academy-budapest/>
42. [Електронний ресурс] – Режим доступу: [https://en.wikipedia.org/wiki/Cooperative\\_Cyber\\_Defence\\_Centre\\_of\\_Excellence](https://en.wikipedia.org/wiki/Cooperative_Cyber_Defence_Centre_of_Excellence), <https://www.eurointegration.com.ua/articles/2017/12/1/7074473/>, <http://www.eurointegration.com.ua/news/2017/11/8/7073389/>
43. Доктрина информационной безопасности Российской Федерации (Указ Президента Российской Федерации от 05.12.2016 № 646). [Електронний ресурс] – Режим доступу: <http://kremlin.ru/acts/bank/41460>
44. [Електронний ресурс]. Режим доступу: [http://recrut.mil.ru/for\\_recruits/research\\_company/companie\\_s.htm](http://recrut.mil.ru/for_recruits/research_company/companie_s.htm), [https://www.nstu.ru/studies/army\\_research](https://www.nstu.ru/studies/army_research)
45. М.Гребенюк, Б.Леонов, Р.Лук'янчук. Досвід Ізраїлю у сфері забезпечення кібербезпеки // К.: Інформація і право – 2018, № 2(25).
46. Конституція України [Електронний ресурс] – Режим доступу: <http://zakon0.rada.gov.ua/laws/show/254>
47. Закон України Про основні засади забезпечення кібербезпеки України № 2163-VIII від 5 жовтня 2017 року. [Електронний ресурс] – Режим доступу: <http://zakon.rada.gov.ua/laws/show/2163-19>
48. Закон Про оборону України: за станом на 01.07.2018 р./, затверджений ВР України від 06.12.1991, № 1932-XII – [Електронний ресурс] – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/1932-12>
49. Закон України Про Збройні Сили України від 6 грудня 1991 року N 1934-XII (зі змінами), [Електронний ресурс] – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/1934-12>
50. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96 // Офіц. вісн. України. — 2016. — № 23.
51. Концепція розвитку сектору безпеки і оборони України, введена в дію Указом Президента України від 14.03.2016 №92/2016
52. Стратегічний оборонний бюлетень України, введений в дію Указом Президента України від 6.06.2016 № 240/2016
53. Візія Генерального штабу ЗС України щодо розвитку Збройних Сил України на найближчі 10 років. [Електронний ресурс]. Режим доступу: <http://www.mil.gov.ua/news/2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi-10-rokiv/>
54. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

## ОПЫТ РАЗВИТИЯ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ И КИБЕРОБОРОНИ ИНОСТРАННЫХ ГОСУДАРСТВ

Сергей Григорьевич Вдовенко

Юрий Григорьевич Даник (доктор технических наук, профессор)

Александр Юрьевич Пермяков (доктор технических наук, профессор)

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

*Стремительное развитие и массовое внедрение достижений электроники, современных информационных и кибер технологий привели к формированию нового спектра рисков и угроз в сфере национальной безопасности и обороны государства, реализуемых в киберпространстве и (или) через киберпространство. Происходит стремительный рост информатизации и автоматизации всех сфер человеческой деятельности, количества хранящейся, обрабатываемой и передаваемой информации, скорости ее передачи и обработки, усложнение систем управления, взаимодействия между ними и связей между процессами управления. Киберугрозы охватывают все базовые сферы общественной деятельности (политическую, военную, правовую, экономическую, энергетическую, инфраструктурную, социальную, духовную, технологическую и т.п.), деструктивно влияя на национальную безопасность в целом.*

*Более 60 стран мира, международные (ЕС) и военно-политические союзы (НАТО), международные организации безопасности (ОБСЕ) сосредотачивают значительные усилия по обеспечению возможностей по своевременному выявлению, предупреждению, нейтрализации и ликвидации угроз в киберпространстве, в частности в сфере обороны.*

*В статье представлены следующие результаты: анализ организации и задач существующих систем кибербезопасности и киберобороны ведущих стран мира в контексте возможности и целесообразности внедрения их опыта в Украине; анализ предпосылок, существующего состояния и*

проблемных вопросов формирования систем кибербезопасности и киберобороны в Украине, а также нужного уровня их всестороннего обеспечения; пути разработки основных теоретических и прикладных положений формирования систем кибербезопасности и киберобороны в Украине.

**Ключевые слова:** кибербезопасность; кибероборона; киберпространство; система кибербезопасности; киберзащита; киберугрозы; система киберобороны; объекты критической инфраструктуры; субъекты кибербезопасности; субъекты киберобороны.

### EXPERIENCE OF DEVELOPMENT OF CYBER SECURITY SYSTEMS AND CYBER DEFENSE FOREIGN STATES

*Serhii Vdovenko*

*Yurii Danyk (Doctor of Technical Science, Professor)*

*Oleksandr Permiakov (Doctor of technical sciences, Professor)*

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

The rapid development and widespread adoption of electronics, modern information and cyber technologies have led to the emergence of a new range of national security and defense risks and threats that are being implemented in cyberspace and (or) across cyberspace. There is a rapid growth of information and automation of all spheres of human activity, the amount of information stored, processed and transmitted, the speed of its transmission and processing, the complexity of control systems, the interaction between them and the links between management processes. Cyber threats cover all basic spheres of public activity (political, military, legal, economic, energy, infrastructure, social, spiritual, technological, etc.), destructively affecting national security as a whole.

More than 60 countries, international (EU) and military-political alliances (NATO), international security organizations (OSCE) are focusing considerable efforts on providing capabilities to detect, prevent, neutralize and eliminate cyberspace threats in a timely manner, in particular in the field of defense.

The results of the article are presented: analysis of the existing cyber security and cyber defense systems of the leading countries in the context of the possibility and expediency of implementing their experience in Ukraine; analysis of the prerequisites, current status and problems of the formation of cyber security and cyber defense systems in Ukraine, as well as the required level of their comprehensive provision; development of basic theoretical and applied provisions for the formation of cyber security and cyber defense systems in Ukraine.

**Keywords:** Critical Infrastructure; Cyberspace; Cyber Defense; Cyber Defense System; Cyber Security; Cyber Defense Entities; Cyber Security Entities; Cybersecurity System; Cyberthreat.

### References

1. V. Buryachok, G. Hulak, V. Khoroshko. Tasks, Forms and Methods of War in Cybernetic Space - K.: Science and Defense №3 - 2011, p.35-42.
2. E. Zhivilo O., O.Chernohog. Cyber Defense Strategy of Ukraine - K.: VITI № 4 - 2017, p. 30-37
3. V. Lipkan, I. Diordica. The National Cyber Security System as an Integral Part of the National Security System of Ukraine - K.: Business, Economy and Law №5- 2017, p. 174-180.
4. I.Gorbenko, A.Zamula, Ye.Semenko. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications - Kharkiv/Telecommunications and Radio Engineering. – 2016. – Vol. 75. – Issue 2. – P. 169–178.
5. I.Gorbenko, O.Zamula. Models and methods of synthesis of cryptographic signals and their optimization by the criterion of time complexity - Kharkiv - Mathematical and computer simulation. Series: Physical and Mathematical Sciences - 2017. Issue 15. p.43-49 - [Electronic resource]. Access mode: [http://nbuv.gov.ua/UJRN/Mtkm\\_fiz\\_mat\\_2017\\_15\\_10](http://nbuv.gov.ua/UJRN/Mtkm_fiz_mat_2017_15_10)
6. Yu.Danik, S.Vdovenko. Problems and Prospects of Providing Cyber Defense to the State of K.: MIKNU. Issue 66. 2020 - P. 56-72.
7. Yu. Danik. High-tech aspects of national security and defense. K.: Military Communications. Telecom. October 2018 p. 58-69
8. G. Liddell. Indirect Action Strategy - M.: IL - 1957.
9. DoD C4ISR Cooperative Research Program Assistant Secretary of Defense (C3I) Mr. Arthur L. Money Special Assistant to the ASD (C3I). [Electronic resource]. Access mode: [http://dodccrp.org/files/Alberts\\_NCW.pdf](http://dodccrp.org/files/Alberts_NCW.pdf)
10. Warden, John A. III (September 1995). Chapter 4: Air theory for the 21st century. Battlefield of the Future: 21st Century Warfare Issues.
11. Bryant D.J. Critique, Explore, Compare and Adapt (CECA): A New Model for Command Decisionmaking. Defence R&D Toronto Technical Report, DFDC, Toronto TR, 2003. 63 p.
12. DoD C4ISR Cooperative Research Program Assistant Secretary of Defense (C3I) Mr. Arthur L. Money Special Assistant to the ASD(C3I). [Electronic resource]. Access mode: [http://dodccrp.org/files/Alberts\\_NCW.pdf](http://dodccrp.org/files/Alberts_NCW.pdf)
13. L.Polishchuk, S.Bogutsky M. Current Trends in the Development of Armed Forces Management Systems in Leading Countries of the World - VITI - 2014, p.42-46
14. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 – 2016, 100
15. National Security Strategy of Ukraine, approved by Presidential Decree No 287/2015 of May 26, 2015.
16. S.Neema. Symbiotic Design for Cyber Physical Systems. Defense Advanced Research Projects Agency Program Information. [Electronic resource]. Access mode: <https://www.darpa.mil/program/symbiotic-design-for-cyber-physical-systems>.
17. S.Vodovenko, Y.Danik. Conceptual directions of complex solution of the problem of protection against unauthorized access in complex systems of special purpose. Vinnitsa, VNPU - 2017, p. 61 - 64.
18. Yu.Danik, S.Vdovenko. Chain effects in cyberdenko. Proceedings of the Military Institute of the Taras Shevchenko National University of Kyiv, issue 64 - 2019 - P. 56-71.
19. [Electronic resource]. Access mode: <https://www.usna.edu/wrc/cpsl/index.php>, <https://thetabel.com.ua/news/41889-ssha-rozgotayut-protidronovi-lazerni-sistemi-na-zarubizhnih-bazah>, <https://defence-ua.com/index.php/statti/2245-vyprovuvannya-bpla-6-ho-pokolinnya-ssha-pokazaly-mistse-rosiyi>, <http://www.nanonewsnet.ru/news/2017/kitaitsy-obedinili-v-stayu-tysyachu-dronov>, [https://lb.ua/world/2015/11/17/321192\\_britaniya\\_sozdast\\_spetsial\\_nie.html](https://lb.ua/world/2015/11/17/321192_britaniya_sozdast_spetsial_nie.html), <http://www.lefigaro.fr/international/l-armee-se-dote-de-56-microrobots-de-reconnaissance>, [https://www.linkedin.com/company/national-security-agency?trk=similar-pages\\_result-card\\_full-click](https://www.linkedin.com/company/national-security-agency?trk=similar-pages_result-card_full-click), <https://www.cybercom.mil/About/Mission-and-Vision/>, <https://www.cybercom.mil/>, <https://www.cybercom.mil/About/Leadership/Bio-Display/Article/1512978/commander-uscybercom/>,

- [https://en.wikipedia.org/wiki/United\\_States\\_Cyber\\_Command](https://en.wikipedia.org/wiki/United_States_Cyber_Command),  
[https://military.wikia.org/wiki/Second\\_United\\_States\\_Army](https://military.wikia.org/wiki/Second_United_States_Army)  
<https://www.globalsecurity.org/military/agency/usaf/afcyber.htm>,  
<https://www.public.navy.mil/fcc-c10f/Pages/home.aspx>,  
<https://www.navy.mil/local/fccc10f/> [https://www.armed-services.senate.gov/imo/media/doc/Gilday\\_05-23-17.pdf](https://www.armed-services.senate.gov/imo/media/doc/Gilday_05-23-17.pdf),  
<https://www.candp.marines.mil/Organization/Operating-Forces/US-Marine-Corps-Forces-Cyberspace-Command/>  
<https://www.epravda.com.ua/news/2018/10/23/641908/>  
<https://www.rbc.ua/rus/news/ssha-proveli-kiberataku-iranski-raketnye-1561260168.html> <https://lexinform.com.ua/v-sviti/ssha-pochaly-kiberoperatsiyu-proty-rosiyi/>  
<https://www.arcyber.army.mil/>,  
<https://www.fifthdomain.com/dod/cybercom/2019/07/25/what-the-future-holds-for-cyber-command/> **20.** Moore, Gordon E. (1965). Cramming more phenomenon onto integrated circuits. *Electronics Magazine*. c. 4 [Electronic resource]. Access mode: <https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf>
- 21.** Moore, Gordon E. No Exponential is Forever: But "Forever" Can Be Delayed!, *International Solid-State Circuits Conference 2003 / SESSION 1 / PLENARY / 1.1 -2003*. [Electronic resource]. Access mode: <https://ieeexplore.ieee.org/document/1234194> **22.** Kurzweil, Ray (2005). *The Singularity Is Near. When Humans Transcend Biology*. Penguin Books [Electronic resource]. Access mode: [http://stargate.inf.elte.hu/~seci/fun/Kurzweil/Ray\\_Singularity\\_Near\\_The\\_hardbac\\_ed\\_Bv1\\_D.pdf](http://stargate.inf.elte.hu/~seci/fun/Kurzweil/Ray_Singularity_Near_The_hardbac_ed_Bv1_D.pdf)
- 23.** Recently discovered phenomenon could provide a way to bypass the limits to Moore's Law. [Electronic resource]. Access mode: <https://phys.org/news/2017-10-phenomenon-bypass-limits-law.html> **24.** V. Begma, V. Shemaev. Technology development in the world's leading countries. Lessons for Ukraine. [Electronic resource]. Access mode: <https://defence-ua.com/index.php/statti/publikatsiji-partneriv/8982-rozvytok-tekhnolohiy-u-providnykh-krayinakh-svitu-uroky-dlya-ukraviny>
- 25.** Network Centric Warfare Market by Platform (Land, Air, Naval, Unmanned), Application (ISR, Communication, Computer, Cyber, Combat, Control & Command), Mission Type, Communication Network, Architecture, and Region - Global Forecast to 2021. [Electronic resource]. Access mode: <https://www.marketresearch.com/MarketsandMarkets-v3719/Network-Centric-Warfare-Platform-Land-10188278/>
- 26.** BMC4ISR means Battle Management/Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance. [Electronic resource]. Access mode: <http://acronymsandslang.com/definition/24656/BMC4ISR-meaning.html> **27.** Summit Meeting of NATO Heads of State and Government - Lisbon, Portugal, 19-20 Nov 2010. [Electronic resource]. Access mode: <https://www.nato.int/cps/en/natolive/events/66529.htm> **28.** S.Vodovenko, Y. Danik, S. Pharaoh. Definitional problems of terminology in cybersecurity and cyber defense and ways of solving them. - Kharkiv: KhNU. VN Karazin - 2019, No.1 (12). [Electronic resource]. Access mode: <https://doi.org/10.26565/2519-2310-2019-1-02> **29.** DOD Dictionary of Military and Associated Terms As of January 2020. [Electronic resource]. Access mode: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> **30.** DOD. Joint Publication 3-12, *Cyberspace Operations*, 8 June 2018/. [Electronic resource]. Access mode: [https://fas.org/irp/doddir/dod/jp3\\_12.pdf](https://fas.org/irp/doddir/dod/jp3_12.pdf) **31.** Statement by lieutenant general Paul M. Nakasone Commander, United States Army Cyber Command before the Subcommittee on Cybersecurity Committee on Armed Services United States Senate second session. 115th congress May 23, 2017. [Electronic resource]. Access mode: [https://www.armed-services.senate.gov/imo/media/doc/Nakasone\\_05-23-17.pdf](https://www.armed-services.senate.gov/imo/media/doc/Nakasone_05-23-17.pdf)
- 32.** International Strategy For Cyberspace: Prosperity, Security and Openness in a Networked World. Washington DC: The White House, May 2011. [Electronic resource]. Access mode: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/internationalstrategy\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf) **33.** Secretary of State Hillary Rodham Clinton On the Release of President Obama Administration's International Strategy for Cyberspace. May 16, 2011. [Electronic resource]. Access mode: <http://www.state.gov/secretary/rm/2011/05/163523.htm>
- 34.** Department of Defense. The Department of Defense Cyber Strategy - April 2015 National Cyber Strategy of the United States of America. September 2018. [Electronic resource]. Access mode: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
- 35.** Summary Department of Defense Cyber Strategy - 2018. [Electronic resource]. Access mode: [https://media.defense.gov/2018/sep/18/2002041658/-1-1/1/cyber\\_strategy\\_summary\\_final.pdf](https://media.defense.gov/2018/sep/18/2002041658/-1-1/1/cyber_strategy_summary_final.pdf) **36.** Cyber Readiness Index 2.0 A Plan for Cyber Readiness: a baseline and an index. Potomac Institute for Policy Studies 901 N. Stuart St. Suite 1200 Arlington, VA, 22203, [Electronic resource]. Access mode: <https://www.potomacinstitute.org/images/CRIndex2.0.pdf> **37.** [Electronic resource]. Access mode: <https://www.dw.com/uk/ukr-rss-MetaUA-ukr-V-Mire-3051-xml-mrss>, [https://espreso.tv/news/2015/03/23/u\\_nimechchyni\\_vyrishyly\\_vst\\_ano\\_vyty\\_pravy\\_la\\_dlya\\_kiberviy\\_n](https://espreso.tv/news/2015/03/23/u_nimechchyni_vyrishyly_vst_ano_vyty_pravy_la_dlya_kiberviy_n) **38.** [Electronic resource]. Access mode: <https://intvua.com/news/society/1537605491-velika-britaniya-priynvala-rishennya-pro-stvorennya-kiberviyusk.html>, <https://dt.ua/WORLD/britaniya-pochalazbilshuvaty-svoiy-kiberviyuska-zmi-289016.html>, <https://www.unian.ua/world/1112130-velikobritaniya-zbilshue-finansuvannya-kiberviy-n-10-raziv.html> **39.** White book on National Security of the Republic of Poland. Published by National Security Bureau. Warsaw Poland, 2013. P.263. **40.** [Electronic resource]. Access mode: <https://www.unn.com.ua/uk/news/1766148-polscha-stvorit-viyska-kiberoboroni> **41.** Disinformation as a Cyber Threat in the V4: Capabilities and Reactions to Russian Campaigns [Electronic resource]. Access mode: <https://stratpol.sk/wp-content/uploads/2018/08/Infographic-Cyber-V4-STRATPOL.pdf> **42.** Cyber defense academy in Budapest. [Electronic resource]. Access mode: <https://dailynewshungary.com/cyber-defense-academy-budapest/> <https://dailynewshungary.com/cyber-defense-academy-budapest/> **43.** [Electronic resource]. Access mode: [https://en.wikipedia.org/wiki/Cooperative\\_Cyber\\_Defence\\_Centre\\_of\\_Excellence](https://en.wikipedia.org/wiki/Cooperative_Cyber_Defence_Centre_of_Excellence), <https://www.eurointegration.com.ua/articles/2017/12/1/7074473/>, <http://www.eurointegration.com.ua/news/2017/11/8/7073389/>
- 44.** Doctrine of Information Security of the Russian Federation (Decree of the President of the Russian Federation of 05.12.2016 No. 646). [Electronic resource]. Access mode: <http://kremlin.ru/acts/bank/41460> **45.** [Electronic resource]. Access mode: [http://recrut.mil.ru/for\\_recruits/research\\_company/companies.htm](http://recrut.mil.ru/for_recruits/research_company/companies.htm), [https://www.nstu.ru/studies/army\\_research](https://www.nstu.ru/studies/army_research) **46.** M. Grebenyuk, B. Leonov, R. Lukyanchuk. Israel's experience in cybersecurity // K.: Information and Law - 2018, No. 2 (25). **47.** Constitution of Ukraine [Electronic resource]. Access mode: <http://zakon0.rada.gov.ua/laws/show/254> **48.** Law of Ukraine On the Fundamental Principles of Cyber Security of Ukraine No. 2163-VIII of October 5, 2017. [Electronic resource]. Access mode: <http://zakon.rada.gov.ua/laws/show/2163-19> **49.** Law on Defense of Ukraine, approved by the Verkhovna Rada of Ukraine dated 06.12.1991, No. 1932-XII — [Electronic resource]. Access mode: <http://zakon4.rada.gov.ua/laws/show/1932-12> **50.** Law of Ukraine On the Armed Forces of Ukraine of December 6, 1991 N 1934-XII. [Electronic resource]. Access mode: <http://zakon3.rada.gov.ua/laws/show/1934-12> **51.** Ukraine's cybersecurity strategy, approved by Presidential Decree No. 96 of March 15, 2016 // Official. hanging Of Ukraine. - 2016. - № 23. **52.** The Concept of Development of the Security and Defense Sector of Ukraine. Implemented by the Decree of the President of Ukraine of 14.03.2016 # 92/2016 **53.** Strategic Defense Bulletin of Ukraine. Enacted by Presidential Decree of June 6, 2016 No. 240/2016 **54.** Vision of the General Staff of the Armed Forces of Ukraine on the development of the Armed Forces of Ukraine for the next 10 years. [Electronic resource]. Access mode: <http://www.mil.gov.ua/news/2020/01/11/vizyva-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-najblizhchi-10-rokiv/> **55.** National Security Strategy of Ukraine, approved by Presidential Decree No 287/2015 of May 26, 2015.



Леонід Броніславович Каневський (кандидат технічних наук)  
Максим Сергійович Повх  
Сергій Миколайович Шумський

Національний університет оборони України імені Івана Черняхівського, Київ, Україна

## ПЕРСПЕКТИВИ КОМБІНОВАНОГО ВИКОРИСТАННЯ ВИДОВИХ ЗАСОБІВ ПОВІТРЯНО-КОСМІЧНОГО БАЗУВАННЯ ДЛЯ ПІДВИЩЕННЯ ІНФОРМАТИВНОСТІ РОЗВІДУВАЛЬНОГО ЗАБЕЗПЕЧЕННЯ ВІЙСЬК (СИЛ)

У статті проведено аналіз можливостей виконання завдань розвідувального забезпечення військ (сил) щодо визначення положення та прогнозування характеру дій противника за інформацією від видових засобів спостереження що базуються в повітряно-космічному просторі за досвідом антитерористичної операції та операції Об'єднаних сил. Визначено, що існуючі підходи у Збройних Силах України є не достатніми і потребують розвитку та удосконалення.

З метою часткового вирішення даної проблеми були розглянуті підходи щодо комбінованого використання засобів повітряного та космічного базування. Запропоновано алгоритм для вибору оптимального способу добування достовірних відомостей про склад, угруповання, дії, наміри противника.

Впровадження запропонованих підходів дозволить: підвищити інформативність та повноту розвідувального забезпечення Збройних Силах України, що сприятиме організації та плануванню діяльності військ (сил) в операції Об'єднаних сил, більш раціонально розподіляти та використовувати ресурс технічних видів розвідки повітряно-космічно базування.

**Ключові слова:** космічні апарати подвійного призначення, геоінформаційні технології, безпілотні авіаційні комплекси, розвідувально-інформаційне забезпечення військ (сил).

### Вступ

Ретроспективний аналіз збройних конфліктів за останні 100 років [1-3] вказує на те, що розвиток збройної боротьби перебуває в якісно новій стадії, коли вирішальна роль вже відводиться не багаточисельним арміям і величині калібру зброї, а високоточної неядерній зброї, яка за своєю руйнівною силою еквівалентна ядерній, а, інколи, й вище за неї. Загально відомі принципи, які сприяють перемозі є дії на випередження противника, що можливо завдяки використанню достовірних даних високорозвиненої системи розвідувального забезпечення.

В рамках даної статті для розвитку та удосконалення видової розвідки, як складової системи воєнної розвідки пропонується розглянути засоби повітряно-космічно базування. До складу таких засобів варто віднести космічні апарати (КА) оптико-електронного моніторингу Земної поверхні (наприклад: КА "WorldView-1,-2,-3,-4", "Eros-B", "Pleiades-1B", "GeoEye-1", тощо), спеціалізовані літаки розвідки (наприклад: Су-24 МР, Ан-30Б, Ту-154, U-2, CN-235 CASA, тощо), а також безпілотні літальні апарати з апаратурою фото та відеоспостереження (наприклад: RQ-4 Global Hawk, PD-1, Fly Eye, Лелека-100, Фурія, тощо).

Враховуючи досвід бойових дій на сході України варто відмітити, що на озброєні російського агресора є далекобійні та всепогодні засоби ураження, які володіють високою мобільністю. Для ефективного протистояння жорстко постає питання щодо підвищення вимог до оперативності й достовірності отримання розвідувальних відомостей, точності визначення координат об'єктів (цілей) противника і часу передачі розвідувальних даних до споживача інформації. В такій ситуації актуальним є пошук

підходів до використання засобів повітряно-космічно базування, де в обмежених умовах (відсутності своїх космічних систем та деяких технічних видів повітряної розвідки) виникає потреба оптимальної організації систематичного добування розвідувальних відомостей про противника.

Комплексування даних від засобів повітряно-космічного базування може стати основою для тематичної обробки з можливістю всеосяжної оцінки противника, прогнозування характеру його дій та ефективного планування дії своїх військ (сил).

**Постановка проблеми.** Завдання добування інформації про противника із використанням високотехнологічних засобів повітряно-космічно базування вимагає застосування принципів системного аналізу і методів синтезу різночасових даних від фізично різних за своєю будовою засобів добування інформації. Для якісного процесу перетворення вхідного потоку окремих роз'єднаних відомостей від усіх засобів повітряно-космічно базування в єдиний завершений результат у вигляді відомостей про склад, угруповання, ймовірний характер дій і наміри противника варто розглянути можливості застосування геоінформаційних технологій. Основою для формування такого роду відомостей має стати тематична обробка даних з повітряно-космічних систем. Для цього виникає необхідність виділення основних її складових (фаз), дослідження логічних зв'язків комплексування різноструктурних даних з виділенням та подальшим вирішення виникаючих проблем.

В контексті вирішення даного завдання, розглянемо противника, як окремий елемент на Земній поверхні, що за своїм характером може бути складним (аеродром, склад озброєння тощо) чи простим (літак, танк, військовий автомобіль)

об'єктом розвідки. Цільова функція тематичної обробки буде зводитись до детального аналізу, систематизації, повторної перевірки і підтвердженні отриманих в ході обробки інформаційних даних для представлення споживачу достовірних відомостей з оцінки противника.

Основна проблема повітряної розвідки із застосуванням видових засобів літаків та безпілотних літальних апаратів полягає в суперечності між великими розмірами площі, що оглядається, і незначними геометричними розмірами переважної більшості цілей, які розвідують, що призводить до виникнення величезних обсягів первинної розвідувальної інформації, обробка яких для вище зазначених систем і апаратів космічного базування є різною і не упорядкованою по відношенню один до одного.

Для отримання шуканого результату з урахуванням теорії прийняття рішень перед безпосереднім процесом добування розвідувальних даних має передувати вибір альтернативи, як варіанту застосування засобу повітряно-космічного базування результати яких належатимуть континуальній множині  $\{X\}$ .

В загальному вигляді функція корисності для прийняття рішення може бути представлена як  $\Phi = [y(x), g]$ , де  $x = (x_i)_{i=1}^n \in X$ , відповідно  $y$  – представляє собою частинні критерії і визначається як  $y = \{y_k\}_{k=1}^s \in M = \{0 \leq y_k \leq A_k, k \in [1, s]\}$ , де  $A$  множина обмежень, а  $g$  множина можливих зовнішніх умов.

З метою побудови ефективної розвідувально-інформаційної системи на основі засобів повітряно-космічно базування постає задача вироблення таких підходів та побудови такої оптимальної ієрархічної системи, яка дозволила б проводити вибір найкращого варіанту добування інформації про противника з повітряно-космічного простору.

**Аналіз останніх досліджень і публікацій.** Аналіз сучасних принципів ведення збройної боротьби [1–5] вказує на те, що у ЗС провідних держав світу головні зусилля під час підготовки та ведення бойових дій спрямовані на досягнення інформаційної переваги над противником шляхом удосконалення системи управління силами і засобами розвідки. В зв'язку з цим, основні зусилля провідних країн світу зосереджені на вирішенні таких завдань: адаптації існуючих систем збору, обробки і розподілення інформації до функціонування в єдиному інформаційно-комунікаційному просторі та надання доступу військам (силам), що беруть участь у бойових діях, до даних всіх засобів розвідки, що знаходяться в цій мережі.

Порівнюючи Грузино-Осетинський конфлікт 2008 року із «турботливою» участю Російської Федерації [3] та досвіду подій на сході України (аналітичні дані з 2014 по 2018 роки з відкритих джерел [6–9]) можна побачити тенденцію та напрями розвитку російського агресора. Оцінка події 2008 року на території Грузії [3] свідчать про недостатність у повітряно-космічних силах Російської Федерації (РФ) сучасної високоточної зброї з супутниковою системою наведення, основною зброєю на той час залишалася звичайна бомба та некерована ракета. Практично повна відсутність застосування безпілотних авіаційних комплексів (БпАК). Не зважаючи на це командування угруповання збройних сил РФ використовували інформацію космічних систем

спостереження. Цьому свідчать факти того, що з достатньо високою організованістю було знищено: авіаційний завод, декілька кораблів у Поті, всі аеродроми. Варто відмітити, що зазначені об'єкти є стаціонарними і не вимагають високої оперативності уточнення відомостей про них, а їх координати є незмінними у часі.

Розглядаючи діяльність російського агресора на оперативному та оперативно-тактичному рівнях можна дійти висновку, що інформація космічних систем розвідки або не використовувалась, або мала низьку ефективність (близьку до нуля). Це пояснюється тим, що бомбові удари з повітря по рухомим сухопутним військам Грузії проводились із запізненням на одну дві доби, що давало можливість грузинському керівництву часно передислокувати їх. Використання РФ дальнього стратегічного бомбардувальника ТУ-22-М для задач фотографування результатів власних бомбових ударів для оцінки ефективності виконання завдань призвели до того, що він був збитий зенітним ракетним комплексом «Бук-М1», відповідно подальше застосування літаків-розвідників МІГ-25МР, Су-25Р, Су-24МР скоротилось у рази.

Невизначеність у точності оцінки координат дислокації грузинських військ, що відходили, не дозволила використати повітряні десанти і гелікоптерні рухомі загони мінування для ускладнення відходу грузинських військ. Підвищення оперативності та достовірності отримання таких розвідувальних відомостей можна було б компенсувати за рахунок систематичного використання БпАК чого не було зроблено.

Аналіз досвіду бойових дій на сході України протягом 2014–2018 років [6–9] вказує на те, що незаконні збройні формування під керівництвом РФ за рахунок своїх штатних підрозділів безпілотної авіації активно нарощують їх застосування. Безпілотні літальні апарати противника виконували завдання шляхом ведення оптико-електронної розвідки з метою виключення раптових дій Об'єднаних сил (особливо в період проведення ротації українських військових підрозділів), уточнення лінії розмежування та контроль діяльності своїх військ. Протягом останнього року в [9] відмічено понад 650 випадків застосування БпАК противника, з них основна частина безпілотних літальних апаратів типу «Орлан-10», «Форпост», «Елерон», «Гранат» та різні типи квадрокоптерів.

Оцінка характеру застосування БпАК та інтенсивність вогню противника в зоні проведення операції Об'єднаних сил (ООС), протягом доби, вказують на те, що вогневому ураженню артилерійського підрозділу передують розвідка об'єкту ураження. При цьому, на виконання завдання та дешифрування матеріалів повітряної розвідки БпАК противнику необхідно до 8 годин. Застосування літаків-розвідників переважно проводиться в періоди ротацій підрозділів Збройних Сил України, це пояснюється потребою протиборчої сторони у широкомасштабному добуванні різносторонніх розвідувальних даних.

Огляд останніх досліджень [3, 10] показує, окремі переваги використання космічної компоненти, літаків-розвідників та БпАК. В інших роботах [5, 11] виокремлюються та розвиваються напрями щодо перспективи використання космічних апаратів дистанційного зондування Землі, як систем подвійного призначення з метою

інформаційно-розвідувального забезпечення військ (сил). Враховуючи відсутність комплексного дослідження питань об'єднання інформації від усіх можливих засобів повітряно-космічного базування з метою виявлення переваг та проблемних питань у цьому напрямку в рамках даної статті пропонується розглянути перспективи комбінованого використання засобів повітряно-космічного базування щодо вибору оптимального способу розвідувального забезпечення військ (сил).

**Мета статті** – дослідити можливості комбінованого використання даних від засобів повітряно-космічного базування (КА оптико-електронного моніторингу Земної поверхні, літаків фото-розвідки, БпАК) для підвищення повноти та достовірності відомостей про противника.

### **Виклад основного матеріалу дослідження**

Проведений огляд сучасних тенденцій ведення збройної боротьби вказує на необхідність пошуку нових, більш дієвих підходів до проведення заходів розвідувального забезпечення за інформацією від видових засобів повітряного та космічного базування у Збройних Сил України. Актуальним залишається питання розробки та впровадження інтегрованої системи управління та розвідки, як єдиного інформаційного простору, з можливістю використання будь-яким споживачем усієї необхідної інформації.

Якщо активне застосування в зоні проведення ООС БпАК (PD-1, Лелека-100, Фурія, Мара, тощо) дозволило підвищити оперативність отримання розвідувальної інформації, у порівнянні з літаками-розвідниками та КА, то питання повноти та високої достовірності залишається відкритим. В рамках формалізованого в статті завдання на прикладі военного дешифрування матеріалів повітряної розвідки, де кінцевим джерелом із усієї сукупності повітряно-космічних систем приймемо БпАК. Відповідно до цього варто зауважити, що крім суперечності між великими розмірами площі, що оглядається, і незначними геометричними розмірами переважної більшості цілей, які розвідують, ще добавиться проблема пробації военного дешифрування, що на сьогоднішній день проводиться оператором, який обмежений фізичними характеристиками та своєю кваліфікацією.

У вузькому розумінні процес добування відомостей про противника із застосуванням КА чи літаків-розвідників і навіть БпАК буде мати однаковий характер і складатиметься з таких основних складових, як: аналіз, усвідомлення, постановка завдання; планування на виконання; тематична обробка отриманих даних та формування звітно-інформаційних документів. Узагальнення окремо отриманих відомостей про противника проводиться у спеціально визначених структурних підрозділах і як правило до самих виконавців таке узагальнення не надходить. Нажаль відсутність відповідного зворотного зв'язку аж ніяк не сприяє плануванню роботи цих засобів окремо або при їх спільному застосуванні. А відсутність на сьогоднішній день підходу щодо планування комплексування даних від різних засобів повітряно-космічного базування не дозволяє в повній мірі виділяти нові розвідувальні ознаки та в повній мірі оцінити ймовірний характер дій противника. Таким чином, для прикладу, де кінцевим джерелом із усієї

сукупності повітряно-космічних систем буде БпАК. Апріорними даними для його планування і застосування має стати довідково-інформаційна система на базі геоінформаційних технологій наповнення якої необхідно проводити на основі космічних знімків у видимому діапазоні з розрізненістю ~0,5 м та можливістю автоматизованого оцінювання зміни обстановки у часі з переривом не більше 3 діб.

Додатково використання геоінформаційної системи буде спрощувати вирішення таких основних завдань:

доведення до органів управління та військ (сил) цифрової картографічної інформації про місцевість і об'єкти на ній;

генералізацію (масштабування) цифрової картографічної інформації;

створення, розповсюдження і накопичення в електронному вигляді графічних документів.

Іншим прикладом є комплексування різноструктурних даних в межах одного часового інтервалу (протягом першої половини дня), де дані про один і той самий об'єкт отримані від БпАК це – фотознімок у видимому діапазоні, а від КА дистанційного зондування Землі – багатоспектральний знімок. Такий підхід дозволяє виділити зв'язок з просторовими і спектральними аналітичними моделями, а при наявності бібліотек спектральних еталонів дозволить використовувати спектрально-просторовий (субпіксельний) аналіз результатом якого повинна стати автоматична ідентифікація наземних об'єктів на поверхні Землі.

Для удосконалення процесу організації збору інформації про противника в ході проведення ООС із використанням засобів видового спостереження повітряно-космічного базування пропонується проводити комплексування даних від цих джерел за структурно-логічною схемою поданою на рис. 1.

По суті основною відправною точкою реалізації роботи структурно-логічної схеми комплексування даних з різних засобів повітряно-космічного базування є постановка завдання. Слід розуміти, що головна залежність вироблення необхідного завдання для подальшого забезпечення військ (сил) розвідувальною інформацією буде пов'язана не лише з потребами добування розвідувальних відомостей про противника, а й від тактико-технічних характеристик (ТТХ) доступних на момент виконання завдання видових засобів спостереження повітряно-космічного базування, вибір яких при плануванні та застосуванні буде здійснюватися на основі рішення багатокритеріальної задачі на що додатково впливатимуть фактори природного чи антропогенного характеру (у тому числі наявність протиборчих систем противника, наприклад, засобів радіоелектронної боротьби). Також на цей процес впливатиме апріорна розвідувальна інформація, яка паралельно може надходити, як по каналам оперативної інформації так і по каналам від спеціалізованої бази даних (БД).

Основним принципом побудови добування розвідувальних відомостей про противника має стати оптимальний розподіл зусиль між засобами повітряно-космічного базування. В рамках існуючого протиріччя, постає завдання щодо вирішення багатокритеріальної задачі яка потребує вибору достатніх засобів добування розвідувальних даних та визначення послідовності

їх застосування. Оптимізаційний підхід передбачає використання математичних моделей і критерію оптимізації в явному вигляді. Основою для вирішення такої задачі є пошук альтернативи, яка є найкращою з точки зору деякого критерію. Такий підхід дає можливість підвищити якість рішення за рахунок таких факторів:

дозволяє знаходити варіанти розв'язку задачі при різних значеннях реальних обмежень на змінні

та різних початкових умовах.

дозволяє спростити процедуру вибору кращого рішення завдяки використанню аналітичних критеріїв, при цьому можна одночасно використати декілька критеріїв;

наявність множини методів розв'язання задач динамічної оптимізації дає можливість вибрати кращу альтернативу.

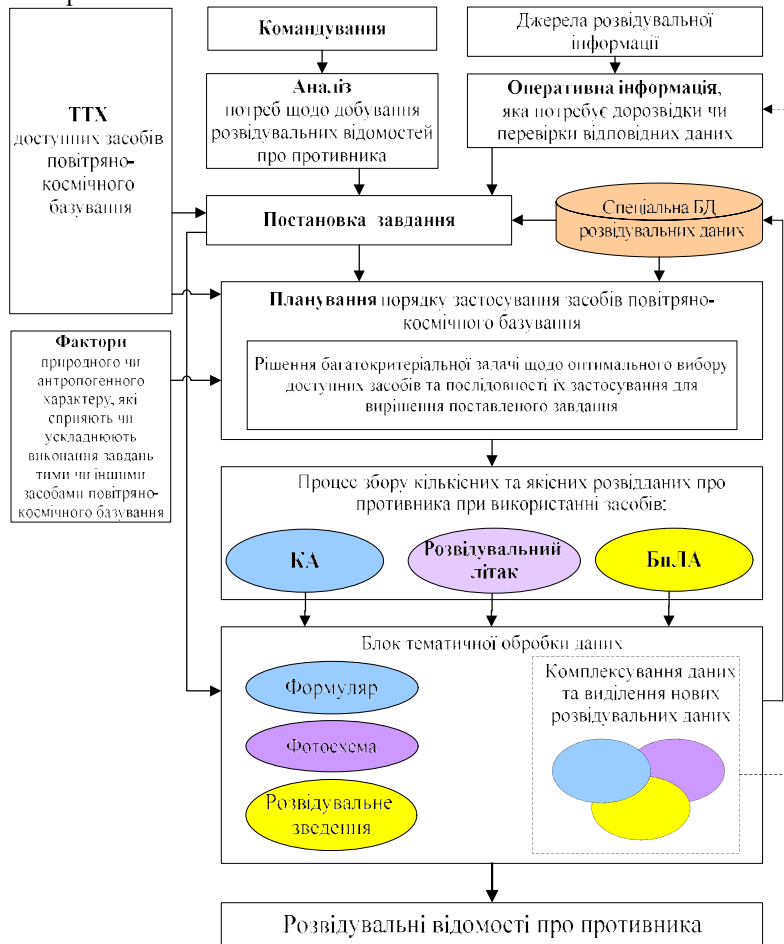


Рис. 1. Структурно-логічна схема комплексування даних з різних засобів видового спостереження повітряно-космічно базування

Відповідно до цього на схемі, що представлена на рис. 1 запропоновано ввести блок формування та узагальнення факторів які сприятимуть або ускладнюватимуть виконання завдань і враховуватимуться в процесі планування при вирішенні багатокритеріальної задачі. З урахуванням математичної формалізації завдання в певний фіксований момент часу при прийнятті рішення щодо застосування того чи іншого засобу повітряно-космічного базування вектор  $r$  прийме фіксоване значення. В такому випадку функція корисності для прийняття рішення може бути представлена скалярною згортокою часткових критеріїв [12]:

$$\Phi = [y(x), r]_{r=r^0} = Y[y(x), r]^0, \quad (1)$$

де:  $Y[y(x), r]^0$  – скалярна згортка побудована за схемою компромісів, адекватної заданій ситуації.

Якщо вектор критеріїв  $y(x)$  пронумерований вектором обмежень  $A$  з урахуванням початкових умов у вигляді трьох основних складових, таких як: ТТХ засобів повітряно-космічного базування; очікуваний результат відповідно до поставленого завдання; данні від спеціалізованої бази

розвідувальних даних, то:

$$y_0(x) = \{y_k(x) / A_k\}_{k=1}^s, \quad (2)$$

В такому випадку рішення багатокритеріальної задачі можна обмежити лінеаризованою моделлю:

$$Y[y_{ok}(x)]^0 = \sum_{k=1}^s a_k^0 y_0(x), \quad (3)$$

де:  $a_k^0$  – вагові коефіцієнти, які представляють собою вектор  $a^0 = \{a_k^0\}_{k=1}^s \in \Gamma_a$ , що визначений на симплексі  $\Gamma_a = \{a \mid a_k \geq 0, \sum_{k=1}^s a_k = 1\}$ .

Такий підхід, без сумніву володіє перевагами простоти але поряд з тим характеризується рядом недоліків, які притаманні методу лінеаризації. Як правило лінійна модель приводить до правильного результату у невеликому колі навколо робочої точки, положення якої залежить від ситуації прийняття багатокритеріального рішення. Відповідно будь яка зміна ситуації за заданою схемою на рис.1 вимагає нового визначення вагових коефіцієнтів моделі.

Варто відмітити важливість та необхідність

створення спеціалізованої бази розвідувальних даних, доступ до якої для всіх відповідних рівнів має бути організований саме із впровадженням автоматизованої системи управління й формування єдиного інформаційно-комунікаційного простору. Відповідно, такі дані мають стати основою для планування щодо

застосування засобів видового спостереження повітряно-космічного базування та усвідомлення завдань командирами на тактичному рівні. А варіанти тематичної обробки доцільно було б оптимізувати за напрямками добування інформації, що представлені на рис.2.

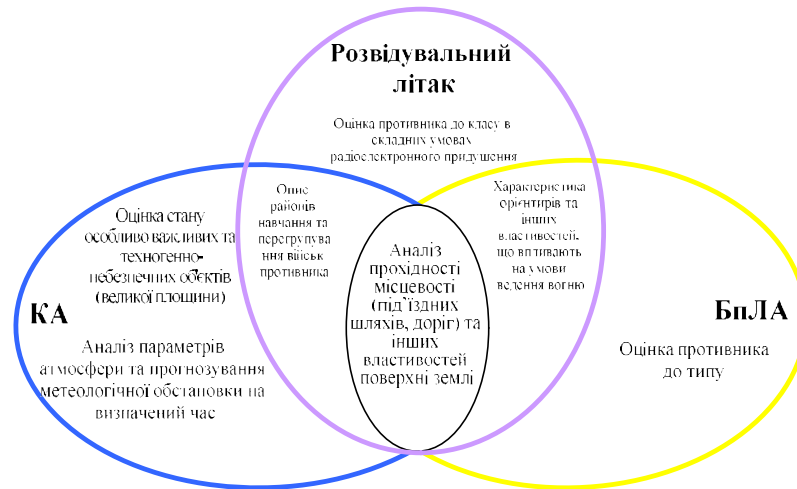


Рис. 2. Характеристика даних, які варто використовувати в процесі комплексування

З рис. 2 можна побачити, що при відповідному плануванні та застосуванні КА і розвідувальних літаків об'єднання інформації можливо проводити за двома напрямками: опис районів спостереження та перегрупування військ противника і аналіз прохідності місцевості та інших властивостей поверхні Землі, тоді, як при застосуванні КА і БпЛА лише за одним (аналіз прохідності місцевості та інших властивостей поверхні Землі). При цьому слід розуміти, що таке подання не обмежується лише зазначеними напрямками. Важливо відмітити той факт, що дані від КА можна використовувати, як апіорні для планування і застосування БпЛА з метою уточнення даних про противника та його оцінки до типу об'єктів шляхом дешифрування матеріалів повітряної розвідки отриманих з БпЛА. Такий підхід обмежується лише творчістю та кваліфікацією користувачів даної інформації. Але ефективне використання повітряно-космічної компоненти неможливе без створення багатофункціональної та інтегрованої інфраструктури систем обміну інформацією між добувними підрозділами і споживачами. А комплексування інформації від КА, літаків та БпЛА на різних рівнях її отримання і проходження дозволить заповнювати пробіли інформаційно-розвідувальної діяльності та більш повно розкривати наміри та дії противника.

### Висновки й перспективи подальших досліджень

Проведений в роботі огляд сучасних тенденцій

### Література

1. Історія війн та військового мистецтва. Навч. Посібник / Під заг.ред. С. І. Береснева та інш. – Х.: ХУ ПС, 2007. – 230 с. 2. Розвиток військового мистецтва в локальних війнах 90-х років ХХ ст. – К.: НАУО, 2003. – 109 с. 3. Дробаха Г.А. Розвиток тактики дій засобів повітряного нападу в локальних конфліктах ХХІ століття / Г. А. Дробаха, С. М. Піскунов, І. М. Тихонов // Збірник наукових праць. – Житомир : ЖВІ ДУТ, 2015. – Випуск 10. – С. 87–94. 4. Davis J.R. Defending Future Hybrid Threats / J.R. Davis // Military Review. – Fort Leavenworth, September-October 2013. – No.5. – P. 21- 29. 5. Попов М. О. Видова космічна розвідка в локальних

ведення збройної боротьби дозволив виробити ряд підходів реалізації яких дозволить підвищити повноту та достовірність розвідувально забезпечення Збройних Силах України. Це сприятиме організації та плануванню діяльності військ (сил) в операції Об'єднаних сил і дасть змогу більш раціонально розподілити та використовувати ресурс засобів видового спостереження повітряно-космічно базування. Для цього запропоновано вирішення багатокритеріальної задачі за схемою компромісів обмеженою лінеаризованою моделлю щодо вибору достатніх засобів добування розвідувальних даних та визначення послідовності їх застосування. Створення спеціалізованої бази розвідувальних даних, мають стати не лише апіорною основою для планування із застосування засобів видового спостереження повітряно-космічного базування, а за рахунок доступу до неї споживачів на усіх рівнях (включаючи тактичний).

Подальші дослідження необхідно спрямувати на вирішення проблем щодо розширення можливостей використання даних космічного сегменту за рахунок побудови приймальних комплексів інформації з іноземних космічних апаратів. Удосконалення методів комплексування різномірної інформації на основі геоінформаційних технологій. Розширення можливостей застосування БпЛА в складних умовах радіоелектронного подавлення зі сторони противника.

військових конфліктах / М. О. Попов, М. В. Топольницький, В. О. Подліпаєв // Наука і оборона. – 2015. – № 1. – С. 25–35. 6. <https://www.facebook.com/pressjfo.news/?ref=search> (Сторінка Операція об'єднаних сил / Joint Forces Operation). 7. <https://ukr.media/news-ato/> 8. <https://112.ua/ato>. 9. <https://www.slovoidilo.ua/2019/02/17/karta/karta-oos-sytuacziya-sxodi-ukrayiny-17-lyutoho>. 10. Zibtsev S. Wildfires Risk Reduction From Forests Contaminated by Radionuclides: A Case Study of the Chernobyl Nuclear Power Plant Exclusion Zone / S. Zibtsev // Living with fire Addressing global change thought integrated fire

management (International wildland fire conference Sun City, South Africa, 9–13 May 2011). – Sun City, 2011. – P. 23. **11. Ковбасюк С. В.** Методичні підходи до процесу дешифрування даних дистанційного зондування Землі середньої розрізненості в інтересах національної безпеки й оборони / С. В. Ковбасюк, Д. Л. Федорчук, Г.

Д. Носова // Збірник наукових праць. – Житомир : ЖВІ ДУТ, 2015. – Випуск 10. – С. 87–94. **12.** Многокритериальные решения: модели и методы: монография / А.Н.Воронин, Ю.К.Зиатдинов, М.В.Куклинский. – К.: НАУ, 2011. – 348 с.

**ПЕРСПЕКТИВЫ КОМБИНИРОВАННОГО ИСПОЛЬЗОВАНИЯ ВИДОВЫХ СРЕДСТВ ВОЗДУШНО-КОСМИЧЕСКОГО БАЗИРОВАНИЯ ДЛЯ ПОВЫШЕНИЯ ИНФОРМАТИВНОСТИ РАЗВЕДЫВАТЕЛЬНОГО ОБЕСПЕЧЕНИЯ ВОЙСК (СИЛ)**

*Леонид Брониславович Каневский (кандидат технических наук)  
Максим Сергійович Повх  
Сергій Миколайович Шумський*

*Национальный университет обороны Украины имени И. Черняховського, Киев, Украина*

*В статье проведен анализ возможностей выполнения заданий разведывательного обеспечения войск (сил) относительно определения положения и прогнозирования характера действий противника по информации от видовых средств наблюдения что базируются в воздушно-космическом пространстве за опытом антитеррористической операции и операции Объединенных сил. Определено, что существующие подходы в Вооруженных Силах Украины являются не достаточными и нуждаются в развитии и усовершенствовании.*

*С целью частичного решения данной проблемы были рассмотрены подходы комплексного использования средств воздушно-космического базирования. Предложен алгоритм для выбора оптимального способа добывания достоверных сведений о составе группировке, действий и намерений противника.*

*Внедрение предложенных подходов позволит: повысить информативность разведывательного обеспечения Вооруженных Силах Украины, что будет способствовать организации и планированию деятельности войск (сил) в операции Объединенных сил, более рационально распределить и использовать ресурс средств воздушно-космического базирования.*

**Ключевые слова:** космические аппараты двойного назначения, геоинформационные технологии, беспилотные авиационные комплексы, информационного обеспечения войск (сил).

**PROSPECTS OF COMBINED USE OF SPECIFIC AIRCRAFT BASES FOR IMPROVEMENT OF INFORMATIVE SENSITIVENESS**

*Leonid Kanevskyy (Candidate of technical sciences)  
Maksym Povkh  
Serhii Shumskyy*

*National Defense University of Ukraine named after Ivan Cherniakhovskyy, Kyiv, Ukraine*

*The article analyzes the capabilities of troops (forces) informational support task performance concerning the enemy position and modus operandi based on the Anti-Terrorist Operation and Joint Forces Operation. It was identified that currently the approaches of intelligence and informational support existing in the Armed Forces of Ukraine in the area of military security context are insufficient and this situation requires searching for some methods for raising its efficiency.*

*For the partial solution of this problem there have been examined the approaches of the air and space basing assets combined use. The algorithm was suggested for choosing the optimal way of reliable data acquisition concerning the enemy forces composition, activities and intentions.*

*The introduction of suggested ways will enable to: increase the intelligence and informational support awareness of the Armed Forces of Ukraine promoting better troops (forces) activity organization and planning in the Joint Forces Operation, to distribute and utilize the resources of the air and space basing assets more efficiently.*

**Key words:** dual-purpose space vehicles, geo-informational technologies, unmanned areal complexes, troops (forces) informational support.

**References**

1. History of wars and martial arts. Educ. Manual / Under the editorship SI Beresneva et al. - X. : XY ПС, 2007. - 230 p. **2.** The development of martial arts in the local wars of the 90's of the twentieth century. - K. : NAUO, 2003. - 109 p. **3. Drobakh GA** The development of tactics of air attack in local conflicts of the XXI century / GA Drobakh, SM Piskunov, IM Tikhonov // Collection of scientific works. - Zhytomyr: THE LIFE OF DUT, 2015. - Issue 10. - P. 87-94. **4. Davis J.R.** Defending Future Hybrid Threats / J.R. Davis // Military Review. - Fort Leavenworth, September-October 2013. - No.5. - P. 21- 29. **5. Popov MO** Specific space exploration in local military conflicts / MA Popov, MV Topolnitsky, VO Podlipayev // Science and Defense. - 2015. - № 1. - P. 25–35. **6.** <https://www.facebook.com/pressjfo.news/?ref=search> (Joint Forces Operation page). **7.** <https://en.media/news-ato/> **8.** <https://112.ua/ato>

**9.** <https://www.slovoidilo.ua/2019/02/17/karta/karta-oos-sytuacziya-sxodi-ukrayiny-17-lyutoho>. **10. Zibtsev S.** Wildfires Risk Reduction From Forests Contaminated by Radionuclides: A Case Study of the Chernobyl Nuclear Power Plant Exclusion Zone / S. Zibtsev // Living with fire Addressing global change thought integrated fire management (International Wildland Fire Conference Sun City, South Africa, 9–13 May 2011). - Sun City, 2011. - P. 23. **11. Kovbasyuk SV** Methodical approaches to the process of decryption of data of remote sensing of the Earth of average disparity in the interests of national security and defense / SV Kovbasyuk, DL Fedorchuk, G. D. Nosova // Collection of scientific works. - Zhytomyr: THE LIFE OF DUT, 2015. - Issue 10. - P. 87-94. **12.** Multicriteria solutions: models and methods: a monograph / AN Voronin, Yu.K. Zioldinov, MV Kuklinsky. - K. : NAU, 2011. - 348 p.

Алі Енверович Бекіров (кандидат технічних наук)<sup>1</sup>

Володимир Жоржевич Яценюк (кандидат технічних наук, доцент)<sup>1</sup>

Олександр Станіславович Крейдун<sup>2</sup>

<sup>1</sup>Харківський національний університет Повітряних Сил ім. Івана Кожедуба, Харків, Україна

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

## ТЕХНОЛОГІЯ СЕЛЕКЦІЇ ОБЛАСТЕЙ АЕРОФОТОЗНІМКУ З РІЗНОЮ НАСИЧЕНІСТЮ ДЛЯ СТЕГАНОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

Сучасні системи збору та обробки інформації широко представлені оптичними системами моніторингу, які використовуються для ведення повітряної розвідки, моніторингу об'єктів критичної інфраструктури і транспортних комунікацій. Проблемними обмеженнями при розробці нових та удосконалення існуючих систем є підвищення вимог кінцевого користувача щодо якості цифрових зображень в умовах обмеження пропускної здатності каналів передачі даних. Для зменшення обсягів аерофотознімків пропонується використовувати стеганографічні перетворення з селекцією областей різної семантичної насиченості.

В статті проводиться аналіз можливості селекції об'єктів інтересу за допомогою методів машинного розпізнавання контурної інформації на основі ковзаючої маски. Для усунення системних обмежень зазначеного підходу, які полягають у відсутності можливості виявлення елементів опису об'єкту інтересу, пропонується використовувати операцію згортки на основі набору фільтрів. Розробляється технологія селекції незначимих областей, які використовуються як контейнери для вбудовування інформації та областей з об'єктами інтересу, як корисного стеганографічного повідомлення. Перший етап передбачає вибір незначимих областей на основі коефіцієнту різниці елементів. На другому етапі відбувається фільтрація зображення на основі операції згортки з набором фільтрів, які відповідають очікуваному відгуку зображення після фільтрації.

**Ключові слова:** стеганографічне перетворення, операція згортки, системи моніторингу, виявлення об'єктів.

### Вступ

Розвиток і постійне вдосконалення технологій збору, обробки і передачі інформації впливає підвищення ефективності функціонування систем моніторингу. Процес імплементації нових підходів відбувається не тільки в технічних рішеннях, але в більшій мірі, в математичних алгоритмах обробки даних [1].

**Постановка проблеми.** Системи збору інформації широко представлені оптичними системами моніторингу з формування видових зображень. До областей застосування таких систем відносяться: повітряна розвідка, моніторинг транспортних комунікацій і об'єктів критичної інфраструктури держави. В умовах гібридного протистояння підвищується значимість таких систем моніторингу, а значить, і підвищуються вимоги кінцевого отримувача до якості видових зображень і оперативності їх доставки. Так з одного боку, потрібно забезпечити доступність видових зображень заданої якості в режимі реального часу в тому числі в умовах застосування алгоритмів гарантованого захисту інформації. З іншого боку, канали передачі видових зображень мають обмежену пропускну здатність. Рішення проблеми зниження обсягів видових зображень здійснюється на основі використання методів компресії цифрових зображень. В цьому випадку зниження необхідних обсягів даних

здійснюється за рахунок усунення статистичної та психовізуальної надлишковості зображень. Обмеженнями даних методів при вирішенні задачі компресії видових зображень є відсутність можливості селекції областей з різною семантичною насиченістю [2].

Іншим напрямком цифрової обробки зображень, який активно розвивається є методи цифрової стеганографії. Алгоритми стеганографії передбачають вбудовування корисної інформації в цифрові зображення. В основі, завданням методів стеганографії є забезпечення конфіденційності даних шляхом візуального приховування інформації від стороннього спостерігача. Вбудовування інформації здійснюється за допомогою заміни частин зображення, які мають психовізуальну надлишковість. Іншим можливим напрямком використання стеганографії є зменшення обсягів видових зображень.

У цьому випадку в якості корисної вбудованої інформації використовуються такі частини зображення, які визначаються як значущі для кінцевого користувача. І навпаки в якості контейнерів пропонується використовувати складові зображення, які можуть позначатися як менш значущі. [3-7].

**Метою статті** є розробка методу селекції областей видових аерофотознімків для стеганографічного вбудовування.

### Огляд методів виділення контурної інформації

Серед існуючих стеганографічних методів вбудовування найбільш поширеними є алгоритми безпосередньої заміни елементів  $\{a_{ij}\}$  представлення зображення-контейнера  $A$  елементами інформаційного повідомлення  $\{b_h\}$  на основі наступного виразу [8,9]:

$$a'_{ij} = b_h, \quad A' = \{a_{11}, a_{12}, \dots, a'_{ij}, \dots, a_{n,m}\},$$

де  $A'$  - зображення, що містить вбудовані елементи  $a'_{ij}$ .

Тут  $b_h$  -  $h$ -й елемент, інформаційної послідовності, що вбудовується,  $V = \{b_1; \dots; b_h; \dots; b_H\}$ ,  $i = 1, n$ ,  $j = 1, m$ ,  $h = 1, H$ .

Методи безпосередньої заміни широко представлені алгоритмами заміни найменш значущих біт елементів зображення-контейнера. В даному випадку молодші біти відповідають за найменшу зміну градацій яскравості елемента контейнера і мають шумову природу. Ступінь внесених в зображення-контейнер спотворень PSNR прямо пропорційно обсягу  $W_{em}$  вбудовуваної інформації. Для усунення сформульованих обмежень пропонується підхід, який заснований на селекції областей зображення з різною семантичною насиченістю з подальшим категорюванням на області для вбудовування і області, які виступають в якості вбудованої інформації. Тоді всі сегменти  $\{A_{\alpha\beta}\}$  вихідного зображення  $A$  розбиваються на дві підмножини:

підмножина сегментів  $A_{\alpha\beta}^{(незнач)}$  зображення з незначною семантичною насиченістю, ;

підмножина сегментів  $A_{\alpha\beta}^{(знач)}$  вихідного зображення з об'єктами інтересу.

В цьому випадку всі сегменти  $\{A_{\alpha\beta}\}$  можуть розглядатися, як множина  $\{C\}$  контейнерів для стеганографічного вбудовування та множина  $\{B\}$  вбудовуваних інформаційних повідомлень, що задаються наступним виразом:

$$A_{\alpha\beta} \in \begin{cases} C, & A_{\alpha\beta} \rightarrow A_{\alpha\beta}^{(незнач)}; \\ B, & A_{\alpha\beta} \rightarrow A_{\alpha\beta}^{(знач)} \end{cases}$$

Для селекції областей аерофотознімка з різною семантичною насиченістю часто використовують підходи на основі теорії машинного розпізнавання. Методи машинного розпізнавання засновані на обробці та фільтрації зображення з метою пошуку та аналізу ознак, що характеризують класи областей. Значна область аерофотознімка має велику кількість значущих для кінцевого користувача областей і навпаки, незначний сегмент характеризується великою кількістю другорядних незначущих областей.

При вирішенні задачі класифікації областей аерофотознімка важливим є визначення ознак

об'єктів, які виступають для користувача об'єктами інтересу. Об'єктами інтересу для систем аеромоніторинга спеціального призначення виступають об'єкти інфраструктури, дороги і магістралі, будівлі та споруди, транспортні засоби і т.д. З позиції синтаксичного представлення, об'єкти інтересу характеризуються побудовою за допомогою елементів просторового представлення зі схожими значеннями. У той же час межі об'єктів інтересу можна розглядати як стик однорідних областей. В цьому випадку сусідні елементи просторового представлення контурів об'єктів будуть характеризуватися значними перепадами.

Найбільш поширені і вживані на практиці підходи виявлення контурів об'єктів аерофотознімка є градієнтні методи. Градієнтні методи засновані на локальному визначенні значення збільшення яскравості (градієнта) і напрямлення їх найбільшої зміни. Подальша обробка передбачає визначенням максимальних значень градієнта яскравості, їх статистичної обробки і розподілу на рівні. В даному випадку рівні можуть бути інтерпретовані як ступені семантичної значущості аерофотознімка.

Найбільш поширеним способом пошуку контурів є обробка зображення  $A$  ковзаючою маскою  $G$ . Маска  $G$  являє собою квадратну матрицю з коефіцієнтами  $\{g\}$  (рис 1).

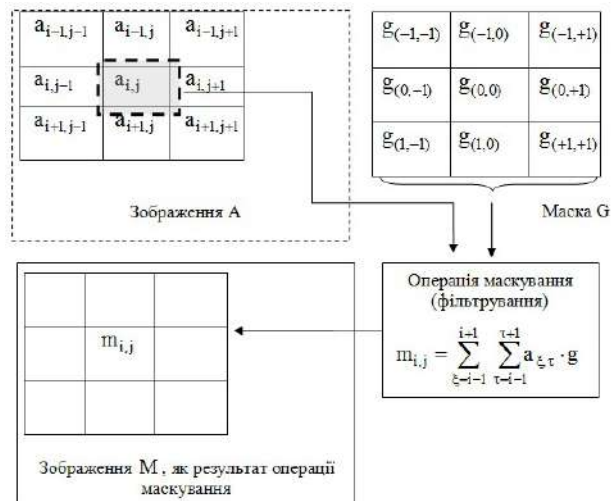


Рис 1. Схема реалізації фільтрації зображення на основі ковзаючої маски

Процес обробки зображення  $A$  на основі матриці  $G$  називається фільтрацією або маскуванням і задається наступним функціоналом  $f(\bullet)$ :

$$M = f(A, G),$$

де  $M$  - зображення, отримане внаслідок обробки зображення  $A$  на основі маски  $G$ .

Процес фільтрації заснований на поступовому просторовому переміщенні маски фільтра від елемента до елемента зображення. Значення елемента  $g_{ij}$  (результат фільтрації) розраховується з урахуванням попередніх і наступних елементів в двовимірному просторі.

На рисунку 2 представлені результати операції маскування аерофотознімка на основі оператора Собеля з різними рівнями бінарізації.



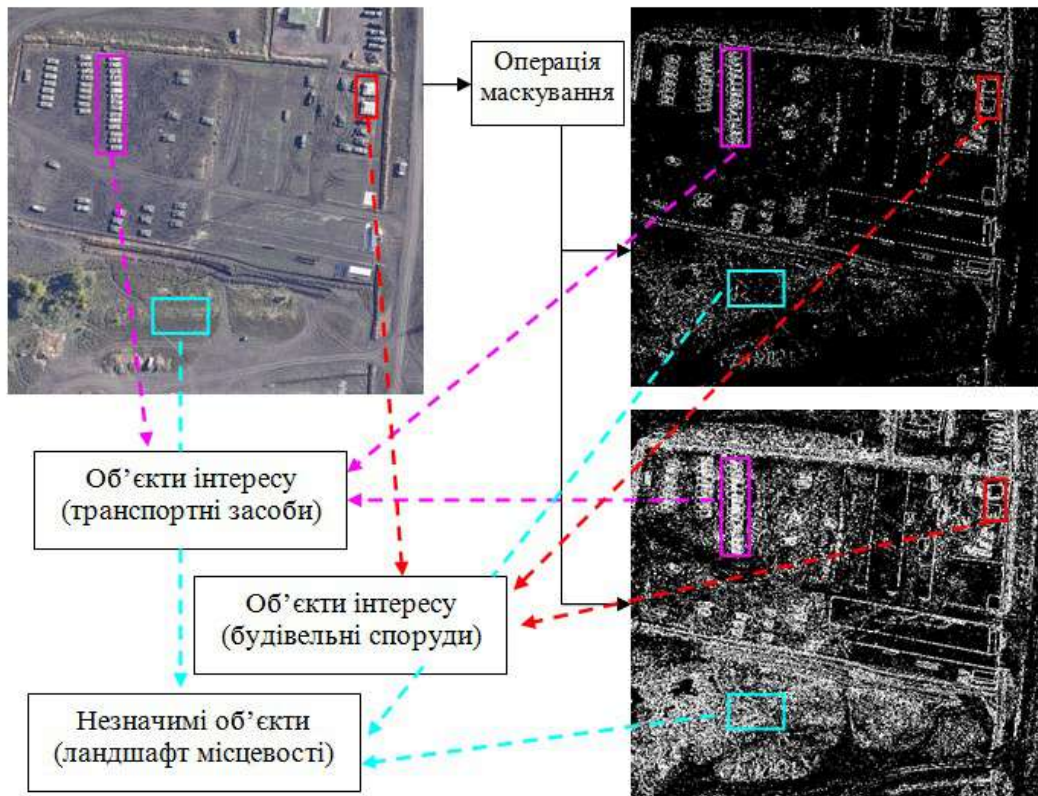


Рис. 3. Результати операції маскуванн на основі оператора Собеля.

З аналізу результатів на рис 2 можна зробити наступні висновки:

для маски аерофотознімка з високим рівнем бінарзації (варіант А) забезпечується детектування контурної інформації об'єктів інтересу, але при цьому не виділяються позиції елементів, які безпосередньо описують об'єкт;

для результатів маскуванн з високим рівнем бінарзації (варіант А) характерна присутність контурної інформації незначущих об'єктів;

маскуванн з низьким рівнем бінарзації (варіант Б) дозволяє виділити не тільки контурну інформацію про об'єкти інтересу, але і позначити позицію елементів синтаксичного опису об'єкта;

маска (варіант Б) містить велику кількість контурів незначущих об'єктів.

Значить, існуючі підходи виявлення контурної інформації цифрових зображень не в повній мірі забезпечують вимоги для селекції областей з різною семантичною насиченістю для стеганографічного перетворення.

### Розробка технології селекції областей з різною семантичною насиченістю

Для формуванн контейнерів та інформаційних повідомлень для компресійно-стеганографічного перетворення пропонується розробити механізм селекції елементів.

З огляду на те, що етап попередньої вибірки передбачає обробку кожного елемента вихідного аерофотознімка, для зменшення обчислювальної складності механізм селекції пропонується виконувати в два етапи.

Перший етап характеризується обчисленням коефіцієнта К різниці елементів в рамках одного

блоку. Коефіцієнт К визначається як різниця максимального елемента  $a_{kl,max}$  і мінімального елемента  $a_{kl,min}$  блоку на основі виразу:

$$K = a_{kl,max} - a_{kl,min}, \alpha = \overline{1, \theta}, \beta = \overline{1, \Gamma},$$

де  $a_{kl,max}$  - максимальний елемент в k рядку l-му стовпці блоку  $A_{\alpha\beta}$  вихідного аерофотознімка

$$A, \quad k = \overline{1, K}, \quad l = \overline{1, L}.$$

Від значення коефіцієнта К залежить до якого класу насиченості відноситься блок  $A_{\alpha\beta}$  аерофотознімка:

$$A_{\alpha\beta} = \begin{cases} A_{\alpha\beta}^{(незнач)} & \rightarrow \Delta K \geq K_{kl}; \\ A_{\alpha\beta}^{(знач)} & \rightarrow \Delta K < K_{kl}; \end{cases}$$

де  $\Delta K$  - порогове значення коефіцієнта різниці елементів.

На першому етапі селекція передбачає первинне виділення незначущих блоків  $\{A_{\alpha\beta}^{(незнач)}\}$  з всіх блоків  $\{A_{\alpha\beta}\}$  як контейнерів для компресійного стеганографічного перетворення.

Порогове значення  $\Delta K$  визначає кількість значущих і незначущих блоків. У разі, коли значення коефіцієнта  $\Delta K$  збільшується, то кількість незначущих блоків  $\{A_{\alpha\beta}^{(незнач)}\}$  також збільшується, а кількість блоків  $\{A_{\alpha\beta}^{(знач)}\}$  зменшується:

$$\Delta K \uparrow \rightarrow A_{\alpha\beta}^{(знач)} \downarrow \cup A_{\alpha\beta}^{(незнач)} \uparrow.$$

У протилежному випадку виконується наступна умова:

$$\Delta K \downarrow \rightarrow A_{\alpha\beta}^{(\text{знач})} \uparrow \cup A_{\alpha\beta}^{(\text{незнач})} \downarrow.$$

Якщо значення коефіцієнта  $\Delta K = 0$ , тоді всі елементи  $\{a_{kl}\}$  блоку  $A_{\alpha\beta}$  прийматимуть однакове значення.

Другий етап передбачає застосування до аерофотознімка операції згортки. Під операцією згортки передбачається послідовна обробка кожного елемента просторового представлення аерофотознімка плаваючою згорткою  $G$ :

$$G = \begin{bmatrix} g_{11} & \dots & g_{1v} & \dots & g_{1Y} \\ \vdots & & \vdots & & \vdots \\ g_{y1} & \dots & g_{yv} & \dots & g_{yY} \\ \vdots & & \vdots & & \vdots \\ g_{Y1} & \dots & g_{Yv} & \dots & g_{YY} \end{bmatrix}, \quad y = \overline{1, Y}, \quad v = \overline{1, V},$$

де  $g_{yv}$  - елемент згортки  $G$  в  $Y$ -ому рядку  $V$ -ому стовпці.

Відповідь  $a'_{kl}$  для кожного елемента  $a_{kl}$  вихідного аерофотознімка визначається на основі формули:

$$a'_{ij} = \sum_{y=1}^Y \sum_{v=1}^V g_{yv} \cdot a_{k+y-f, l+v-z};$$

де:  $f$  - оператор зміщення згортки по рядках

$$f = \left\lfloor \frac{Y}{2} \right\rfloor + 1;$$

$z$  - оператор зміщення згортки за стовпцями

$$z = \left\lfloor \frac{V}{2} \right\rfloor + 1.$$

Структурна схема механізму селекції блоків представлена на рис 4.

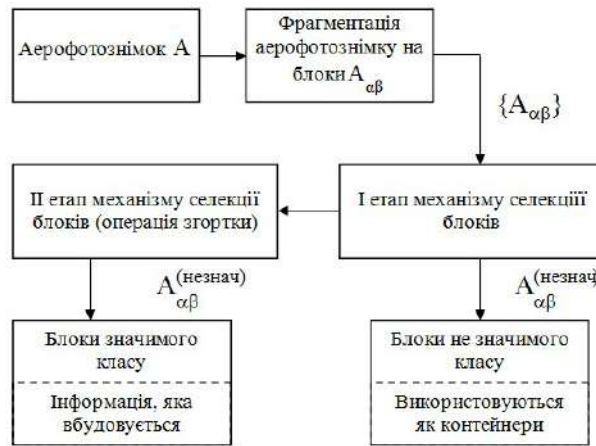


Рис 4. Структурна схема механізму селекції блоків.

Операція згортки є фільтрацією і дозволяє виділити ознаки цифрового зображення, які максимально відповідають значенням і взаємному розташуванню елементів в згортці. Тут елемент  $a'_{kl}$  блоку після фільтрації буде приймати максимальне значення в разі, коли метрика  $\varphi(A_{\alpha\beta}; G)$ , яка характеризує ступінь відмінності між елементами блоку  $A_{\alpha\beta}$  і елементами згортки  $G$  буде мінімальною.

Фільтрація цифрового зображення виконується набором згорток, які представляють собою набір фільтрів з коефіцієнтами, які описують очікуваний відгук. Позиція коефіцієнтів і їх значення в згортці визначається з урахуванням ознак, які містять об'єкти інтересу. Після операції згортки виконується бінаризація зображення за рівнями. Результати фільтрації аерофотознімка з набором ознак представлені на рис 5.

Порівняльна оцінка запропонованого методу селекції та методу виявлення на основі операції маскування проводилось по величині  $Q_1$  процентного відношення виявлених елементів об'єктів інтересу на основі програмної реалізації за формулою:

$$Q_1 = \frac{Q_{\text{знач}}}{n * m},$$

де  $Q_{\text{знач}}$  - кількість значимих елементів аерофотознімка, виявлених на основі програмної моделі.

Результати оцінки ефективності селекції представлені в таблиці 1.

Таблиця 1  
Результати оцінки ефективності селекції областей

Метод обробки	Рівні бінаризації	Q1, %	Q0, %	Q істин
Маскування (оператор Собеля)	Верхній рівень	71,97	28,03	~ 8
	Нижній рівень	93,05	6,95	~ 8
Операція згортки	Верхній рівень	93,34	6,66	~ 8
	Нижній рівень	96,88	3,12	~ 8

З аналізу результатів в таблиці 1 та рис. 5 можна зробити висновок, що значення  $Q_1$  для розробленого методу наближається до істинного значення, при цьому забезпечується висока ступінь виявлення об'єктів інтересу і низька ступінь виявлення не значимих областей.

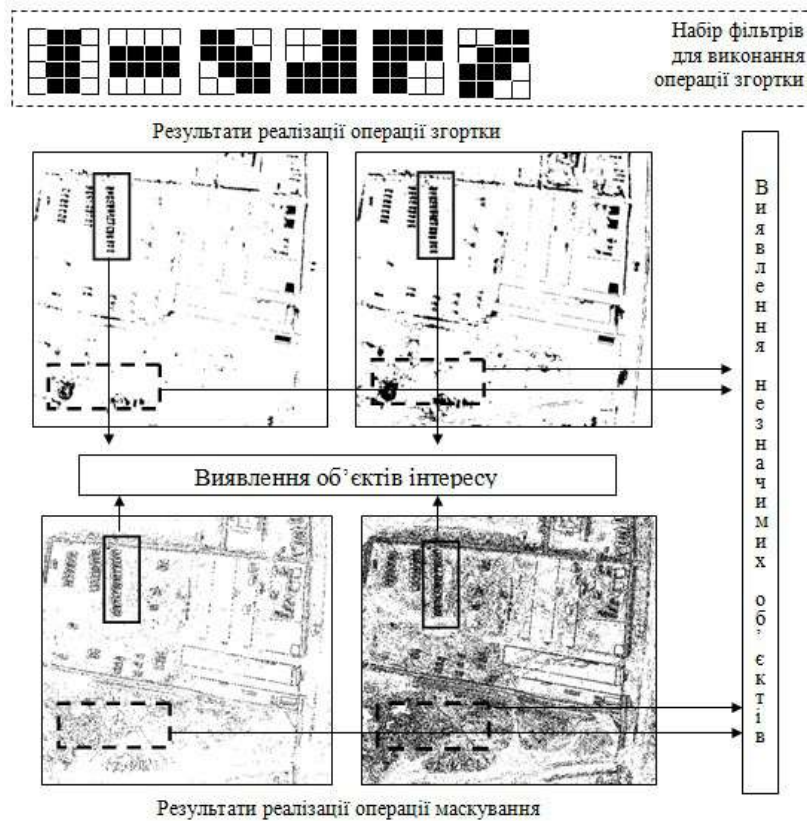


Рис.5. Структурна схема механізму селекції блоків

### Висновки й перспективи подальших досліджень

Проведено аналіз особливостей функціонування оптичних систем моніторингу. Для усунення обмежень, обумовлених підвищенням вимог кінцевого користувача до якості цифрових зображень, запропоновано використовувати методи стеганографічних перетворень. Такий підхід передбачає використання визначених частин аерофотознімку у якості контейнера для вбудовування. Інші частини цифрового зображення уявляють собою корисну інформацію для вбудовування.

Для забезпечення зменшення спотворень у вихідне зображення в процесі стеганографічного вбудовування пропонується здійснювати селекцію блоків аерофотознімку на значимі та незначимі для кінцевого користувача. В цьому випадку блоки без об'єктів інтересу будуть використовуватись у якості контейнера, і навпаки, значимі блоки уявляють собою корисну інформацію.

### Література

1. Al-Shatnawi A.M. A new method in image steganography with improved image quality / Atallah M. Al-Shatnawi // Applied Mathematical Science, Vol. 6, 2012, no. 79, p. 3907-3915.  
 2. Бекіров А.Е. Метод захисту інформації на основі стеганографічних систем // Озброєння та військова техніка. – 2015. – №1 – С. 29 – 36.  
 3. Бекіров А.Е. Пути повышения информационной безопасности ресурсов в системах специального назначения / Баранник В.В., Рябуха Ю.Н., Бекіров А.Е., Комолов Д.И. // Четверта міжнародна науково-практична конференція [«Інформаційні технології та комп'ютерна інженерія»], (Вінниця, 28 - 30 травня 2014 р.) / Вінницький національний технічний університет, Вінниця, 2014. – С. 151.  
 4. Avinash K. Gulve A high capacity secured image steganography method with five pixel pair differencing and LSB substitution / Avinash K. Gulve, Madhuri S. Joshi // IJ. Image. Graphics and Signal Procusing, 2015, 5, p 66-74.

Проведено аналіз методів машинного розпізнавання контурної інформації на основі ковзаючої маски (оператор Собеля). Визначений метод виявляє перепади значень елементів просторового представлення на стиках однорідних областей, які уявляють собою контури об'єктів. Обмеженнями використання операції маскуванія при селекції блоків є відсутність можливості визначення елементів представлення аерофотознімку, які описують об'єкти інтересу.

Для усунення виявлених обмежень пропонується технологія селекції блоків з різною семантичною значимістю Перший етап технології передбачає селекцію блоків на основі коефіцієнту різниці елементів. На другому етапі виконується операція згортки на основі набору фільтрів, які описують відгук фільтрації, що очікується.

Проведено порівняльний аналіз методу виявлення об'єктів на основі маскуванія та операції згортки.

5. Horoshko V.A. Metody i sredstva zashchity ifnornacii. / Horoshko V.A., Chekatov A.A. –K.: Junior, 2003. – 501s.  
 6. Judin O.K. Zahist informacii v mrezhah peredachi danih: pidruchnik / G.F. Konahovich, O.G. Korchenko, O.K. Judin. – K.: Vidavnicтво TOV NVP «INTERSERVIS», 2009. – 714s.  
 7. Bekirov A. A steganographic method based on the modification of regions of the image with different saturation / Barannik V., Bekirov A., Lekakh A., Barannik D // 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018  
 8. Bekirov A. Detections of sustainable areas for steganographic embedding / Vladimir Barannik; Andriy Alimpiev; Ali Bekirov; Dmitry Barannik // 2017 IEEE East-West Design & Test Symposium.  
 9. Jassim F.A. Five modulus method for Image compression / Firas A. Jasim // Signal and Image Processing: An international Journal (SIPIJ), vol. 3, no 5, pp. 26-34. 2012.

**ТЕХНОЛОГИЯ СЕЛЕКЦИИ ОБЛАСТЕЙ АЭРОФОТОСНИМКА С РАЗЛИЧНОЙ НАСЫЩЕННОСТЬЮ ДЛЯ СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ**

*Али Энверович Бекиров (кандидат технических наук)<sup>1</sup>  
Владимир Жоржевич Яценюк (кандидат технических наук, доцент)<sup>1</sup>  
Александр Станиславович Крейдун<sup>2</sup>*

<sup>1</sup>*Харьковский национальный университет Воздушных Сил им. Ивана Кожедуба, Харьков, Украина*  
<sup>2</sup>*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

Современные системы сбора и обработки информации широко представлены оптическими системами мониторинга, которые используются для ведения воздушной разведки, мониторинга объектов критической инфраструктуры и транспортных коммуникаций. Проблемными ограничениями при разработке новых и совершенствовании существующих систем является повышение требований конечного пользователя относительно качества цифровых изображений в условиях ограниченной пропускной способности каналов передачи данных. Для уменьшения объемов аэрофотоснимков предлагается использовать стеганографические преобразования с селекцией областей с различной семантической насыщенности.

В статье проводится анализ возможности селекции объектов интереса с помощью методов машинного распознавания контурной информации на основе скользящей маски. Для устранения системных ограничений указанного подхода, которые заключается в отсутствии возможности выявления элементов описания объекта интереса, предлагается использовать операцию свертки на основе набора фильтров. Разрабатывается технология селекции незначимых областей, которые используются как контейнеры для встраивания информации и областей с объектами интереса, как полезного стеганографического сообщения. Первый этап предусматривает выбор не значимых областей на основе коэффициента разницы элементов. На втором этапе происходит фильтрация изображения на основе операции свертки с набором фильтров, которые соответствуют ожидаемому отклику изображения после фильтрации.

**Ключевые слова:** стеганографическое преобразование, операция свертки, системы мониторинга, выявление объектов.

**TECHNOLOGY OF SELECTION OF AERIAL PHOTO AREA WITH VARIOUS SATURATION FOR A STEANOGRAPHIC TRANSFORMATION**

*Ali Bekirov (Doctor of philosophy)<sup>1</sup>  
Vladimir Yachenok (Doctor of philosophy, Associate Professor)<sup>1</sup>  
Aleksandr Krejdun<sup>2</sup>*

<sup>1</sup>*Kharkiv National University of Air Force named after Ivan Kozhedub, Kharkiv, Ukraine*  
<sup>2</sup>*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

Modern systems for collecting and processing information are widely represented by optical monitoring systems that are used for aerial reconnaissance, monitoring of critical infrastructure and transport communications. The problematic limitations in developing new and improving existing systems are increasing the end-user requirements regarding the quality of digital images in the conditions of limited bandwidth of data transmission channels. To reduce the volume of aerial photographs, it is proposed to use steganographic transformations with the selection of areas with different semantic saturations.

The article analyzes the possibility of selecting objects of interest using methods of machine recognition of contour information based on a moving mask. To eliminate the systemic limitations of this approach, which is the inability to identify elements of description of the interest's object, it is proposed to use the convolution operation based on a set of filters. A technology is being developed for selecting insignificant areas that are used as containers for embedding information and areas with objects of interest, as a useful steganographic message. The first stage involves the selection of non-significant areas based on the coefficient of difference between the elements. At the second stage, the image is filtered based on the convolution operation with a set of filters that correspond to the expected image response after filtering.

**Key words:** steganographic transformation, convolution operation, monitoring systems, object identification.

**References**

1. Al-Shatnawi A.M. A new method in image steganography with improved image quality / Atallah M. Al-Shatnawi // Applied Mathematical Science, Vol. 6, 2012, no. 79, p. 3907-3915. 2. Bekirov A.E. Metod zahistu informacii na osnovi steganografichnih sistem // Ozbroennija ta vijskova tehnika. – 2015. №1 S. 29 – 36. 3. Bekirov A.E. Puti povysheniya informacionnoj bezopasnosti resursov v sistemah special'nogo naznachenija / Barannik V.V., Rjabuha Ju.N., Bekirov A.E., Komolov D.I. // Четверта міжнародна науково-практична конференція [«Інформаційні технології та комп'ютерна інженерія»], (Vinnicja, 28 - 30 travnja 2014 r.) / Vinnic'kij nacional'nij tehničnij universitet, Vinnicja, 2014. – S. 151. 4. Avinash K. Gulve A high capacity secured image steganography method with five pixel pair differencing and LSB substitution / Avinash K. Gulve, Madhuri S. Joshi // I.J. Image. Graphics and Signal Procecing, 2015, 5, p 66-74. 5. Basics of the case-method. Available at: <http://www.pprog.ru/Osnovi>

%20keis - metoda.doc. 6. Pohrebelnaia N. Y. (2008). Keis-metod kak uslovye formyrovanyia yssledovatel'skykh sposobnostei studentov vuza [Case-method as a condition for the formation of research abilities of university students]. Nauka y shkola, 737. 7. Bekirov A. A steganographic method based on the modification of regions of the image with different saturation / Barannik V., Bekirov A., Lekakh A., Barannik D // 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018. 8. Bekirov A. Detections of sustainable areas for steganographic embedding / Vladimir Barannik; Andriy Alimpiev; Ali Bekirov; Dmitriy Barannik // 2017 IEEE East-West Design & Test Symposium. 9. Jassim F.A. Five modulus method for Image compression / Firas A. Jasim // Signal and Image Processing: An international Journal (SIPIJ), vol. 3, no 5, pp. 26-34. 2012.

*Юрій Аркадійович Гусак (доктор військових наук, с.н.с.)*

*Ігор Іванович Шовкошитний (кандидат військових наук, с.н.с.)*

*Іван Михайлович Старинський*

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

## МОДЕЛЮВАННЯ ДІЙ РАДІОЛОКАЦІЙНОЇ РОЗВІДКИ В КОМПЛЕКСНІЙ СИСТЕМІ ВІЯВЛЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

У статті розглядається радіолокаційний канал системи комплексної протидії безпілотним літальним апаратам (БпЛА) [4]. Як відомо, система комплексної протидії включає в себе засоби виявлення, а саме: засоби радіотехнічної та радіолокаційної розвідки, оптико-електронні, акустичні, тепловізійні засоби виявлення безпілотних літальних апаратів та пункти візуального спостереження, а також засоби ураження - станції радіоелектронної боротьби, бойові лазерні системи та системи надпотужного надвисокочастотного випромінювання, вогневі засоби ураження. Зазначені засоби створюють систему комплексної протидії безпілотним літальним апаратам. На прикладі радіолокаційного засобу виявлення (радіолокаційної станції) показано, яким чином можна формалізувати канали комплексного виявлення безпілотних літальних апаратів. Математична модель радіолокаційного виявлення побудована на основі марковської моделі «загибелі та розмноження».

Процес виявлення та ідентифікації БпЛА представлено графом станів каналу радіолокаційного виявлення, на основі якого записано систему диференціальних рівнянь для ймовірності перебування каналу радіолокаційного виявлення у відповідних станах. Знайдені рішення системи диференціальних рівнянь у сталому режимі. Введені нові показники, а саме: приведена інтенсивність виявлення БпЛА та приведена інтенсивність правильного виявлення БпЛА (ідентифікації повітряної цілі як БпЛА). Показано, що приведена інтенсивність виявлення БпЛА залежить від ймовірності виявлення їх конкретним радіолокаційним засобом (радіолокаційною станцією), а приведена інтенсивність правильного виявлення БпЛА – від характеристик радіолокаційного засобу виявлення. Математична модель є універсальною та дає можливість отримати ймовірності виявлення БпЛА для будь-якого каналу виявлення.

У статті проведено аналіз залежності ймовірностей перебування каналу радіолокаційного виявлення від ефективної поверхні розсіювання (ЕПР) БпЛА та від дальності його виявлення. Наведені відповідні графіки та зроблено висновок про те, що математична модель адекватно описує процес виявлення БпЛА радіолокаційним каналом.

**Ключові слова:** комплексна протидія БпЛА, модель масового обслуговування, радіолокаційні засоби.

### Вступ

В умовах особливого періоду в країні, коли продовжуються бойові дії на сході України, виник конфлікт в Азовському морі, особлива увага має приділятися підвищенню якості підготовки військових фахівців різних рівнів. Це пояснюється тим, що складне озброєння і військову техніку (ОВТ) мають експлуатувати грамотні спеціалісти, які володіють достатніми теоретичними знаннями і практичними навичками, можуть приймати правильні рішення у проблемних ситуаціях.

**Постановка проблеми.** Аналіз досвіду сучасних війн і збройних конфліктів свідчить про стрімке зростання ролі БпЛА, сфери застосування яких, починаючи з другої половини ХХ сторіччя, значно розширились. Новітні безпілотні авіаційні комплекси стали невід'ємним елементом розвідувальних і розвідувально-ударних систем у

війнах нинішнього покоління, однією з характерних рис якого вважається ведення безконтактних бойових дій з отриманням у реальному часі розвідувальної інформації та миттєвим завданням ударів по об'єктах. Постійне збільшення кількості та типів засобів безпілотної авіації зумовило необхідність проведення досліджень стосовно виявлення та боротьби з ними.

Основним засобом виявлення в сучасних системах протиповітряної оборони є радіолокаційні станції. Вони здатні засікати літаки і вертольоти на відстані до декількох десятків кілометрів, залежно від характеристик цілі і особливостей місцевості. У ряді випадків БпЛА, особливо легкого класу, не завжди є ціллію для існуючих РЛС, оскільки ці апарати мають малу

ЕПР, через що їх виявлення стає досить непростим завданням.

Комплексні дослідження щодо виявлення безпілотних авіаційних комплексів та протидії їм показали, що виявлення тактичних БПЛА є складним завданням для більшості існуючих РЛС [1]–[2]. Одним із напрямів вирішення цієї проблеми є розроблення сучасних радіолокаційних засобів на основі моделювання їх дій у комплексній системі виявлення БПЛА. Для цього необхідно розробити адекватну математичну модель, яка б давала можливість врахувати як характеристики БПЛА, так і характеристики радіолокаційних засобів їх виявлення.

**Аналіз останніх досліджень і публікацій.** Аналіз більшості праць [5]–[7], присвячених проблемним питанням виявлення БПЛА, свідчить про те, що нині розроблені та застосовуються підходи, які описують окремі способи виявлення БПЛА як об'єкта повітряного нападу. Однак немає наукових праць щодо процесу моделювання дій радіолокаційних засобів виявлення БПЛА в комплексній системі протидії їм.

За масштабом виконуваних завдань найбільш поширеними є БПЛА тактичного та оперативно-тактичного призначення [2]; [3]. Саме ці типи БПЛА є найбільш проблемними щодо їх своєчасного виявлення та знищення. За останні роки здійснюються активні пошуки ефективних способів та засобів боротьби із зазначеними типами літальних апаратів. Нині поки що таких засобів у військах немає, а виявлення БПЛА здійснюється тими радіолокаційними засобами, які є в розпорядженні командування.

Особливостями БПЛА, як об'єктів для засобів радіолокаційної розвідки, є:

можливість польоту до об'єктів удару (розвідки) на гранично малих висотах, що ускладнює їх своєчасне виявлення, а також впливає на безперервність їх супроводження підрозділами РТВ та ЗРВ;

мала радіолокаційна помітність, яка зумовлена малою ЕПР, що також ускладнює своєчасне виявлення радіолокаційними засобами РТВ та ЗРВ;

виявлення БПЛА відбувається в зоні засвічувань від місцевих предметів, що потребує включення апаратури захисту від пасивних завад.

### Виклад основного матеріалу дослідження

У роботі [4] запропоновано математичну модель комплексної протидії БПЛА, у якій розглядаються два етапи комплексної протидії – виявлення та ураження. Так, на етапі виявлення застосовувалися засоби радіотехнічної та радіолокаційної розвідки, оптико-електронні, акустичні, тепловізійні засоби виявлення БПЛА та візуального спостереження тощо, а на етапі ураження – станції радіоелектронної боротьби, лазерні системи та системи надпотужного НВЧ-випромінювання, вогневі засоби тощо.

У зазначеній математичній моделі досліджувалися характеристики процесу

виявлення БПЛА. Для цього було побудовано граф процесу комплексного виявлення БПЛА (рис. 1).

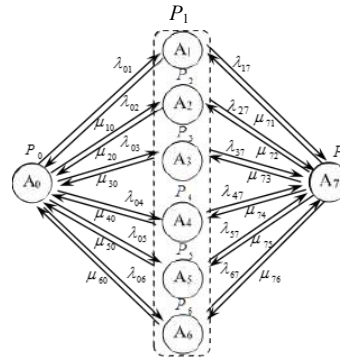


Рис. 1 Граф станів системи комплексного виявлення БПЛА

- де станам графа відповідають наступні події:  
 A<sub>0</sub> – всі канали виявлення вільні, БПЛА немає;  
 A<sub>1</sub> – БПЛА виявлено 1-м каналом;  
 A<sub>2</sub> – БПЛА виявлено 2-м каналом;  
 ...  
 A<sub>6</sub> – БПЛА виявлено 6-м каналом;  
 A<sub>7</sub> – БПЛА ідентифіковано.

При цьому,  $\lambda_0$  – інтенсивність появи БПЛА в зоні виявлення, а  $\mu_1, \mu_2, \dots, \mu_6$  є інтенсивностями обслуговування відповідного каналу виявлення БПЛА.

Розглянемо систему радіолокаційної розвідки, як окрему складову системи комплексного виявлення БПЛА.

Проаналізуємо модель радіолокаційного виявлення БПЛА. Для цього побудуємо граф станів системи радіолокаційного виявлення БПЛА (рис. 2), де стан S<sub>1</sub> відповідає ситуації, коли БПЛА немає в межах зони виявлення засобу радіолокаційного виявлення повітряних цілей; стан S<sub>2</sub> – ситуації, коли БПЛА перебуває у зоні виявлення і радіолокаційний засіб веде розвідку; стан S<sub>3</sub> – ситуації, коли повітряну ціль ідентифіковано як БПЛА (рис. 2).

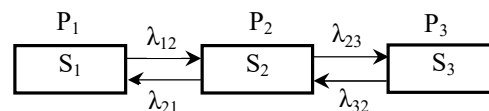


Рис. 2 Граф станів системи радіолокаційного виявлення БПЛА

Ймовірність перебування системи радіолокаційного виявлення у станах S<sub>k</sub>, де k = 1, n, позначимо як P<sub>k</sub>(t).

Відповідно до графа станів (рис. 2) система диференціальних рівнянь для імовірностей перебування системи у відповідних станах має вигляд:

$$\begin{cases} \frac{dP_1}{dt} = -\lambda_{12}P_1 + \lambda_{21}P_2 \\ \frac{dP_2}{dt} = -\lambda_{21}P_2 - \lambda_{23}P_2 + \lambda_{12}P_1 + \lambda_{32}P_3 \\ \frac{dP_3}{dt} = \lambda_{23}P_2 - \lambda_{32}P_3 \end{cases}, \quad (1)$$

де  $P_1, \dots, P_3$  – ймовірності перебування системи у станах  $S_1, \dots, S_3$  відповідно;

$\lambda_{12}$  – інтенсивності переходу системи зі стану  $S_1$  у стан  $S_2$ ;

$\lambda_{23}$  – інтенсивності переходу системи зі стану  $S_2$  у стан  $S_3$ ;

$\lambda_{21}$  – інтенсивності переходу системи зі стану  $S_2$  у стан  $S_1$ ;

$\lambda_{32}$  – інтенсивності переходу системи зі стану  $S_3$  у стан  $S_2$ .

З точки зору виявлення БПЛА, інтенсивність переходу системи зі стану  $S_1$  у стан  $S_2$  – це інтенсивність виявлення повітряної цілі РЛ-засобом, яка описується виразом:

$$\lambda_{12} = \frac{1}{t_{12}} P_{12}, \quad (2)$$

де  $P_{12}$  – ймовірність виявлення повітряної цілі РЛ-засобом;

$t_{12}$  – середній час виявлення повітряної цілі РЛ-засобом.

Інтенсивність переходу системи зі стану  $S_2$  у стан  $S_3$  – це інтенсивність правильного виявлення повітряної цілі як БПЛА, яка описується виразом:

$$\lambda_{23} = \frac{1}{t_{23}} P_{23}, \quad (3)$$

де  $P_{23}$  – ймовірність правильного виявлення повітряної цілі РЛ-засобом як БПЛА;

$t_{23}$  – середній час правильного виявлення повітряної цілі в каналі РЛ-виявлення.

Інтенсивність переходу системи зі стану  $S_3$  у стан  $S_2$  – це інтенсивність правильного не виявлення повітряної цілі, яка описується виразом:

$$\lambda_{32} = \frac{1}{t_{32}} P_{32}, \quad (4)$$

де  $P_{32} = 1 - P_{23}$  – ймовірність правильного не виявлення оператором повітряної цілі як такої, що не належить до БПЛА;

$t_{32}$  – середній час правильного не виявлення повітряної цілі як такої, що не належить до БПЛА.

Інтенсивність переходу системи зі стану  $S_2$  у стан  $S_1$  – це інтенсивність того, що повітряна ціль не буде виявлена РЛ-каналом, яка описується виразом:

$$\lambda_{21} = \frac{1}{t_{21}} P_{21}, \quad (5)$$

де  $P_{21} = 1 - P_{12}$  – ймовірність не виявлення повітряної цілі РЛ-засобом;

$t_{21}$  – середній час перебування повітряної цілі у зоні виявлення РЛ-засобу.

Відповідно до [8] ймовірність виявлення повітряної цілі  $P_{12}(D)$  залежно від дальності ( $D$ ) описується наступним виразом:

$$P_{12}(D) = e^{-\left(\frac{D}{D_0}\right)^4}, \quad (6)$$

де  $D_0 = f(\sigma_u)$  – функція, яка описує залежність дальності виявлення повітряної цілі РЛ-засобом від ЕПР повітряної цілі ( $\sigma_u$ ).

Введемо:

показник приведеної інтенсивності виявлення повітряної цілі РЛ-засобом:

$$\alpha_1 = \frac{\lambda_{12}}{\lambda_{21}} = \frac{P_{12}}{P_{21}} = \frac{P_{12}}{1 - P_{12}}, \quad (7)$$

показник приведеної інтенсивності правильного виявлення повітряної цілі РЛ-засобом:

$$\alpha_2 = \frac{\lambda_{23}}{\lambda_{32}} = \frac{P_{23}}{P_{32}} = \frac{P_{23}}{1 - P_{23}}, \quad (8)$$

Відповідно до [9] рішенням системи диференціальних рівнянь (1) з урахуванням виразів (7) та (8) є:

$$\begin{cases} P_1 = \frac{1}{1 + \alpha_1(1 + \alpha_2)} \\ P_2 = \alpha_1 P_1 \\ P_3 = \alpha_1 \alpha_2 P_1 \end{cases} \quad (9)$$

$P_1$  – ймовірність того, що повітряної цілі немає в зоні виявлення радіолокаційного засобу;

$P_2$  – ймовірність того, що повітряна ціль виявлена радіолокаційним засобом;

$P_3$  – ймовірність того, що повітряна ціль правильно виявлена (ідентифікована) як БПЛА.

Відповідно до [10] можемо записати вираз ймовірності правильного виявлення повітряної цілі:

$$P_{ПВ} = \frac{1}{2} \left[ 1 + \Phi \left( v \sqrt{\frac{N_i}{2} - \frac{\ln \lambda_{пор}}{v \sqrt{2N_i}}} \right) \right], \quad (10)$$

де  $\Phi$  – інтеграл ймовірності;

$v = P_c / P_{ш}$  – відношення потужності сигналу до потужності шуму на виході лінійної частоти приймача;

$\lambda_{пор}$  – порогове значення відношення правдоподібності;

$N_i = F_i \varphi_{0,5} / 6n_A$  – число обробляючих імпульсів цілі, де  $\varphi_{0,5}$  – ширина діаграми направленості на рівні половини потужності та  $n_A$  – швидкість обертання антени (об/хв).

Основна формула для визначення максимальної дальності виявлення повітряної цілі РЛ-засобом виглядає наступним чином [10]:

$$D_{max} = D_0 = \sqrt[4]{\frac{P_{пер} G_{max} S_A \sigma_{ц}}{16\pi^2 P'_{пр.мін} v_p}} = \sqrt[4]{\gamma \sigma_{ц}}, \quad (11)$$

де  $\gamma = \frac{P_{пер} G_{max} S_A}{16\pi^2 P'_{пр.мін} v_p}$  – коефіцієнт, який має одне

значення для конкретного РЛ-засобу;

$P_{пер}$  – потужність, випромінювана передавачем;

$P'_{пр.мін}$  – гранична чутливість приймача;

$G_{max}$  – максимальний коефіцієнт направленої дії антени;

$S_A$  – ефективна площа антени;

$\sigma_{ц}$  – ефективна відбиваюча площа цілі;

$\nu_p$  – коефіцієнт розрізнення.

Відповідно до виразу (10) знайдемо ймовірність правильного виявлення повітряної цілі для РЛС X1-M “Око” (табл. 1) [1]:

$$P_{пв} = \frac{1}{2} \left[ 1 + \Phi \left( 1,5 \sqrt{\frac{2,5}{2} - \frac{\ln 1,5}{1,5\sqrt{50}}} \right) \right]$$

Таблиця 1  
Можливості РЛС X1-M “Око” з виявлення маловисотних малорозмірних цілей

Тип	Дальність виявлення повітряних цілей з ЕПР 1 м <sup>2</sup> (0,3 м <sup>2</sup> ; 0,1 м <sup>2</sup> ) на малих висотах, км				
	Нц=100 м	Нц=300 м	Нц=500 м	Нц=1000 м	Нц=4000 м
X1-M “Око”	- (-; 4,2)	- (-; 5)	- (-; 5,5)	- (-; 6)	даних немає

Підставивши значення  $P_{пв}$  у вираз (8), визначимо показник приведеної інтенсивності правильного виявлення повітряної цілі РЛ-засобом:

$$\alpha_2 = \frac{P_{23}}{1 - P_{23}} = \frac{0,75}{1 - 0,75} = 3.$$

Якщо підставити у вираз (6) значення максимальної дальності дії РЛС (табл. 2), то можна побудувати графіки залежності ймовірності виявлення БпЛА від дальності та ЕПР БпЛА (рис. 3).

Таблиця 2

Характеристики розсіювання (ЕПР) деяких типів БпЛА, отримані за результатами моделювання, а також значення  $D_{max}$  для РЛС X1-M “Око” [1]

№ з/п	Тип БпЛА	Кругова медіана ЕПР, м <sup>2</sup>		$D_{max}$ , м	Приблизні аналоги
		см	дм		
1.	Орлан-10	0,03	0,05	5477	“Гранат-4”, “Карнивора”, “Skylark-3”, “Hero-400”
2.	Форпост	0,1-0,11	0,11	7401	“RQ-7 Shadow”, “Корсар”, “RQ-2 Pioneer”, “Hermes-90”, “Aerostar”, “Sperwer B”, “CH-3”
3.	Оріон	0,97-0,05	0,67	13161	“Hermes 900”, MQ-1 “Reaper” MQ-1C “GreyEagle”, “Дозор-600”, “CH-4”

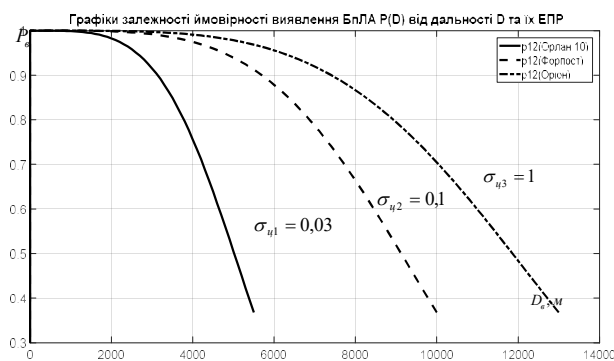


Рис. 3. Графіки залежності ймовірності виявлення БпЛА P(D) від дальності D та їх ЕПР ( $\sigma_{ц}$ )

Результати моделювання дій радіолокаційного каналу виявлення на базі РЛС X1-M “Око” в системі комплексного виявлення безпілотних літальних апаратів відображені на рис. 4–6.

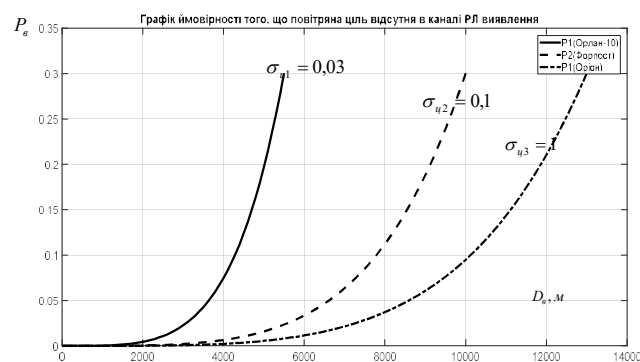


Рис.4. Графік ймовірності того, що повітряної цілі немає в каналі РЛ-виявлення

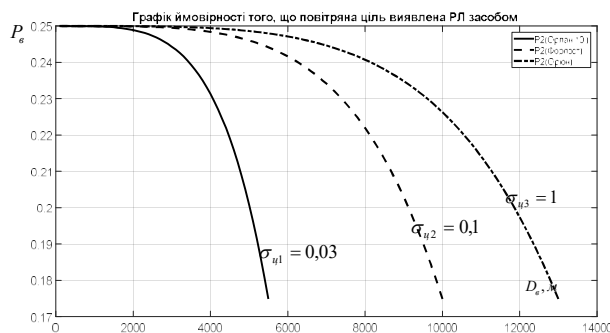


Рис. 5. Графік ймовірності того, що повітряна ціль виявлена РЛ-засобом

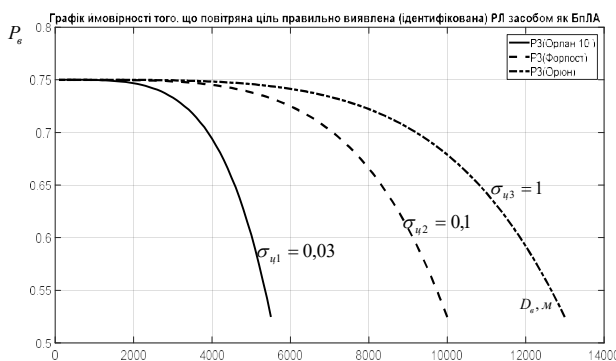


Рис. 6. Графік ймовірності того, що повітряна ціль правильно виявлена (ідентифікована) РЛ-засобом як БпЛА



Аналіз графіків на рис. 3–6 показує, що запропонована математична модель виявлення БпЛА засобами РЛ-розвідки адекватно та очікувано реагує на зміну вхідних параметрів значень ЕПР цілі.

### Висновки і перспективи подальших досліджень

Таким чином, розроблена математична модель радіолокаційного виявлення БпЛА адекватно описує процес функціонування засобів

радіолокаційної розвідки та дає можливість оцінювати ймовірності перебування радіолокаційного каналу комплексної системи протидії БпЛА в тому чи іншому стані залежно від ЕПР цілі, а також технічних характеристик радіолокаційного засобу виявлення БпЛА.

Перспективами подальших досліджень є використання даної моделі виявлення разом з іншими складовими системи виявлення БпЛА, які зазначалися вище.

### Література

1. Аналіз можливостей наявної системи протидії безпілотним літальним апаратам противника: звіт про НДР шифр “Градiснт” (промiж.) / ЦНДІ ЗС України. 2019. 248 с. Інв. № 17992. 2. Звіт про результати досліджень на навчаннях на тему: “Визначення можливостей наявних та перспективних засобів виявлення та протидії (ураження) безпілотних авіаційних комплексів та застосування ударних безпілотних літальних апаратів”. Київ: ВНУ ГШ ЗС України, 2017. 127 с. 3. Шуенкин В. А., Донченко В. С. Прикладные модели теории массового обслуживания. В помощь студентам специальности “Прикладная математика”: учебн. пособ. Київ: НМК ВО, 1992. 398 с. 4. Гусак Ю. А., Старинский И. М. Математична модель комплексної протидії безпілотним літальним апаратам // Зб. наук. пр. ЦНДІ ЗС України. Київ. 2019. № 3 (89). С. 243–251. 5. Теорія і практика боротьби з малорозмірними низьколітними цілями (оцінка можливостей, тенденцій розвитку засобів протиповітряної оборони): моногр. / І. С. Романченко,

О. М. Загорка, С. Г. Бутенко, О. В. Дейнега. Житомир: Полісся, 2011. 344 с. 6. Про затвердження Концепції створення системи комплексної протидії безпілотним авіаційним комплексам противника від 10.04.2017 № 884/с/дск: Наказ начальника Генерального штабу Збройних Сил України. Київ. 2017. 14 с. 7. Даник Ю. Г. Аналіз ефективності виявлення тактичних безпілотних літальних апаратів пасивними та активними засобами спостереження // Збірник наукових праць ЖВІ ДУТ, 2015. Вип. 10. С. 5–20. 8. Справочник офицера противоздушной обороны / под ред. Г. Зиминой. – Москва: Воениздат, 1981. 431 с. 9. Вентцель Е. С. Исследование операции: задачи, принципы, методология. – 2-е изд., стер. – Москва: Наука. Гл. ред. физ.-мат. лит., 1988. 208 с. (Пробл. науки и техн. прогресса). 10. Справочник по основам радиолокационной техники / под ред. В. В. Дружинина. – Москва: Воениздат, 1967. 768 с.

## МОДЕЛИРОВАНИЕ ДЕЙСТВИЙ РАДИОЛОКАЦИОННОЙ РАЗВЕДКИ В КОМПЛЕКСНОЙ СИСТЕМЕ ОБНАРУЖЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Юрий Аркадьевич Гусак (доктор военных наук, с.н.с.)  
Игорь Иванович Шовкошитный (кандидат военных наук, с.н.с.)  
Иван Михайлович Старинский

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

В статье рассматривается радиолокационный канал системы комплексного противодействия беспилотным летательным аппаратам [4]. Как известно, система комплексного противодействия включает в себя средства обнаружения, а именно: средства радиотехнической и радиолокационной разведки, оптико-электронные, акустические, тепловизионные средства обнаружения беспилотных летательных аппаратов и пункты визуального наблюдения, а также средства поражения - станции радиоэлектронной борьбы, боевые лазерные системы и системы сверхмощного СВЧ-излучения, огневые средства поражения. Указанные средства создают систему комплексного противодействия беспилотным летательным аппаратам. На примере радиолокационного средства обнаружения (радиолокационной станции) показано, каким образом можно формализовать каналы комплексного обнаружения беспилотных летательных аппаратов. Математическая модель радиолокационного обнаружения построена на основе марковской модели “гибели и размножения”.

Процесс выявления и идентификации БпЛА представлен графом состояний канала радиолокационного обнаружения, на основе которого записано систему дифференциальных уравнений для вероятности пребывания канала радиолокационного обнаружения в соответствующих состояниях. Найдены решения системы дифференциальных уравнений в установившемся режиме. Введены новые показатели, а именно: приведенная интенсивность обнаружения БпЛА и приведенная интенсивность правильного обнаружения БпЛА (идентификации воздушной цели как БпЛА). Показано, что приведенная интенсивность обнаружения БпЛА зависит от вероятности обнаружения их конкретным радиолокационным средством (радиолокационной станцией), а приведенная интенсивность правильного обнаружения БпЛА – от характеристик радиолокационного средства обнаружения. Математическая

модель является универсальной и дает возможность получить вероятности обнаружения БпЛА для любого канала обнаружения.

В статье проведен анализ зависимости вероятности пребывания канала радиолокационного обнаружения от эффективной поверхности рассеивания (ЭПР) БпЛА и от дальности его обнаружения. Приведены соответствующие графики и сделан вывод о том, что математическая модель адекватно описывает процесс обнаружения БпЛА радиолокационным каналом.

**Ключевые слова:** комплексное противодействие беспилотным летательным аппаратам, модель массового обслуживания, радиолокационные средства.

## THE ACTION SIMULATION OF RADAR INTELLIGENCE IN A COMPLEX SYSTEM THE DISCOVERY OF UNMANNED AERIAL VEHICLES

*Yurii Husak (Doctor of Military Sciences, Senior Researcher)*

*Ihor Shovkoshynyi (Candidate of Technical Sciences, Senior Researcher)*

*Ivan Starynskyi*

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

The article discusses radar channel system integrated counter unmanned aerial vehicles [4]. As it is known, the system of complex counter includes a detection means, namely the means of radio and radar reconnaissance, electro-optical, acoustic, thermal means of detecting unmanned aerial vehicles, and paragraphs visual observation and weapons stations warfare, military laser system and heavy duty microwave radiation, firepower destruction. These means create an integrated counter unmanned aerial vehicles. For example, radar detection (radar) shows how to formalize the complex detection of unmanned aerial vehicles. A mathematical model of the radar detection is constructed based on Markov model "death and reproduction".

The process of detection and identification the UAV is represented by the state graph of the channel radar detection, based on which the written system of differential equations for the probability of stay of the channel radar detection in the respective states. Found solution of the system of differential equations in the steady state. Introduced new indicators, namely: the intensity of the detecting UAV and the intensity of the correct detection of the UAV (identify aerial targets like UAVs). It is shown that the intensity of detection of the UAV depends on the probability of discovery their particular means radar (radar station), and given the intensity of the correct detection of the UAV from the characteristics of the radar detection means. A mathematical model is universal and allows to obtain the probability of detection of the UAV for any channel detection.

In the article the analysis of the dependence of the probability of staging of the channel radar detection from the effective surface scattering (ESS) of the UAV and the range of detection. His given the corresponding graphs and it is concluded that the mathematical model adequately describes the discovery process of the UAV radar channel.

**Key words:** integrated UAV counteraction, queuing model, radar means.

### References

1. Analysis of the capacity of the existing system to counter unmanned aerial vehicles of the enemy: a report on research code "Gradient" (interm.) / CSRI of the Armed Forces of Ukraine. 2019. 248 p. inv. 17992.
2. A report about research on the training of on the teachings on the theme: "identifying opportunities for existing and prospective means of detection and reaction (destruction) of unmanned aircraft systems and applications of attack unmanned aerial vehicles". Kyiv: Scientific Department of the General staff of armed forces of Ukraine, 2017. 127 p.
3. **Shuyenkin V. A.**, Donchenko V. S. Application of the model of the Queuing theory. To help for students specialty "Applied mathematics": teaching manual. Kyiv: NMK VO 1992. 398 p.
4. **Gusak, Y. A.**, Starynskyi, I. M. Mathematical model of an integrated counteraction unmanned aerial vehicles // Coll. of scienc. worksof CSRI of the Armed Forces of Ukraine, Kyiv, No. 3 (89) pp. 243-251.
5. Theory and practice of struggle against against small-size low altitude targets (the assessment of opportunities, trends in the development of air defense): monograph. / I. S. Romanchenko, A. M. Zagorka, S. G. Butenko, A. V. Deynega. Zhitomir: Polesie. 2011. 344 p.
6. On approval of the Concept of an integrated system to counter unmanned aviation systems of the enemy from 10.04.2017 No. 884/S/DSK: the order of the chief of the General staff of the Armed Forces of Ukraine: Kyiv, 2017. 14 p.
7. **Danik Yu. G.** Analysis of the efficiency of tactical unmanned aerial vehicles detection by passive and active observation observation means / Collection of scientific works ZhVI DUT, 2015. Vol. 10. P. 5-20.
8. Air defence officer's reference book, ed. by G. Zimin. – Moscow: Voenizdat, Military Publishing, 1981. 431 p.
9. **Ventzel E. S.** Investigation of operations: problems, principles, methodology. 2nd ed. Moscow: Nauka. Main. Ed. Of Phys. – math. lit 1988. – 208 p. (Problems of science and Techn. progress).
10. A reference book to the fundamentals of radar technology / edited by V. V. Druzhinin. – Moscow: Voenizdat, 1967. 768 p.

*Владислав Віталійович Сотник (кандидат технічних наук, старший науковий співробітник)*

*Олександр Олексійович Расстригін (доктор технічних наук, професор)*

*Артем Валерійович Купчин*

*Центральний науково-дослідний інститут озброєння та військової техніки ЗС України, Київ, Україна*

## МЕТОДИКА ВІДБОРУ КРИТИЧНИХ ТЕХНОЛОГІЙ

Прогнозні дослідження, в іноземній практиці більш відомі як форсайт, являють собою передумову для стабільного розвитку країни. В даній роботі проведений аналіз найбільш поширених методів технологічного форсайту, які використовуються як в Україні, так і закордоном. Встановлені як позитивні, так і негативні сторони кожного. В результаті дослідження авторами запропоновано рейтинг найпоширеніших методів науково-технологічного форсайту, показано недоцільність використання деяких методів для технологічного прогнозування в оборонній сфері України.

Для визначення переліку перспективних критичних технологій авторами запропонована комбінована методика, яка поєднує в собі експертні та статистичні методи.

В роботі описаний повний алгоритм проведення прогнозного дослідження щодо визначення переліку критичних технологій в оборонній сфері України. Запропонований форсайт-проект включає два етапи експертного опитування, а також бібліометричний та патентний аналіз. Крім того, продемонстровано повну структуру прийняття рішення стосовно відбору технологій до переліку критичних. Наведені основні принципи формування експертної комісії, визначено оптимальну кількість експертів у групах та ітерацій під час опитування. Також запропоновані узагальнені критерії відбору технологій до переліку критичних, на основі групового поєднання часткових критеріїв.

Запропоновано принцип граничного відсікання певних технологій на основі апроксимації функції, диференціювання та визначення точки однакових приростів абсцис та ординат. При цьому апроксимованою функцією є найбільш достовірна наближена функція до графіку, який описує залежність узагальненої оцінки критичності від номеру технології в порядку зростання. В практичному розумінні граничний рівень відбору технологій є межею, до якої зростання рівня критичності технологій набагато менше, ніж відповідне зростання після неї.

Результатом прогнозного дослідження за допомогою запропонованої методики є отримання переліку перспективних критичних технологій в оборонній сфері України.

**Ключові слова:** форсайт; прогнозні дослідження; критичні технології; ключові технології; метод аналізу ієрархії; Делфі.

### Вступ

“Об’єктивний аналіз – ефективні рішення”, – лозунг корпорації RAND, яка є безумовним світовим лідером прогнозних досліджень.

Наукові досягнення неодмінно приносять дивіденди, а практика останніх десятиліть показує, що успішні світові лідери все більше вкладають у науку, як каталізатор розвитку економіки країни. Південна Корея у 2017 р. витратила 4,29% свого ВВП на наукові дослідження, за нею йде Ізраїль (4,11%) і Японія (3,58%) [1]. В ЄС ситуація наступна: Швеція – 3,4%, Австрія – 3,16%, Данія – 3,05%, Німеччина – 3,02% [2]. На жаль Україна не підтримує світову тенденцію, питома вага витрат на наукові дослідження у 2018 році становила 0,47% від ВВП.

Здійснення наукових досліджень за всіма напрямками вимагає значних затрат, тому уряди країн сконцентровують максимум зусиль на розвиток найбільш важливих, ключових наукових напрямках та технологіях – критичних технологіях (далі – КТ) [3]. Для уніфікації розуміння терміну

авторами запропоновано власну дефініцію.

КТ – це стратегічно важлива для держави сукупність знань та виробничих операцій, готових виробів і матеріалів, які не можуть бути гарантовано імпортованими і без застосування яких виготовлення, ремонт і обслуговування існуючих, а також створення новітніх зразків озброєння не можливе. В даній статті буде розглянуто формування переліку лише перспективних КТ. Формування переліку існуючих КТ відбувається за допомогою інших методів та підходів, що не є метою даної роботи.

Основними інструментами для виявлення КТ є методи прогнозних досліджень, в іноземній практиці більш відомі як форсайт (від англ. Foresight – передбачення, погляд у майбутнє). По суті всі методи прогнозування складають основу методології форсайту.

Першими країнами, які використовували форсайт, як інструмент розроблення політики розвитку, були Японія та Америка. На початку

1970-х років у Японії застосували метод Делфі для прогнозування в науці та технологіях. Після цього естафету поступово підхопили і решта країн [4]. За кількістю публікацій прослідковується тренд на значне підвищення популярності цієї тематики з початку 1990-х років, а потім ще більший виток з 2000-х [5].

**Постановка проблеми.** У 2017 році Україна приєдналася до світової практики визначення своїх технологічних пріоритетів, шляхом формування та систематичного уточнення переліку критичних технологій. Однак чітко визначеної методики відбору технологій не існує, як не існує і загальноприйнятого поняття критичної технології.

**Аналіз остатніх досліджень і публікацій.** В багатьох наукових роботах, як українських, так і закордонних вчених, описані основні методи оцінки технологій для включення їх до переліку критичних.

Так, в роботі [4] зазначено, що основними методами є: огляд літератури, Делфі, експертні панелі, бібліометричний та патентний аналіз, інтерв'ю, конференція, мозковий штурм, дорожні карти, сценарії, SWOT-аналіз. У [6-8] зазначено, що основою прогнозування є використання комплексу методів експертних оцінок, зокрема – Делфі [6-7].

У роботах російських вчених провідне місце у прогнозуванні також займає метод Делфі. Крім того, вживаними методами є: метод аналізу ієрархій [9], бібліометричний та патентний аналіз, огляд науково-технічної інформації, мозковий штурм, еталонний аналіз (бенчмаркінг) [10].

Метод критичних технологій, який описаний у роботі [10], оперує звичайним експертним опитуванням. Це значно знижує якість експертної оцінки, в порівнянні з тим же Делфі. Крім того, не запропоновано принцип граничного рівня критичності технологій під час їх відбору.

Відомо, що у РФ для формування переліку КТ у 1996 та 2008 роках застосовувався метод Делфі [11], в Європі, крім того, використовували SWOT-аналіз [12]. Європейські вчені також зазначають, що найпоширеніший метод – Делфі, а часто використовуваними є метод сценаріїв, експертні панелі, дорожні карти, SWOT-аналіз [5], [13-16].

**Метою даної роботи** є розроблення ефективного механізму формування переліку критичних технологій для оборонної сфери України, шляхом комбінування найбільш підходящих методів прогнозування, виявлення та усунення їх недоліків.

### Виклад основного матеріалу дослідження

Проаналізувавши роботи [4-7], [9-16] автори статті запропонували 12-ти бальний рейтинг найпоширеніших методів науково-технологічного форсайту (рис.1).

Експерти погоджуються, що не існує універсальної методики форсайту [5], [13], [15-16]. Дослідження, проведені британськими вченими, показали, що зазвичай здійснюється комбінування методів (із 33 найбільш поширених) для якісного проведення форсайту [13].

З метою оцінки потенційної можливості застосування запропонованих вище методів, проаналізуємо специфіку кожного з них.

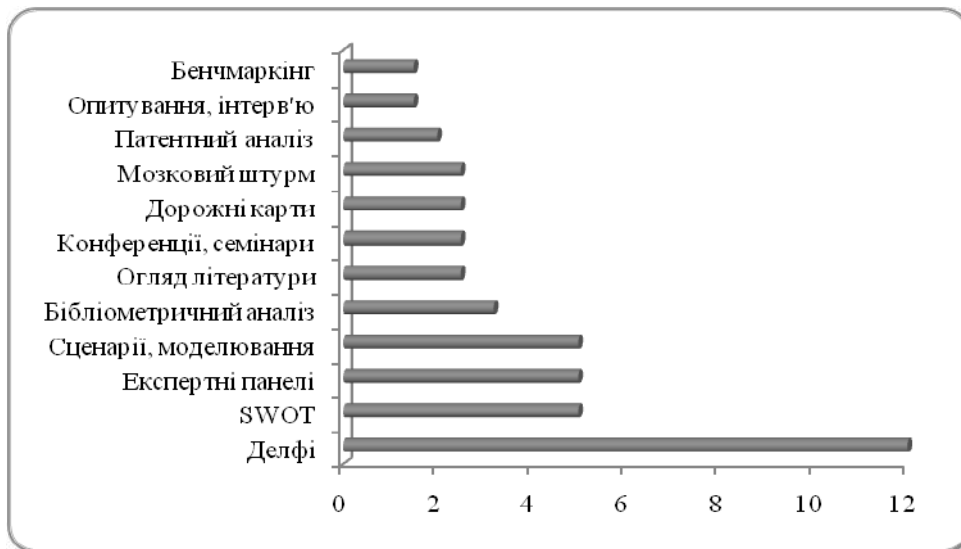


Рис. 1. Рейтинг методів форсайту

**1. Бенчмаркінг (benchmarking) – метод еталонного аналізу.** Це метод, в якому здійснюється об'єктивне порівняння чисельних показників запропонованих КТ із еталонними. У випадку прогнозування пріоритетних КТ України доцільно прийняти за еталон загальносвітові тенденції. Однак виявлення таких тенденцій – це окреме досить складне дослідження, тому такий

метод раціонально застосовувати лише для звуження вже опрацьованого переліку КТ.

**2. Опитування та інтерв'ю.** Досить простий метод, який базується на особистому спілкуванні з респондентом. Такий підхід не дозволяє експертам абстрагуватися від психологічного та емоційного фону, що вносить похибки у відповіді. Крім того, метод вимагає значних витрат часу, особливо

якщо експерти знаходяться в різних місцях.

**3. Патентний аналіз.** Проаналізувавши кількість виданих патентів на винаходи по рокам, можна прослідкувати тенденції розвитку певної технології, що дає можливість спрогнозувати її актуальність в довгостроковій перспективі. Запропонований аналіз варто проводити як за патентною базою України, так і за хоча б декількома найбільш розвиненими країнами. Однак, зважаючи на величезну кількість рубрик (більше 70 тисяч) у міжнародному класифікаторі патентів, такий аналіз буде досить трудомістким.

**4. Мозковий штурм (brainstorm).** Основою методу є генерація нових ідей, творче і негайне прийняття рішень експертами стосовно щойно запропонованих питань. Використання цього методу не є можливим, оскільки експерти ще на етапі їх відбору заздалегідь мають розуміти суть експертного опитування. Тому ефект неочікуваності буде відсутній, що в принципі нівелює суть методу взагалі.

**5. Дорожні карти.** Метод дорожньої карти – це деталізований і покроковий варіант розвитку КТ. Експерти прогнозують не лише кінцевий продукт від впровадження технології, а й етапи її розвитку, враховуючи всі можливі чинники. Для планування на 20 років цей метод стане складним в реалізації, оскільки врахувати всі чинники не реально.

**6. Конференції, семінари.** Організоване зібрання експертів з індивідуальними виступами та обговоренням. Цей метод було б доцільно використовувати для затвердження остаточного переліку КТ, як в групах експертів за напрямками, так і в експертній комісії загалом.

**7. Бібліометрія (бібліометричний аналіз та огляд літератури).** По суті бібліометрія (від грецької «biblio» - книга, «metro» - міряти) включає в себе огляд літератури (наукові публікації, книги, звіти, веб-сайти, матеріали конференцій та ін.), індекс цитувань, рейтинг авторів, розподіл за країнами і т.д. Такий аналіз дає конкретні кількісні показники, завдяки чому досить легко побудувати ранжування технологій.

**8. Сценарії.** Розробка сценаріїв досить схожа на метод дорожніх карт, тільки в цьому методі здійснюється розробка декількох варіантів розвитку КТ, також враховуючи всі можливі чинники на всіх етапах розвитку. Потім експертами скорочується кількість сценаріїв, шляхом об'єднання схожих чи видалення неприйнятних.

**9. Метод експертних панелей.** Експертна комісія поділяється на групи (експертні панелі) відповідно до фахової приналежності. Експертні групи оцінюють “критичність” технологій на основі встановлених критеріїв. Зазвичай цей метод комбінується з опитуванням, обговоренням, бібліометричним аналізом та ін. Обробка результатів опитування експертів може здійснюватись різними методами. Одним із таких є **метод аналізу ієрархії Сааті.**

**10. SWOT-аналіз.** Процес полягає в розділенні факторів впливу на чотири категорії: сильні

(Strengths) та слабкі (Weaknesses) сторони певної технології, можливості (Opportunities) та загрози (Threats), пов'язані з її реалізацією. Результатом такого аналізу має бути рішення: «Входитиме певна технологія до переліку критичних, чи ні?» У запропонованому методі оцінюється кожна технологія окремо. SWOT-аналіз має місце у разі прийняття рішень стосовно невеликої кількості альтернатив, при цьому початковий перелік КТ має бути вже сформований на початок опитування.

**11. Делфі.** Базовим принципом цього методу є відсутність впливу думок експертів між собою. Кожен експерт окремо відповідає на поставлені йому питання, при цьому не знаючи, хто входить до складу експертної групи та як вони відповідають. При такому підході відкидається вплив групової думки. Крім того, опитування можна здійснювати за екстериторіальним принципом. Зазвичай проводять декілька ітерацій, постійно зменшуючи список альтернатив до того моменту, доки не буде отримана усереднена думка від більшості експертів.

Після проведеного аналізу стає зрозумілим, що такі методи як бенчмаркінг, опитування, мозковий штурм, дорожні карти та сценарії, конференції та семінари, а також SWOT-аналіз в чистому вигляді не можуть використовуватись для технологічного форсайту. За відсутності значної кількості статистичних даних про певні технології, ми також не можемо застосувати виключно методи бібліометрії та патентного аналізу.

В запропонованій методиці відбору критичних технологій авторами пропонується скомбінувати статистичні та експертні методи.

**Методика відбору критичних технологій.** У 2019 році відбувалася актуалізація переліку КТ України в оборонній сфері, що по своїй суті означає проведення форсайт-проекту. Авторами даної роботи запропонована методика, яка враховує не тільки світові тенденції форсайту, а й специфіку оборонної сфери України зокрема.

**На першому (підготовчому) етапі** організатори дослідження формують експертну комісію, визначаються із кількісним складом експертних груп та їх компетентністю (рис. 2).

Більшість науковців, які вивчають прогнози дослідження, упускають питання відбору експертів, відмежовуючись фактом найвищої кваліфікації для останніх. Однак, в деяких роботах все ж запропоновані методи відбору експертних груп. Наприклад, прийом «сніжного кому», коли кожен експерт пропонує декілька прізвищ спеціалістів у досліджуваній темі, а ті, в свою чергу, пропонують нових і т.д. В таких умовах упускаються думки науковців з інших наукових «кланів». Досить поширений варіант відбору експертів за допомогою формальних ознак (посада, вчене звання, науковий ступінь та ін.).

Найбільш вживаними методами оцінки компетентності експертів є: самооцінка, взаємооцінка, оцінка за об'єктивними формальними даними та оцінка відповідності відповідей експерта [17-21]. Коефіцієнт

конкордації, як характеристика узгодженості експертної думки, є інструментом для розуміння схожості та єдності мислення експертів.

Однак, у випадку технологічного прогнозу, оцінювання експертів за відповідністю їх відповідей до узагальноної думки не може бути застосований, оскільки є невизначена вірогідність того, що саме експерт з іншою (не загальною) думкою може дати якісний і креативний прогноз.

Авторами публікації не будуть розглядатися всі «за» та «проти» кожного методу, оскільки це окреме досить дискусійне питання. Єдине в чому погоджується більшість авторів подібних публікацій – експерти мають бути спеціалістами найвищої кваліфікації в досліджуваній тематиці. Ніяких універсальних методик не існує, а вибір компетентних експертів є справою організаторів дослідження та показником їх фаховості.

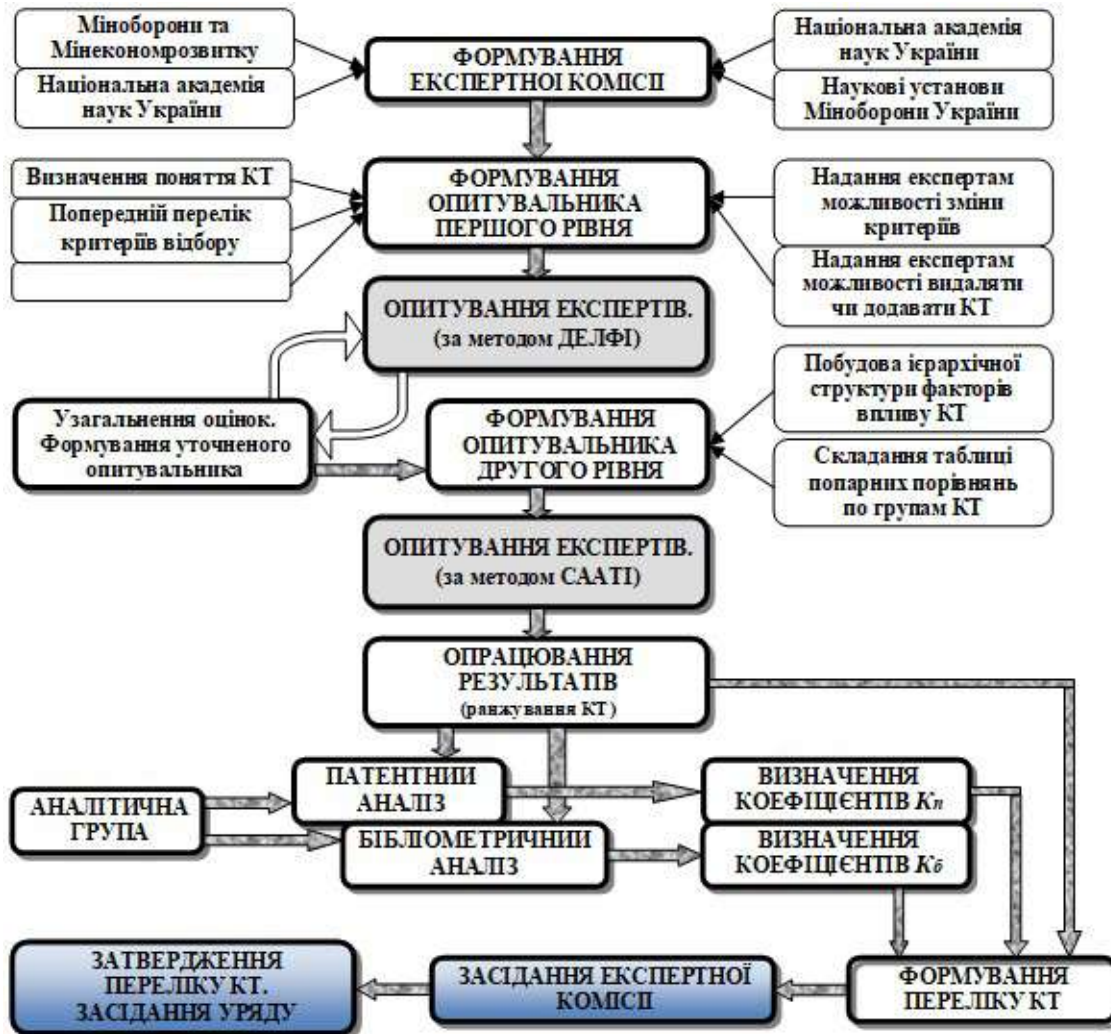


Рис. 2. Структурно-логічна схема визначення критичності технологій

Основну масу голосів експертної комісії має забезпечувати наукова спільнота, яка спеціалізується на розробці та дослідженні перспективних технологій. Пропонується обирати експертів від науково-дослідних установ Міністерства оборони, як найбільш висококваліфікованих науковців у галузі розвитку перспективних оборонних технологій; від науково-дослідних установ Національної академії наук України, як розробників фундаментальних засад розвитку КТ; та (у разі необхідності) експертну комісію можна доповнити представниками від Міністерства освіти і науки, які спеціалізуються на науково-технологічних прогнозах.

Не можна оминати увагою представників підприємств оборонно-промислового комплексу

(далі – ОПК). Основою бізнесу є отримання прибутків, а не створення якісного товару, тому експерти можуть бути не об'єктивними. Однак ігнорувати їх голоси ми не можемо, оскільки саме їх підприємства будуть впроваджувати КТ в промисловість і тільки представники ОПК володіють інформацією про розробки, які вже ведуться на підприємстві, та перспективні.

До складу експертних груп також можуть бути включені експерти Міністерства оборони, як основний замовник і споживач, а також представники Міністерства економічного розвитку, які можуть оцінити КТ з точки зору можливості їх подвійного використання.

Проаналізувавши роботи [17-19] стає зрозумілим, що у більшості форсайт проєктів

середня кількість експертів у одній тематичній групі становить не більше 20 осіб. А дослідження, проведені американськими вченими у роботі [20], демонструють середню кількість експертів у межах 18-34 особи. Досить цікавим є той факт, що зазвичай вистачає 2-3 ітерації (за методом Делфі) для отримання консенсусного рішення.

Наступним кроком на підготовчому етапі має бути формування опитувальника, першим компонентом якого варто поставити визначення терміну КТ (наведено у вступі до даної статті).

Другим компонентом має бути попередній перелік КТ. За наявності ресурсів було б доцільно

провести масштабний бібліометричний аналіз та доповнити попередній перелік КТ новими перспективними технологіями, які можуть бути застосовані в оборонній сфері. Крім того, в опитувальнику обов'язково мають бути запропоновані критерії відбору.

Перелік критеріїв визначається відповідно до факторів, які впливають на прийняття рішень експертами. Такі фактори та узагальнюючі критерії наведені у табл. 1. Користуючись методом аналізу ієрархій досить легко продемонструвати структуру прийняття рішень щодо відбору технологій до переліку критичних (рис. 3).

Таблиця 1

Критерії оцінювання критичності технологій

№	Фактор впливу на прийняття рішення	Узагальнений критерій
1.	Використання у всіх видах ЗС України	Масштаб застосування
2.	Використання в інших силових структурах	
3.	Подвійне використання	
4.	Відповідність світовим тенденціям розвитку науки і технологій	Перспективність
5.	Потенційна необхідність застосування у перспективних зразках	
6.	Кадрове забезпечення для проведення наукових досліджень	Науково-технічний потенціал
7.	Рівень готовності виробничої, випробувальної та іншої матеріально-технічної бази	
8.	Ціна зразка перспективного озброєння	Економічна привабливість
9.	Науково-дослідні витрати	
10.	Експлуатаційні витрати зразка ОВТ	
11.	Підвищення тактико-технічних характеристик	Ефективність
12.	Вирішення принципово нових завдань	
13.	Строки серійного виробництва ОВТ та поставки у війська	Строки виготовлення

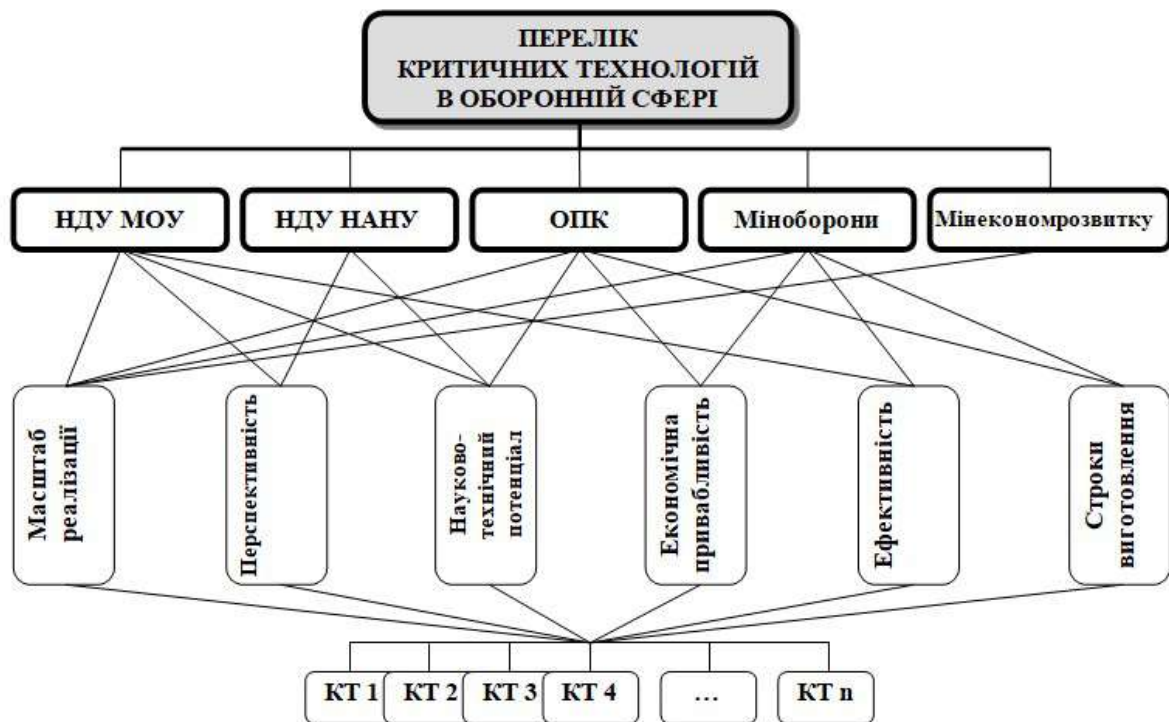


Рис. 3. Ієрархічна структура вибору критичних технологій

Другий етап (основний) включає в себе два рівні опитування експертів, патентний і бібліометричний аналіз та опрацювання результатів.

Перший рівень опитування здійснюється за методом Делфі (рис. 3), який є найбільш поширеним серед форсайтів і досить добре описаний у багатьох роботах, зокрема у [17-20],

тому деталі процесу опитування упускаємо.

Експертам дозволяється доповнювати запропонований перелік КТ та критеріїв відбору. Виставляючи знак «+» або «-», експерт пропонує включити чи виключити певний пункт з переліку, при цьому кожен експерт може аргументувати свій вибір. В результаті опитування організатори отримують максимальну кількість можливих варіантів критеріїв і КТ та конкретну кількість голосів за чи проти них. Це є основою для формування нових опитувальників.

Якщо експерти одногосно видаляють зі своїх опитувальників певну КТ чи критерій, це є підставою для організаторів видалити ці пункти з опитувальників наступної ітерації.

Друга ітерація здійснюється також за методом Делфі. Однак тепер експерти мають виставити оцінки за 10-бальною шкалою для кожної КТ та критерію. При цьому експерти знайомляться не тільки із оцінками, а й із судженнями та аргументацією колег з попереднього туру. Таким чином експерти можуть коригувати свою думку, відповідно до зазначених аргументів, що зближує їх оцінку до узгодженої.

За відсутності консенсусу у відповідях групи, класичний метод Делфі має продовжуватись доти, доки не буде досягнена узгоджена думка. Однак, такий прийом тягне за собою зворотну дію – конформізм. Багатьом експертам просто набридне участь в такому довготривалому проекті, а

наступні оцінки вже не будуть такими ж обдуманими, як і раніше. Крім того, ймовірно, деякі учасники експертизи не будуть досить принциповими та приєднуються до загальної думки [18]. На цьому етапі можна визначити перелік досліджуваних об'єктів з відповідним ранжуванням. Якщо замовник досліджень висунув вимогу стосовно кількості КТ у фінальному переліку, відповідно організатори відбирають визначену кількість з найвищим рейтингом та включають такі технології до матриць попарних порівнянь за методом Сааті. Однак, у випадку коли вищезазначеної вимоги не висунуто, тоді виникає серйозне питання, а які ж об'єкти досліджень варто пропускати до наступного туру?

Запропонований варіант розв'язання такої задачі ґрунтується на диференціюванні апроксимованої функції та знаходженні точки  $x_0$ , в якій похідна буде рівна 1. Відомо, що в околі такої точки приріст функції та приріст аргументу будуть рівними. До  $x_0$  приріст функції зростає менше ніж приріст аргументу, а після неї – більше. Тому точка  $x_0$  слугуватиме для нас межею, до якої значення функції зростає несуттєво.

Для кращого розуміння розглянемо приклад.

**Приклад.** Експертна група оцінювала 12 запропонованих технологій за 10-ти бальною шкалою. Узагальнені оцінки критичності виявились наступними:

Таблиця 2

Узагальнені оцінки критичності технологій (приклад)

Порядковий номер критичної технології	1	2	3	4	5	6	7	8	9	10	11	12
Узагальнена оцінка (оцінка критичності технології)	2	1	2	5	9	8	9	10	10	5	4	1

На рисунку 4 можна спостерігати графік, який є вираженням таблиці 2, але побудований за принципом зростання оцінок по технологіям, а не за порядковими номерами. За допомогою

програми Excel будемо відповідний графік, проводимо апроксимацію та отримуємо наближену функцію з певною достовірністю. Такі функції можемо спостерігати у табл. 3 та рис. 5.

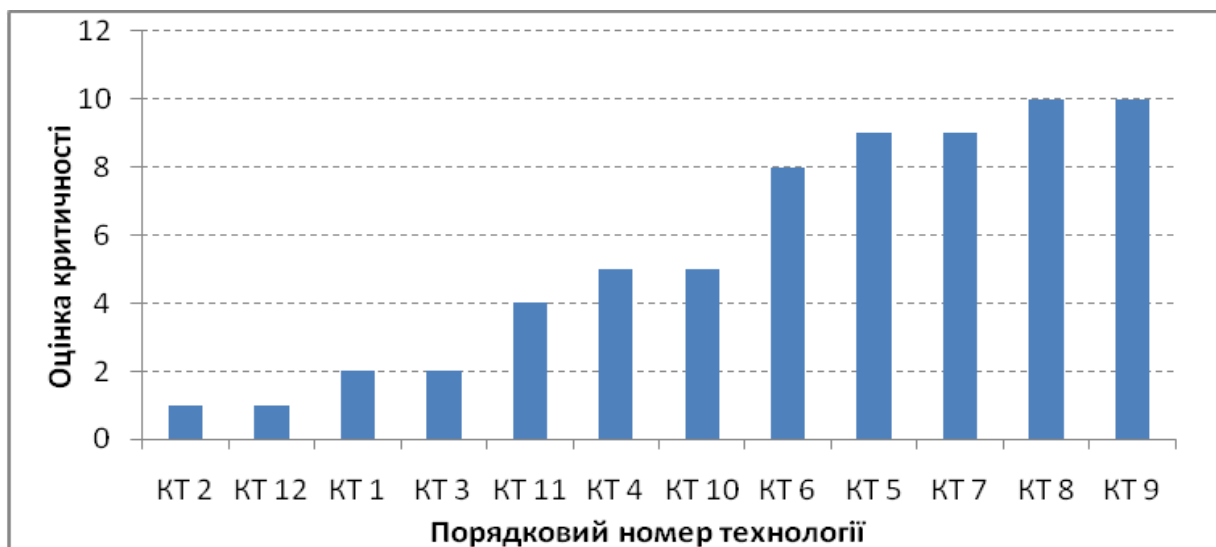


Рис. 4. Розподіл критичних технологій у порядку зростання узагальненої оцінки



Наближені (апроксимовані) функції		
Функція апроксимації	Математичний вираз наближеної функції	Достовірність апроксимації
Логарифмічна	$y = 4,268 \ln(x) - 1,608$	$R^2 = 0,823$
Експоненціальна	$y = 0,921 e^{0,231x}$	$R^2 = 0,915$
Степенева	$y = 0,65x^{1,112}$	$R^2 = 0,929$
Лінійна	$y = 0,965x - 0,772$	$R^2 = 0,958$
Поліноміальна	$y = -0,016x^3 + 0,324x^2 - 0,803x + 1,535$	$R^2 = 0,981$

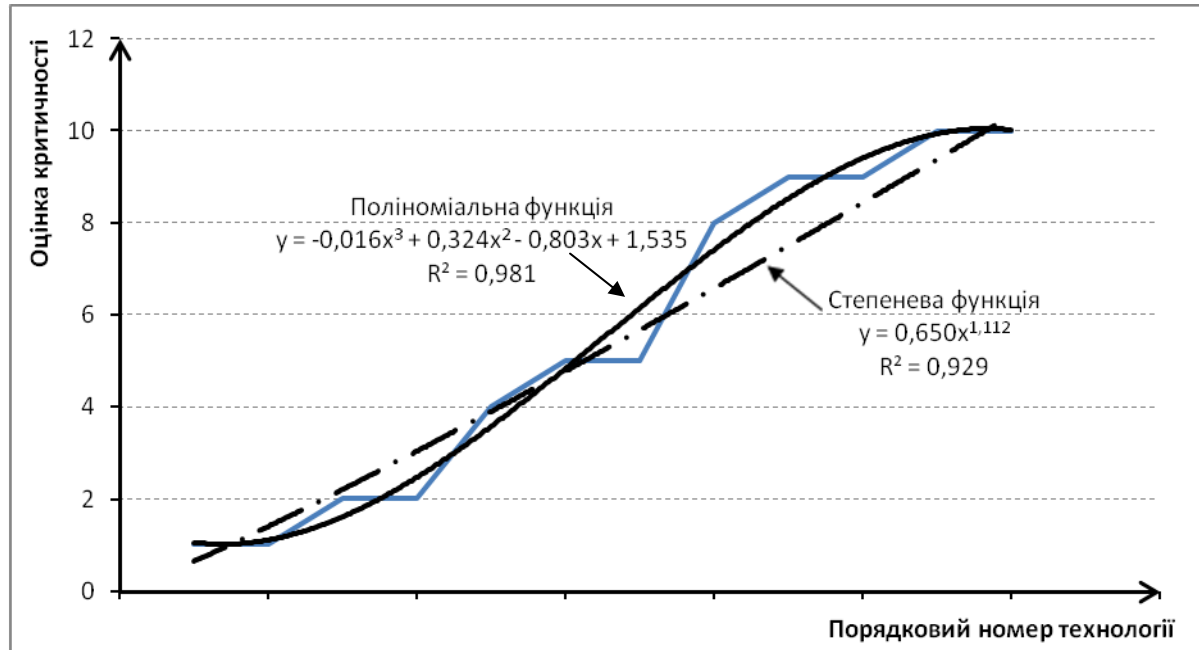


Рис. 5. Побудова апроксимованої функції залежності критичної технології від узагальненої оцінки

Найвищу достовірність побудови наближеної функції має поліноміальна функція, похідна від якої має вираз:  $y' = -0,048x^2 + 0,648x - 0,803$ .

Точка, в якій похідна першого порядку дорівнює одиниці ( $x_0$ ) – це точка, в нескінченно малому околі якої приріст ординати та приріст абсциси рівні. До цієї точки задовольняється нерівність  $\Delta y < \Delta x$ , а після неї  $\Delta y > \Delta x$ .

В нашому практичному випадку до точки  $x_0$  зростання оцінки КТ набагато менше, ніж відповідне зростання після неї. Вирахувавши значення  $x_0$ , ми отримаємо поріг, до якого зростання оцінки технологій не суттєве. Такі технології мають низьку оцінку, тому і не попадають до наступного етапу дослідження.

В нашому випадку:  $y' = 1 \Leftrightarrow x_0 = [4; 9,6]$ . Ми отримали два значення, що означає наявність двох точок, де похідна дорівнює 1. Тобто після точки  $x_0 = 4$  значення функції значно більше зростає, ніж до неї. У наведеному прикладі перші чотири технології не попадають до переліку КТ. Це: КТ2, КТ12, КТ1, КТ3.

**Другий рівень опитування.** Сформований список КТ та критеріїв записують до матриць попарних порівнянь (за методом Сааті). Метод аналізу ієрархії Сааті досить поширений і добре описаний у багатьох джерелах, зокрема у [9], [21-24].

До речі саме метод попарних порівнянь

використовувався у дослідженні [25] для оцінки вагомості характеристик бойових машин.

Завдяки розподіленню КТ за науковими напрямами (тематичними групами), для зручності експертів, матриця попарних порівнянь не має перевищувати розмір 15x15. Крім того, це максимальне значення розмірності матриці, для яких розраховані середні значення випадкових індексів [22].

Опитувальники знову розсилаються експертам, які оцінюють як вагомість критеріїв, так і критичність технологій.

Опрацювавши результати опитування (за методом Сааті), отримаємо попереднє ранжування КТ. Окремо відібраною аналітичною групою проводимо патентний та бібліометричний аналіз за кожною КТ. Щоб прослідкувати тренди, аналіз має проводитись за період не менше 8-10 років. Отримані статистичні дані дають змогу розрахувати додаткові коефіцієнти  $K_n$  та  $K_6$ , які характеризують динаміку розвитку КТ.

$$K_n = \frac{\sum_{i=n+1}^n x_i}{\sum_{i=1}^{n/2} x_i}, K_6 = \frac{\sum_{i=n+1}^n y_i}{\sum_{i=1}^{n/2} y_i}, K = \frac{K_6 + K_n}{2}$$

де:  $K_n$  – коефіцієнт динаміки КТ за патентним аналізом;

$K_6$  – коефіцієнт динаміки КТ за бібліометричним аналізом;

$K$  – статистичний коефіцієнт динаміки КТ;  
 $i$  – рік аналізу;  
 $n$  – період аналізу (кількість років, що охоплюються аналізом);  
 $x$  – кількість виданих патентів;  
 $y$  – кількість публікацій.

Після нормування отримаємо другий ранжований перелік КТ за статистичними показниками. Перемножуючи внормований статистичний коефіцієнт і коефіцієнт пріоритету (отриманий методом Саати), ми отримуємо об'єктивний показник, який враховує як експертні оцінки, так і статистичні дані, після чого проводиться остаточне ранжування КТ.

**Третій етап (заключний).** Ранжований перелік КТ подається на засідання експертної комісії для обговорення та прийняття рішення щодо включення до остаточного переліку КТ з найвищим рейтингом. Після схвалення перелік

### Література

1. **Баланчук І.С.** Досвід інноваційного розвитку Південної Кореї і його адаптація в Україні. *Наука, технології, інновації*. 2018. № 3. С. 50-54. 2. Наукові дослідження і розробки у 2018 році. Держстат: веб-сайт. URL: <https://ukrstat.gov.ua>. 3. **Купчин А., Сотник В.** Критичні технології в оборонній сфері. Новий погляд. *Озброєння та військова техніка*. 2019. № 2. С. 35-42. [https://doi.org/10.34169/2414-0651.2019.2\(22\).35-41](https://doi.org/10.34169/2414-0651.2019.2(22).35-41) 4. **Паладченко О.Ф., Молчанова І.В.** Сучасні підходи і методи проведення прогностичних досліджень: світовий досвід і можливість його використання в Україні. *Наука, технології, інновації*. 2018. № 2. С. 23-32. 5. **Gibson E., Daim T., Garcés E., Dabic M.** Technology foresight: a bibliometric analysis to identify leading and emerging methods. *Foresight and STI governance*. 2018. № 1. Р. 6-24. <https://doi.org/10.17323/2500-2597.2018.1.6.24> 6. **Величко О., Затинайко О., Скурський П.** Реалізація національної безпеки держави в контексті глобальних кліматичних змін. *Наука і оборона*. 2011. № 4. С. 23–24, 28–29. 7. **Довгополий А.С., Сотник В.В., Томчук В.В.** та ін. Пріоритетний розвиток критичних технологій – запорука зміцнення обороноздатності та економічного зростання держави. *Озброєння та військова техніка*. 2019. № 1. С. 16-17. [https://doi.org/1034169/2414-0651.2019.1\(21\).15-21](https://doi.org/1034169/2414-0651.2019.1(21).15-21) 8. **Горбулін В.П., Шеховцов В.С., Шевцов А.І.** Проблемні питання визначення і впровадження критичних технологій у сфері виробництва озброєння. *Вісник НАН України*. 2018. № 2. С. 3. 9. **Буренок В.М., Івлев. А.А., Корчак В.Ю.** Развитие военных технологий XXI века: проблемы планирование, реализация. Тверь: Вид. «Купол», 2009. С. 166, 178. 10. **Соколов А.В.** Метод критических технологий. *Форсайт*. 2007. № 4. С. 64-74. 11. **Мухутдинова Т.З.** Приоритетные направления развития науки, технологий и техники Российской Федерации и критические технологии федерального уровня: история разработки и динамика развития. *Вестник Казанского технологического университета*. 2012. № 14. С. 249. 12. **Кольцов А.В., Октябрьский А.М., Хабарова Т.В.** Критические технологии и приоритетные направления развития науки и техники в рамках реализации ФЦП развития научно-технологического комплекса Российской Федерации. *Инноватика и экспертиза*. 2016. № 3. С. 33, 36. 13. **Georghiou I., Harper J., Keenan M.** The handbook of technology foresight. Concepts and practice. Bodmin, Cornwall: MPG books Ltd, 2008. P. 17-75. URL: [https://books.google.com.ua/books/about/The\\_Handbook\\_of\\_Tech](https://books.google.com.ua/books/about/The_Handbook_of_Tech)

подають на затвердження до Кабінету Міністрів України.

### Висновки й перспективи подальших досліджень

Запропонована в цій роботі методика відбору критичних технологій дає можливість якісно провести аналіз технологій як з точки зору статистичних даних (об'єктивні оцінки), так і враховуючи експертні (суб'єктивні) оцінки. Крім того, поєднання в експертному опитуванні методів Делфі та аналізу ієрархій, дозволило якісно врахувати позитивні сторони кожного з них.

Враховуючи досвід найрозвиненіших країн стосовно розвитку КТ, а також значну увагу, яка приділяється питанням прогностичних досліджень у світі, розроблена методика може стати дієвим інструментом технологічного форсайту та, як наслідок, зростання економіки та обороноздатності країни в цілому.

[nology\\_Foresight.html?hl=uk&id=3SxmAwAAQBAJ&redir\\_esc=y](nology_Foresight.html?hl=uk&id=3SxmAwAAQBAJ&redir_esc=y) 14. **Romanowski M., Nadolny K.** Technological Foresight – characterisation of research methods used in prospective analysis. *Journal of Mechanical and Energy Engineering*. 2018. № 2. P. 101-108. <https://doi.org/10.30464/jmee.2018.2.2.101> 15. **Bühning J., Liedtka J.** Embracing systematic futures thinking at the intersection of Strategic Planning, Foresight and Design. *Journal of Innovation Management*. 2018. № 3. P. 134-152. [https://doi.org/10.24840/2183-0606\\_006.003\\_0006](https://doi.org/10.24840/2183-0606_006.003_0006) 16. **Korreck S.** Opening up Corporate Foresight: What Can We Learn from Open and User Innovation? *Journal of Innovation Management*. 2018. № 3. P. 153-177. [https://doi.org/10.24840/2183-0606\\_006.003\\_0007](https://doi.org/10.24840/2183-0606_006.003_0007) 17. **Кургов А.І., Полікашин О.В., Потіхенський А.І., Александров В.М.** Експертні оцінки. Метод «Делфі» як технологія прийняття управлінських рішень. *Збірник наукових праць ХНУИС*. 2017. № 1(50). С. 118-122. 18. **Горбатенко В., Петренко І.** Метод „Делфі” та специфіка його застосування у прогностичних розробках. *Політичний менеджмент*. 2008. № 6. С. 174-182. 19. **Anthony F. Jorm.** Using the Delphi expert consensus method in mental health research. *The Australian & New Zealand Journal of Psychiatry*. 2015. № 10(49). P. 887-897. <https://doi.org/10.1177/0004867415600891> 20. **Skinner R., Nelson R., Wynne W., Chin and Lesley Land.** The Delphi Method Research Strategy in Studies of Information Systems. *Communications of the Association for Information Systems*. 2015. № 2 (37). P. 31-63. <https://doi.org/10.17705/1CAIS.03702> 21. **Полегенько А.Ф., Круковський-Синевич К.Б., Коростелів О.П.** Метод анализа иерархий. Некоторые аспекты практического применения. Киев: ЦНИИ ВВТ ВСУ, 2011. 154 с. 22. **Саати Т.** Принятие решений. Метод анализа иерархий. М: «Радио и связь», 1993. 278 с. 23. **Ossadnik W., Schinke S., Kaspar R.** Group Aggregation Techniques for Analytic Hierarchy Process and Analytic Network Process: A Comparative Analysis. *Group Decision and Negotiation*. 2015. № 2(25). P. 432-448. <https://doi.org/10.1007/s10726-015-9448-4> 24. **Enrique Mu, Milagros Pereyra-Rojas.** Practical Decision Making. Springer: Cham, 2017. 111p. <https://doi.org/10.1007/978-3-319-33861-3> 25. **Арістархов О., Бісик С., Слюсар В.** Оцінка вагомості показників бронетранспортера за даними опитування з використанням методу парного порівняння. *Озброєння та військова техніка*. 2019. № 2. С. 42-49. [https://doi.org/10.34169/2414-0651.2019.2\(22\).42-49](https://doi.org/10.34169/2414-0651.2019.2(22).42-49)

**МЕТОДИКА ОТБОРА КРИТИЧЕСКИХ ТЕХНОЛОГИЙ**

*Владислав Витальевич Сотник (кандидат технических наук, старший научный сотрудник)*

*Александр Алексеевич Расстрыгин (доктор технических наук, профессор)*

*Артем Валерьевич Купчин*

*Центральный научно-исследовательский институт вооружения и военной техники ВС Украины,  
Киев, Украина*

Прогнозные исследования, в зарубежной практике более известны как форсайт, представляют собой предусловие для стабильного развития страны в любой отрасли. В данной работе проведен анализ основных наиболее распространенных методов технологического форсайта, которые используются как в Украине, так и в других странах. Определены как положительные, так и отрицательные черты каждого из них. Исследование показало, что наиболее распространенными являются методы Делфи, SWOT-анализ, экспертные панели, сценарии, моделирование, библиометрический анализ и др.

Проведенный анализ также указал, что такие методы, как бенчмаркинг, опрос, мозговой штурм, дорожные карты и сценарии, конференции и семинары, а также SWOT-анализ в чистом виде не могут быть применены для форсайта технологий в оборонной сфере. В случае отсутствия определенного количества статистических данных, мы также не можем говорить о применении исключительно методов библиометрического и патентного анализа. По этому, в условиях ограниченного объема статистических данных без экспертных методов не обойтись, но при этом нужно учитывать, что экспертные оценки всегда имеют погрешность.

Для определения перечня критических технологий в оборонной сфере Украины, авторами статьи предложена новая методика технологического форсайта – комбинационная методика отбора критических технологий. Она комбинирует в себе экспертные методы (Делфи и метод анализа иерархий) и статистические (патентный и библиометрический анализ).

В работе описан полный алгоритм проведения прогнозных исследований, касаемо определения перечня критических технологий в оборонной сфере Украины.

Кроме того, продемонстрирована полная структура принятия решений относительно отбора технологий к перечню критических, с описанием состава экспертной комиссии и обобщенными критериями отбора.

Предложен новый принцип отсекаания неприоритетных технологий на основе дифференцирования аппроксимированной функции и определения точки одинаковых приростов абсцисс та ординат. Алгоритм предполагает проведение двух этапов опроса, за методом Делфи и парных сравнений, а также проведение библиометрического и патентного анализа. В результате проведенного форсайта по комбинационной методике мы получаем объективное ранжирование критических технологий.

**Ключевые слова:** форсайт, прогнозные исследования, критические технологии, ключевые технологии, метод анализа иерархий, Делфи.

**METHOD OF THE CRITICAL TECHNOLOGIES SELECTION**

*Vladyslav Sotnyk (Candidate of Technical Sciences, Senior researcher)*

*Oleksandr Rasstrygin (Doctor of Technical Sciences, Professor)*

*Artem Kupchyn*

*Central research institute of armaments and military equipment of the Armed forces of Ukraine, Kyiv,  
Ukraine*

An important condition for the stable development of the country is quality predictive research, in international practice better known as foresight. In this paper, authors analyze the most popular methods of technological foresight, which are used both in Ukraine and in other countries. The positive and negative traits of each of them are determined. This research showed that the most common methods of technological foresight are Delphi, SWOT analysis, expert panels, scenarios, modeling, bibliometric and patent analysis, etc.

The analysis also indicated that methods, such as benchmarking, polling, brainstorming, roadmaps and scenarios, conferences, seminars and SWOT analysis cannot be applied to technological foresight in defense sphere.

We also cannot talk about the use of exclusively methods of bibliometric and patent analysis, if the statistical data is not enough to predictive research. Therefore, we cannot forecast future technological directions without expert methods, but it should be borne in mind that expert estimates always have an error.

The authors proposed a new method of technological foresight to determine the list of critical technologies in the defense sector of Ukraine - the method of critical technologies. It combines expert methods (Delphi and expert panel method) and statistical methods (patent and bibliometric analysis).

The paper describes the complete algorithm of conducting predictive research regarding to determine the critical technologies list in the defense sector of Ukraine.

In addition, the full decision-making structure the selection of technologies to the list of critical ones was demonstrated, with a description of the composition of the expert commission and generalized selection criteria. A new principle is proposed for cutting off non-priority technologies based on differentiation of the approximated function and determination of the point of equal increments of abscissa and ordinate. The algorithm involves carrying out two stages of the survey, the Delphi method and method of pairwise comparisons, bibliometric and patent analysis. As a result of the foresight by the method of critical technologies, we get an objective ranking of critical technologies.

**Key words:** foresight, predictive research, critical technology, key technology, analytic hierarchy process, Delphi.

## References

- Balanchuk I.** (2018), "Dosvid innovaciynoho rozvytku Pivdennoi Korei i yoho adaptaciya v Ukraini" [Experience of innovative development of South Korea and its adaptation in Ukraine], *Science, technologies, innovations*, No. 3, pp. 50-54.
- The official site of ukrstat.gov.ua, "Naukovi doslidjennya i rozrobky u 2018 roczii" [Research and development in 2018], available at: <https://ukrstat.gov.ua> (accessed 20 June 2019).
- Kupchyn A., Sotnyk V.** (2019), "Krytychni tehnologii v oboronniy sferi. Novyi pohlyad" [Critical technologies in the defense sphere. A new look], *Weapons and military equipment*, No. 2, pp. 35-42. [https://doi.org/10.34169/2414-0651.2019.2\(22\).35-41](https://doi.org/10.34169/2414-0651.2019.2(22).35-41)
- Paladchenko O.F., Molchanova I.V.** (2018), "Suchasni pidkhody i metody provedennya prohoznykh doslidjen: svitovyi dosvid i mojljvyst yoho vykorystannya v Ukraini" [Current approaches and methods of predictive research: world experience and the possibility of its use in Ukraine], *Science, technologies, innovations*, No. 2, pp. 23-32.
- Gibson E., Daim T., Garcés E., Dabic M.** (2018), "Technology foresight: a bibliometric analysis to identify leading and emerging methods", *Foresight and STI governance*, No. 1, pp. 6-24. <https://doi.org/10.17323/2500-2597.2018.1.6.24>
- Velychko O., Zatyayko O., Skursky P.** (2011), "Realizaciya nacionalnoi bezpeky derzhavy v konteksti globalnykh klimatichnykh zmin" [Realization of national state security in the context of global climate change], *Science and defense*, No. 4, pp. 23-24, 28-29.
- Dovhopolyi A.S., Sotnyk V.V., Tomchuk V.V., Kopylova Z.M., Bura E.B.** (2019), "Priorityetnyi rozvytok krytychnykh tehnologii – zaporuka zmichennya oboronozdatnosti ta ekonomichnogo zrostannya derjavy" [Priority development of critical technologies - the key to strengthening the defense capability and economic growth of the state], *Weapons and military equipment*, No. 1, pp. 16-17. [https://doi.org/1034169/2414-0651.2019.1\(21\).15-21](https://doi.org/1034169/2414-0651.2019.1(21).15-21)
- Horbulyi V.P., Shekhovcov V.S., Shevczov A.I.** (2018), "Problemni pytannya vyznachennya i vprovadjennya krytychnykh tehnologii u sferi vyrobnyctva ozbroennya" [Problematic issues of identification and implementation of critical technologies in the arms production], *Bulletin of the National Academy of Sciences of Ukraine*, No. 2, p. 3.
- Burenok V.M., Ivlev A.A., Korchak V.U.** (2009), "Razvitie voennykh tehnologii XXI veka: problemy, planirovanie, realizaciya" [Development of military technologies of the 21st century: problems of planning, implementation], Tver: Kupol, pp. 166,178.
- Sokolov A.V.** (2007), "Metod kriticheskikh tehnologii" [Method of the critical technologies], *Foresight*, No. 4, pp. 64-74.
- Mukhutdinova T.Z.** (2012), "Priorityetnye napravleniya razvitiya nauki, tehnologii i tekhniki Rossiyskoy Federaczii i kriticheskie tehnologii federalnogo urovnya: istoriya razrabotki i dinamika razvitiya" [Priority directions of development of science, technology and technology of the Russian Federation and critical technologies of the federal level: development history and dynamics of development], *Bulletin of Kazan Technological University*, No. 14, p. 249.
- Kolczov A.V., Oktyabrskii A.M., Khabarova T.V.** (2016), "Kriticheskie tehnologii i priorityetnye napravleniya razvitiya nauki i tekhniki v ramkakh realizaczii FCP razvitiya nauchno-tehnologicheskoho kompleksa Rossiyskoy Federaczii" [Critical technologies and priority areas for the development of science and technology in the framework of the implementation of the federal target program for the development of the scientific and technological complex of the Russian Federation], *Innovation and Expertise*, No. 3, pp. 33, 36.
- Georghiou I., Harper J.C., Keenan M., Miles I., Popper R.** (2008), The handbook of technology foresight. Concepts and practice, Bodmin, Cornwall: MPG books Ltd, pp. 17, 20, 21, 74, 75, available at: [https://books.google.com.ua/books/about/The\\_Handbook\\_of\\_Technology\\_Foresight.html?hl=uk&id=3SxmAwAAOBAJ&redir\\_esc=y](https://books.google.com.ua/books/about/The_Handbook_of_Technology_Foresight.html?hl=uk&id=3SxmAwAAOBAJ&redir_esc=y) (accessed 21 June 2019).
- Romanowski M., Nadolny K.** (2018), Technological Foresight – characterisation of research methods used in prospective analysis, *Journal of Mechanical and Energy Engineering*, No. 2, pp. 101-108. <https://doi.org/10.30464/jmee.2018.2.2.101>
- Jörn Bühring, Jeanne Liedtka** (2018), Embracing systematic futures thinking at the intersection of Strategic Planning, Foresight and Design, *Journal of Innovation Management*, No. 3, pp. 134-152. [https://doi.org/10.24840/2183-0606\\_006.003\\_0006](https://doi.org/10.24840/2183-0606_006.003_0006)
- Sabrina Korreck** (2018), Opening up Corporate Foresight: What Can We Learn from Open and User Innovation?, *Journal of Innovation Management*, No. 3, pp. 153-177. [https://doi.org/10.24840/2183-0606\\_006.003\\_0007](https://doi.org/10.24840/2183-0606_006.003_0007)
- A. Kurtov, O. Polikashyn, I. Potikhenskiy, V. Aleksandrov** (2017), "Ekspertni otsinky. Metod «Delphi» yak tehnologiya pryynyattya upravlins'kykh rishen" [Expert assessments. The Delphi method as a technology for managerial decision making], *Collection of scientific works of KNUAF*, No.1(50). – pp. 118-122.
- V. Horbatenko, I. Petrenko** (2008), "Metod „Delphi” ta spetsyfyka yoho zastosuvannya u prohoznykh rozrobkakh" [The Delphi method and the specifics of its application in predictive development], *Political management*, No.6. – pp. 174-182.
- Anthony F Jorm** (2015), Using the Delphi expert consensus method in mental health research, *The Australian & New Zealand Journal of Psychiatry*. No.10(49). pp. 887-897. <https://doi.org/10.1177/0004867415600891>
- Richard Skinner; R. Ryan Nelson; Wynne W. Chin and Lesley Land** (2015), The Delphi Method Research Strategy in Studies of Information Systems, *Communications of the Association for Information Systems*. No.2(37), pp. 31-63. <https://doi.org/10.17705/1CAIS.03702>
- A.F.Polegen'ko, K.B. Krukovskiy-Sinevich, O.P. Korostelov** (2011), "Metod analiza ierararkhiy. Nekotoryye aspekty prakticheskogo primeneniya", [Hierarchy Analysis Method. Some aspects of practical application], Kyiv: CRI AME AFU, 154 p.
- T. Saaty** (1993), "Prinyatie resheniy. Metod analiza ierararkhiy" [Decision making. Analytic hierarchy process], Moscow: Radio and communication, 278 p.
- Ossadnik W., Schinke S., Kaspar R.** (2015), Group Aggregation Techniques for Analytic Hierarchy Process and Analytic Network Process: A Comparative Analysis, *Group Decision and Negotiation*, No. 2 (25), pp. 432-448. <https://doi.org/10.1007/s10726-015-9448-4>
- Enrique Mu, Milagros Pereyra-Rojas** (2017), Practical Decision Making, Springer, Cham, 111p. <https://doi.org/10.1007/978-3-319-33861-3>
- Aristarkhov O., Bisyk S., Slyusar V.** (2019), "Otsinka vahomosti pokaznykiv bronetransportera za danyymi opytuvannya z vykorystannyam metodu popamoho porivnyannya" [The evaluation of weighting factors of armored personnel carriers characteristics according to the questionnaire with usage of method of paired comparisons], *Weapons and military equipment*, No. 2, pp. 35-42. [https://doi.org/10.34169/2414-0651.2019.2\(22\).42-49](https://doi.org/10.34169/2414-0651.2019.2(22).42-49)

*Сергій Станіславович Гаценко (кандидат технічних наук)  
Олександр Миколайович Ліщенко  
Андрій Іванович Сотніченко  
Ярослав Анатолійович Жарков*

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

## МАТЕМАТИЧНА МОДЕЛЬ ПРОЦЕСУ РОЗВІДУВАЛЬНО-ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ НЕВИЗНАЧЕНОСТІ

*Одним із основних технічних видів воєнної розвідки України, який постійно здійснюється (ведеться) в мирний час, особливий період, в інтересах національної безпеки і оборони держави та виконання завдань в операціях (бойових діях) є радіоелектронна розвідка.*

*Радіоелектронна розвідка добуває розвідувальну інформацію шляхом викриття функціонування радіоелектронних засобів і систем які застосовуються для управління військами (силами) та зброєю, а також здійснює збір, обробку, аналіз та доведення добутої розвідувальної інформації визначеним споживачам у встановлені терміни.*

*Для безперервного та своєчасного забезпечення споживачів визначеною інформацією, інформаційними (інформаційно-аналітичними) органами здійснюється комплекс заходів розвідувально-інформаційної діяльності, розвідувально-інформаційної роботи.*

*В умовах динамічності, багатогранності процесів обробки, аналізу, зберігання великих об'ємів інформації ключовим залишається завдання зменшення невизначеності інформації викликаной факторами еволюційного розвитку, факторами застосування складних інформаційних систем в різних умовах складної радіоелектронної та оперативної обстановки.*

***Ключові слова:** радіоелектронна розвідка; розвідувально-інформаційна діяльність; розвідувально-інформаційна робота; невизначеність інформації.*

### Вступ

**Постановка проблеми.** Зібрати у визначені терміни, оперативно обробити, проаналізувати та вчасно доповісти це є головним і вирішальним завданням розвідувально-інформаційної діяльності (РІД) в інтересах забезпечення прийняття рішення. Особливістю сучасної РІД є вирішення широкого кола інтелектуальних за змістом завдань: відбір і формування розвідувальних ознак; розпізнавання та ідентифікація об'єктів розвідки при неповній і нечіткій інформації в умовах значної невизначеності вихідних даних.

Відповідно, це зумовлює широке застосування відповідного науково-методичного апарату та впровадження сучасних інформаційних технологій в даний процес. Проте сьогодні стан розробок нових інформаційних технологій для автоматизації зазначених процесів залишається на низькому рівні, а формалізація розвідувально-інформаційної діяльності в умовах невизначеності інформації є актуальним науковим завданням.

**Аналіз останніх досліджень і публікацій.** Результати аналізу останніх досліджень і публікацій вказують на відсутність системного підходу щодо розвитку теорії інформаційно-аналітичної діяльності [1-3]. Можливість застосування інформаційних систем в процесі розвідувально-інформаційної діяльності розглянуто в [4]. В [5] основна увага автором

придільна застосуванню математичного апарату теорії нечітких множин для опису математичних моделей. У статті [6] запропоновано науково-методичний апарат на основі використання математичного апарату теорії нечітких множин, але не враховані інші види невизначеності при обробці інформації.

Все це створює передумови для систематизації знань у галузі РІД, формалізованого представлення процесів РІД та детального аналізу рівнів та видів невизначеностей що впливають на прийняття рішення.

**Мета статті.** Удосконалення науково-методичного апарату процесу розвідувально-інформаційної діяльності в інтересах прийняття рішення та проведення детального аналізу рівнів та видів невизначеностей.

### Виклад основного матеріалу дослідження

РІД являє собою безперервний у часі процес управління розвідувальними органами та містить комплекс заходів з організації та ведення розвідувально-інформаційної роботи для задоволення інформаційних потреб споживачів розвідувальної інформації (рис. 1) [7].

У формальному вигляді РІД являє собою процес створення потоку інформаційних повідомлень, які поступають у систему розвідки, а

потім у систему управління військами. Потік проходить через різні етапи (ланки) обробки, на кожному з яких інформаційні повідомлення

визначаються і до виконавця потрапляють у формі бойових розпоряджень і цілевказівок.

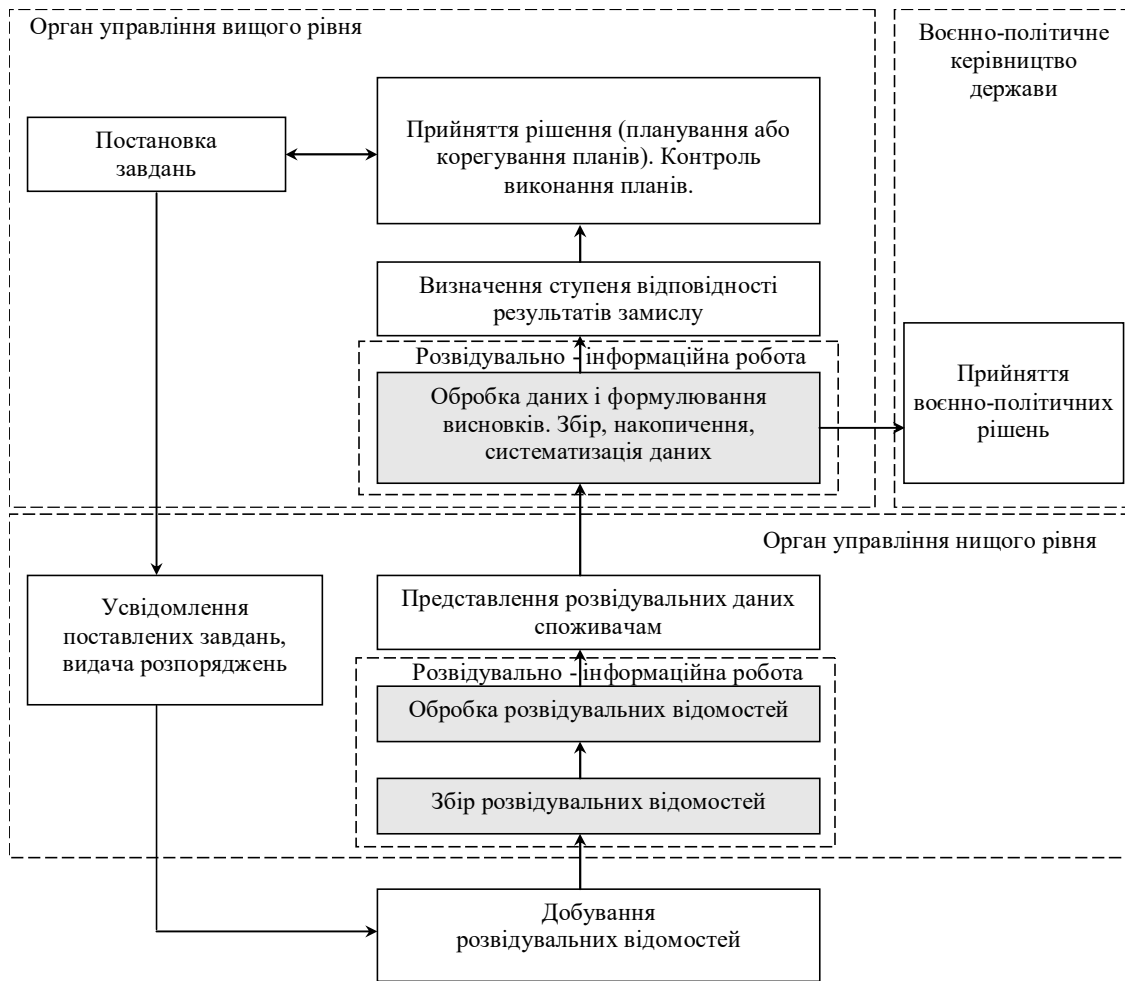


Рис. 1. Процес розвідувально-інформаційної діяльності

Кожен етап РІД являє собою комплекс організаційних заходів циклу управління, що відбуваються на командних пунктах, у штабах, відділах, службах, з використанням технічних засобів обробки і управління. Ланки РІД є частинами конкретних організаційно-технічних систем розвідки і управління військами, що певним чином взаємопов'язані і у формальному вигляді являють собою інформаційну мережу.

Мережа, як засіб формалізації складових процесів РІД (рис. 2) дає можливість відображення структури проходження розвідувальної інформації; представлення у наглядній формі із заданим ступенем деталізації взаємозв'язків і логічні послідовності окремих процесів та їх тривалість; оцінювання ступені важливості кожної організаційної ланки; визначити варіант інформаційної структури, що є оптимальною за певним критерієм.

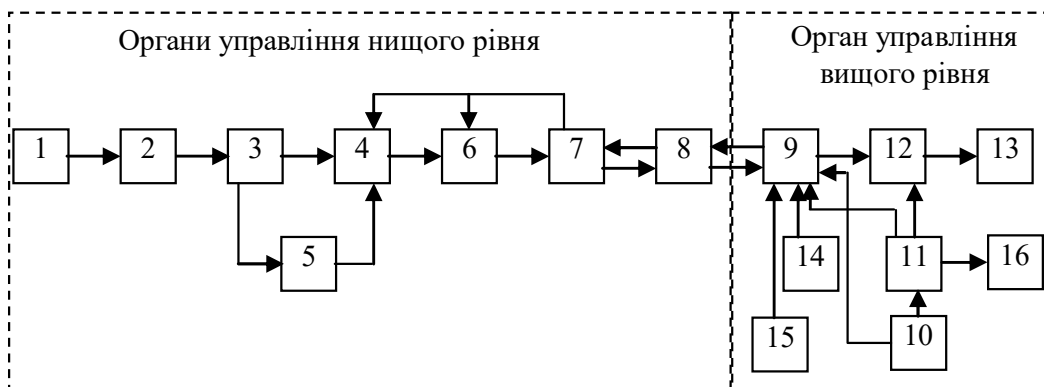


Рис. 2. Інформаційна мережа процесу розвідувально-інформаційної діяльності

Мережа складається з певної кількості ланок  $n_i, i=1, N$ . Кожну  $i$ -ту ланку можна розглядати як певний  $i$ -й стан, у якому послідовно перебуває кожне з інформаційних повідомлень, що утворюють потоки розвідувальних відомостей і даних. Виходячи із сутності процесу РІД ланками мережі, що зображена на рисунку 2, можуть бути:

1 – добування і формування потоків розвідувальних відомостей; 2 – збір, доведення розвідувальних відомостей до органів обробки; 3 – систематизація, вибірка розвідувальних відомостей; 4 – формування реалізацій розвідувальних ознак із добутих розвідувальних відомостей; 5 – визначення місцеположення об'єктів в просторі; 6 – викриття (розпізнавання) оперативно-тактичної приналежності об'єктів та їх станів, діяльності; 7 – оцінювання розвідувальних даних та прийняття рішення щодо їх представлення; 8 – доведення даних до споживачів; 9 – збір, систематизація, узагальнення розвідувальної інформації вищим органом обробки; 10 – оцінювання обстановки та отриманих розвідувальних даних вищим органом обробки; 11 – віддавання розпоряджень та націлювань вищим органом обробки; 12 – усвідомлення поставлених завдань, видача команд на добування; 13 – усвідомлення поставлених завдань, видача команд на ураження; 14, 15 – розвідувальна інформація, що отримана по лінії взаємодії; 16 – усвідомлення поставлених завдань, видача команд на подавлення.

Процес РІД є багатоцільовою слабоструктурованою інформаційною системою у функціонуванні якої виділяють детерміновані та ймовірнісні етапи. При виробленні рішень з управління інформаційними системами в умовах ризику виходять з наявності достовірної статистики за минулі періоди та аналізу тенденцій збереження в майбутньому деяких закономірностей зміни внутрішнього і зовнішнього середовища.

Цей підхід, що спирається з точки зору математики на ймовірнісний характер зовнішнього і внутрішнього середовища, дозволяє виробленню рішенням не вийти за допустимі межі точності управління, дозволяє підвищити об'єктивність управлінського рішення і отримати поточні та прогнози оцінки результату його виконання.

При виробленні рішень з управління інформаційною системою в умовах невизначеності інформаційна неповнота відчувається найбільш гостро, оскільки необхідні для прийняття рішення відомості і факти або відсутність або їх достовірність викликає обґрунтовані сумніви. У цьому випадку, коли вироблення і прийняття рішення не має об'єктивної інформаційної бази, часто стає неминучим залучення кваліфікованих експертів, судження яких дозволяють зменшити дефіцит знань і сформулювати рекомендації в недостатньо однозначній обстановці. Таким чином, як і в ситуації для умов ризику, реалізація

рішення по управлінню інформаційною системою може привести до різних результатів, але в умовах невизначеності їх ймовірності або невідомі, або не мають сенсу (коли ситуація не носить випадкового характеру) [8-10].

Важливою особливістю є базові умови при виробленні та прийнятті рішення (рис. 3) та причини виникнення невизначеності (рис. 4) при виробленні рішень з управління інформаційною системою, їх часто пов'язують з факторами некомпетентності посадових осіб з факторами протидії протиборчої сторони і з факторами випадковості, яка завжди має місце в ході функціонування складних інформаційних систем [8-10].

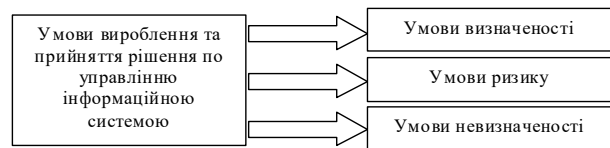


Рис. 3. Загальна класифікація вимог вироблення і прийняття рішення



Рис. 4. Базові причини невизначеності при виробленні і прийнятті рішення

Ступінь невизначеності інформації буває різною - від повного незнання і щодо майбутньої обстановки до припускового знання нижніх і верхніх меж, в рамках яких може варіюватися показник, що характеризує той чи інший аспект якості управління інформаційною системою. Розрізняють ступінь “глибини незнання”, величину поінформованості осіб і систем, що приймають управлінські рішення. Розрізняють ступені [8-10]:

повна поінформованість – їй відповідає близька до одиниці прогнозованість  $G_\tau$  подій

$$\lim_{\tau \rightarrow \tau_k} G_\tau = 1,$$

де  $\tau$  - час, а  $\tau_k$  - кінцевий час прогнозування події;

повна непоінформованість – їй відповідає близька до нуля прогнозованість настання події, що математично виражається співвідношенням

$$\lim_{\tau \rightarrow \tau_k} G_\tau = 0,$$

часткова невизначеність – відповідає подіям, прогнозованість яких лежить в межах від 0 до 1, що може бути виражено нерівністю

$$0 < G_\tau < 1;$$

невизначеність “безнадійна” – відповідає відсутності інформації про ймовірності стану середовища, в рамках якого функціонує інформаційна система.

У цих випадках для визначення найкращих рішень з управління інформаційною системою використовуються критерії гарантованого результату, оптимізму, песимізму, мінімаксного ризику і узагальненого максиміна [8-10].

Варіант загальної класифікації видів невизначеності, що впливає на вироблення рішень в рамках управління складними, багаторівневими системами збору, зберігання, обробки і передачі інформації запропонований на рис. 5.

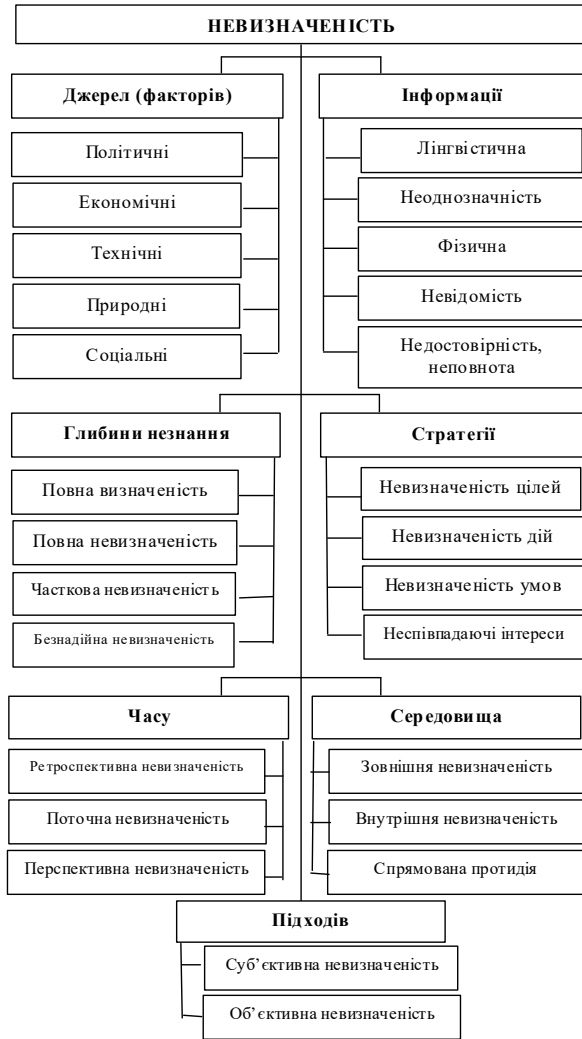


Рис. 5. Базові причини невизначеності при виробленні і прийнятті рішення

Умови невизначеності, що виникають при прийнятті рішень з управління інформаційними системами, об'єктивно обумовлені тим, що складні системи збору, зберігання, обробки і передачі інформації в процесі свого функціонування відчувають залежність від цілого ряду факторів.

Аналіз підходів до прийняття рішення [11] та видів невизначеності що мають місце при прийнятті рішення посадовими особами на організацію збору, зберігання, обробки і передачі інформації в інформаційних системах вказує на те що на сучасному етапі недостатньо розвинуті алгоритми прийняття рішення в умовах нестохастичної невизначеності, а саме,

неоднозначності (нечіткості) і недостатності (неповноти, протиріччя) вихідної інформації для прийняття рішення на управління системами подібного класу.

Що стосується математичних методів зниження невизначеності (з метою підвищення обґрунтованості і достовірності прийнятих рішень), то для прийняття рішень в умовах невідомості, заснованої на імовірнісному характері інформації, що використовується при прийнятті рішення, давно і успішно використовуються методи теорії ймовірностей та математичної статистики. Для нестохастичної невизначеності типу неоднозначності (нечіткості), апробовані і використовуються методи теорії множин, а для нестохастичної невизначеності типу недостовірності, недостатності (неповноти і протиріччя) вихідної інформації, знайшли своє успішне застосування методи теорії штучних нейронних мереж. Найбільш вірогідним і перспективним в подальшому, що поєднує в собі переваги перерахованих методів, що передбачають успіх не тільки обґрунтованості та достовірності, але і оперативності прийнятих рішень, бачиться шлях зниження невизначеності на базі розробки і застосування щодо нових і ефективних математичних методів, заснованих на моделях і алгоритмах теорії нечітких множин.

Відповідно до дослідження видів невизначеностей в інформаційних системах збору, обробки, передачі інформації, яка і є розвідувально-інформаційна діяльність, можливо здійснити математичний опис управління процесом РІД.

Управління РІД, як інформаційною системою є багатокритеріальна задача, розв'язання якої ускладнюється необхідністю врахування групових уподобань осіб, що приймають участь у процесі прийняття рішень. Якість розв'язання задачі підтримки прийняття рішення в процесі управління не може оцінюватись однією функцією і навіть декількома шкалами. Механізм раціонального вибору у таких випадках вимагає додаткової непрямої інформації, що дозволяє, принаймні, порівнювати альтернативи вибору стратегій управління. Формалізована постановка задачі управління системою РІД у математичній формі. Визначимо  $i$ -й функціонал

$$f_i(u_t) = \sum_{t=1}^{T_f} \{T(\mu_{G_i}(x_t), \mu_C(x_t, u_t))\} x_{t+1} = f(x_t, u_t)$$

де:  $T$  - трикутна норма, що є моделлю оператора кон'юнкції для нечітких змінних;  $\mu_{G_i}(x_t)$  - функція належності  $i$ -ї цілі ( $i = 1, \dots, I$ );  $\mu_C(x_t)$  - функція належності обмежень;  $T_f$  - термінальний крок (час змінюється дискретно від 1 до  $T_f$ ).

Постановкою завдання є знаходження такої оптимальної послідовності рішень  $\{u_1, \dots, u_{T_f}\}$ , при якій багатокритеріальні цілі досягають їх



оптимальних значень одночасно протягом ієрархічного процесу прийняття рішення:

$$\max_{u_t \in \Omega_t, t=1, \dots, T_f} \{ [f_1(u_t), \dots, f_I(u_t)] \} x_{t+1} = f(x_t, u_t),$$

$$\mu_{G_i}(u) = 0, \text{ якщо } f_i(u) \leq m_i;$$

$$\mu_{G_i}(u) = \frac{(f_i(u) - m_i)}{(M_i - m_i)}, \text{ якщо } m_i \leq f_i(u) \leq M_i;$$

$$\mu_{G_i}(u) = 1, \text{ якщо } f_i(u) \geq M_i;$$

де:  $f_i(u_t)$  - числове значення, до досягається  $i$ -ю ціллю при формуванні рішення  $u_t \in \Omega$  на кроці  $t$ ;

$\Omega$  - простір векторів рішень, що задовольняють співвідношення динаміки системи та обмеженням:

$$\Omega = \{u_t | x_{t+1} = f(x_t, u_t); g(x_t, u_t) \leq b\},$$

де:  $x_t \in R^N$  - вектор стану динамічної системи;

$u_t \in R^M$  - вектор рішень, відповідно;

$g \in R^K$  - вектор функцій обмежень;

$b \in R^K$  - вектор меж обмежень.

Прийняття рішень можливо, якщо є множина допустимих альтернатив рішень  $u^m \in \Omega$ . Альтернатива рішень  $u^1$  має перевагу перед альтернативою  $u^m$ , якщо  $f_i(u^1) > f_i(u^m)$ ,  $\forall i$ . Альтернатива  $u^1$  строго ефективна (оптимальна по Парето), якщо неможливо знайти таку альтернативу  $u^m (m \neq 1)$ , що  $f_i(u^m) \geq f_i(u^1) \forall i$  та  $f_j(u^m) > f_j(u^1)$  для хоча б одного  $i$ . Задача прийняття рішення  $u^*$  того, що  $f_i(u^*) > f_i(u^m) \forall u^*$  та  $\forall i$ , може бути розв'язана, якщо існує набір можливих «чітких» альтернатив і є модель переваг.

$$\mu_{C_k}(x_t, u_t) = 0, \text{ якщо } g_k(x_t, u_t) > b_k + p_k;$$

$$\mu_{C_k}(x_t, u_t) = \frac{[b_k + p_k - g_k(x_t, u_t)]}{p_k}, \text{ якщо}$$

$$b_k \leq g_k(x_t, u_t) \leq b_k + p_k;$$

$$\mu_{C_k}(x_t, u_t) = 1, \text{ якщо } g_k(x_t, u_t) < b_k;$$

Задача знаходження такої послідовності рішень  $\{u_1, \dots, u_T\}$ , що багатокритеріальні цілі досягають їх оптимальних значень при виконанні нечітких цілей  $G_i$  та нечітких обмежень  $C_k$ , може бути поставлена як задача знаходження максимуму функціонала:

$$\max_{u_t \in \Omega_t, t=1, \dots, T_f} \left\{ \sum_{t=1}^{T_f} T(\mu_{G_i}(x_t), \mu_{C_k}(x_t, u_t)) \right\},$$

при виконанні динамічних співвідношень переходу:  $x_{t+1} = f(x_t, u_t)$ .

Позначимо як  $\mu_{C_k}(x_t, u_t)$  - функцію належності виконання обмежень  $g_k(x_t, u_t)$ ,  $k = 1, \dots, K$ :

де  $b_k$  та  $p_k$  - величини «нечіткості» обмежень.

Обмеження можуть бути агреговані за допомогою трикутної  $T$ -норми:

$$\mu_C(x_t, u_t) = T\{\mu_{C_1}(x_t, u_t), \dots, \mu_{C_K}(x_t, u_t)\},$$

В подальшому будемо використовувати функцію мінімуму в якості  $T$ -норми:

$$\mu_C(x_t, u_t) = \min\{\mu_{C_1}(x_t, u_t), \dots, \mu_{C_K}(x_t, u_t)\}.$$

Визначимо функції належності  $\mu_{G_i}$  виконання  $i$ -ї цілі:

де максимальні вимоги виконання цілі  $M_i [\leq \max_{u \in \Omega} f_i(u)]$ ;

$$\text{мінімальні вимоги } M_i [\geq \min_{u \in \Omega} f_i(u)]$$

Якщо при прийнятті багатокритеріальних рішень зі взаємопов'язаними критеріями є цілі, що перебувають у протиріччі, то не існує оптимального рішення, що задовольняє усі критерії.

Нехай  $f_i, f_j$  - цільові функції. Будемо рахувати, що:

1)  $f_i$ , кооперується з  $f_j$  ( $f_i \uparrow f_j$ ), якщо з  $f_i(u') \geq f_i(u)$  виходить  $f_j(u') \geq f_j(u)$ ;  $\forall u', u \in \Omega$ ;

2)  $f_i$ , конфліктує з  $f_j$  ( $f_i \downarrow f_j$ ), якщо з  $f_i(u') \geq f_i(u)$  виходить  $f_j(u') \leq f_j(u)$ ;  $\forall u', u \in \Omega$ ;

3)  $f_i$ , та  $f_j$  незалежні

Нехай  $f_i$  - цільова функція; введемо ступінь залежності функції  $f_i$  від інших цільових функцій  $f_j (i \neq j)$ :

$$\Delta(f_i) = (w_i - k^{-1}) + (\sum_{f_i \uparrow f_j; i \neq j} w_j) - (\sum_{f_i \downarrow f_j} w_j);$$

$$i = 1, \dots, I.$$

Обчислимо  $\Delta(f_i)$  для  $i = 1, \dots, I$  і змінімо функції належності виконання цілей  $\mu_{G_i}$  в залежності від  $\Delta(f_i)$  наступним чином:

$$\mu_{G_i}(u, \Delta) = \mu_{G_i}(u)^{\exp(\alpha \Delta)}.$$

Значення критерію  $\max_{u \in \Omega} \{\mu_G(u)\}$  - максимізують сумісно усі цілі;  $\mu_{G_i}(u) \in [0, 1]$ ;  $i = 1, \dots, I$ ;  $\mu_G(u) = \min\{\mu_{G_1}(u), \dots, \mu_{G_I}(u)\}$ ; тому критерій  $\max_{u \in \Omega} \{\mu_G(u)\}$  можна рахувати агрегованим критерієм цілей  $G_1, \dots, G_I$ . Якщо відносна важливість задається набором вагових коефіцієнтів:  $w = (w_1, \dots, w_I)$ ;  $w_i > 0$ ;  $\sum_{i=1}^I w_i = 1$ , то для агрегування може використовуватись оператор Колмогорова:

$$\mu_{G_i}(u) = \varphi^{-1} \left( \Gamma^{-1} \sum_{i=1}^I \varphi(\mu_{G_i}(u)) \right),$$

$$\max_{u \in \Omega} \left\{ \varphi^{-1} \left( \Gamma^{-1} \sum_{i=1}^I \varphi(\mu_{G_i}(u)) \right) \right\},$$

де  $\varphi(\cdot)$  - гладка монотонна функція і  $\varphi(0)=0$ ;  $\varphi(1)=1$ . Тоді в якості критерію буде виступати значення

При формуванні рішення повинні виконуватись нечіткі цілі  $G$  і нечіткі обмеження  $C$ . Функція належності ступеня агрегованої цілі при формуванні рішення на кроці  $t$  може вимірюватись функцією належності  $\mu_D(x_t, u_t)$ :

$$\mu_D(x_t, u_t) = T\{\mu_G(x_t), \mu_C(x_t, u_t)\},$$

де  $\mu_C(x_t, u_t) = T\{\mu_{C_1}(x_t, u_t), \dots, \mu_{C_K}(x_t, u_t)\}$  - трикутна  $T$ -норма функції належності виконання обмежень на кроці  $t$ ;  $\mu_G(x_t)$  - агрегований критерій нечітких цілей на кроці  $t$ . Для множини рішень обирається такий вектор  $u_t^*$ , що має найбільший ступень виконання  $\mu_D(x_t, u_t)$ :

$$\mu_D(x_t, u_t^*) = \max_{u_t \in \Omega_t} \mu_D(x_t, u_t) = \max_{u_t \in \Omega} T\{\mu_G(x_t), \mu_C(x_t, u_t)\},$$

Пряме застосування методу нечіткого динамічного програмування для формування оптимальних рішень ускладнено наступними обставинами:

1) «прокляття розмірності» - необхідність значного об'єму адресного простору запам'ятовуючого пристрою (в залежності від кількості вузлів і розмірності вектору станів, кількості вузлів і розмірності вектору управління та необхідної кількості кроків); для розв'язання даної проблеми необхідно застосовувати ітераційні методи;

2) необхідна траєкторія вектору станів і вектору управління не співпадають з передбаченими вузлами вектору станів і вектору управління; для розв'язання даної проблеми необхідно застосовувати методи апроксимації між вузлами;

3) для виконання початкових умов, що накладаються на вектор стану  $x_1$ , необхідно щоб вектори станів  $x_t$  задовольняли динамічним співвідношенням переходу:

$$x_{t+1} = f(u_t, x_t); \quad t = 1, \dots, T-1,$$

з необхідним початковим вектором стану  $x_1$

Сформулюємо ієрархічний метод рішення багатокритеріальної задачі у вигляді співвідношення:

$$\max_{u_t \in \Omega_t, t=1, \dots, T} \{ \rho_D(u_{(1)}) \mid x_{t+1} = f(x_t, u_t) \},$$

де  $\rho_D(u_{(1)}) = \sum_{t=1}^T \mu_D(x_t, u_t)$ ;  $u_{(1)} = \{u_1, u_2, \dots, u_T\}$ ;

$\mu_D(x_t, u_t)$  - визначається з функції належності виконання цілей  $\mu_{G_i}$ .

Визначимо величину  $\Phi_t(u_t, x_t)$  на кроці  $t$  співвідношенням:

$$\Phi_t(u_t, x_t) = \{ \rho_D^{(t)}(u) \mid x_{t+1} = f(x_t, u_t); \tau \geq t \},$$

та оптимальну величину  $\Phi_t^*(u_t, x_t)$

$$\Phi_t^*(u_t, x_t) = \max_{u_t \in \Omega_t, t=1, \dots, T} \{ \rho_D^{(t)}(u) \mid x_{t+1} = f(x_t, u_t); \tau \geq t \},$$

де  $\rho_D^{(t)}(u_{(t)}) = \sum_{\tau=t}^T \mu_D(x_\tau, u_\tau)$ ;  $u_{(t)} = \{u_t, u_{t+1}, \dots, u_T\}$ .

Тоді принцип звичайного динамічного програмування у випадку нечіткої постановки перетворюється у рекурентне співвідношення:

$$\Phi_t^*(u_t, x_t) = \max_{u_t \in \Omega_t, t=1, \dots, T} \{ \rho_D^{(t)}(u_{(t)}) + \Phi_{t+1}^*(u_{t+1}, x_{t+1}) \};$$

$$t = T, T-1, \dots, 1.$$

де  $u_t$  - рішення на кроці  $t$ ; оптимальна послідовність векторів рішень

$$u_{(t)}^* = \{u_t^*, u_{t+1}^*, \dots, u_T^*\},$$

при яких виконується умова рекурентного співвідношення, повинна визначатися для всіх вузлів  $x_t$ . Після отримання оптимальної

послідовності рішень  $u_{(t)}^*$  може бути визначена послідовність векторів станів, що задовольняють динамічні співвідношення:

$$x_{t+1} = f[u_t^*(x_t), x_t]; \quad t = 1, \dots, T-1$$

та початковій умові  $x_1$ .

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

Проведена класифікація невизначеностей, що впливають на прийняття рішення при управлінні розвідувально-інформаційною діяльністю, інформаційною системою збору, обробки, передачі інформації. З врахуванням цього розроблено математичну модель процесу управління системою розвідувально-інформаційної діяльності, що являє собою сукупність математичних співвідношень, що відображають ієрархічний процес знаходження оптимальної послідовності рішень. Для практичної реалізації процесу прийняття рішення запропоновано застосовувати принципи нечіткого ітеративного динамічного програмування.

Найбільш вірогідним і перспективним в подальшому, для підвищення обґрунтованості, достовірності і оперативності прийнятих рішень, для зниження невизначеності застосування нових і ефективних математичних методів, заснованих на моделях і алгоритмах теорії нейрон-нечітких мереж.

*Література*

- 1. Method** of integral estimation of channel state in the multiantenna radio communication systems S. Kalantaievska, H. Pievtsov, A. Kuvshynov, S. Hatsenko, A. Shyshatskyi, S. Yarosh, S. Zubrytskyi, R. Zhyvotovskiy, S. Petruk, V. Zulko Eastern-european journal of enterprise technologies. Vol. 5, No 9 (95) pp. 60-76, 2018: Information and controlling system. **2. Development** of methodology for complex processing of geopatronic data in the geoinformation system of special purpose in conditions of diversity and nenophynedy A. Koshlan, O. Salnikova, M. Chekhovska, R. Zhyvotovskiy, Ye. Prokopenko, T. Hurskyi, A. Yefymenko, Ye. Kalashnikov, S. Petruk, A. Shyshatskyi Eastern-european journal of enterprise technologies. Vol. 5, No 9 (95) pp. 35-45, 2019: Information and controlling system.. **3. Method** of Immunity Minimization of the Free Platform ed Inertial Navigation System of Unmanned Aircrafts R. Bieliakov, S. Hatsenko, O. Fesenko, R. Zhyvotovskiy, S. Petruk, 2nd Ukraine Conference on Electrical and Computer Engineering Lviv, Ukraine, July 2-6, pp. 803-808, 2019. **4. Застосування** інформаційних систем для аналізу радіоелектронної обстановки Ю. І. Радковець, В. А. Шуренок, Р. В. Дзюбчук, М. А. Роговец, ВВР № 17, 2008 р, С. 47-56. **5. Пермяков О. Ю.** Теоретические основы обработки нечетких данных в аналитических задачах специального математического обеспечения: Дисс. на соис. уч. степени д. т. н. К.: 1995. 198 с. **6. Гаценко С. С.** Зуйко В. В., Зотов С. В. Методика вироблення та надання рекомендацій в умовах невизначеності та суперечливості розвідувальної інформації: Збірник наукових праць ЦНДІ ОБТ ЗСУ. 2016. № 3 (62). С. 12–23. **7. Військовий** стандарт 01.101.004, реєстраційний номер А2187/000033, с. 24. **8. Анфилатов, В. С.** Теоретические Основы автоматизации управления войсками и связью. Часть 1. (Системные основы автоматизации управления войсками и связью: Учебн. пособие / В.С. Анфилатов. СПб.: ВАС. 2014. 312с. **9. Москвин Б. В.** Теория принятия решений: учебник / Б.В. Москвин. СПб.: ВКА им. Л.Ф. Можайского, 2014. 364 с. **10. Военная** системотехника и системный анализ. Модели и методы подготовки и принятия решений в сложных организационно-технических комплексах в условиях неопределенности и многокритериальности / Под ред. Б.В. Соколова. - СПб.: ВИКУ им. А.Ф. Можайского, 1999. - 496 с. **11. Гаценко С. С.** Інформаційна система оцінювання оперативної обстановки в умовах невизначеності: К.: НУОУ, 2017. № 1 (140), С. 157–165.

**МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЦЕССА РАЗВЕДЫВАТЕЛЬНО-ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ**

*Сергей Станиславович Гаценко (кандидат технических наук)*

*Александр Николаевич Лищенко*

*Андрей Иванович Сотниченко*

*Ярослав Анатолиевич Жарков*

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

*Одним из основных технических видов военной разведки Украины, который постоянно осуществляется (ведется) в мирное время, особый период, в интересах национальной безопасности и обороны государства и выполнения задач в операциях (боевых действиях) является радиоэлектронная разведка.*

*Радиоэлектронная разведка добывает разведывательную информацию путем вскрытия функционирования радиоэлектронных средств и систем применяемых для управления войсками (силами) и оружием, а также осуществляет сбор, обработку, анализ и доведение добытой разведывательной информации определенным потребителям в установленные сроки.*

*Для непрерывного и своевременного обеспечения потребителей определенной информацией, информационными (информационно-аналитическими) органами осуществляется комплекс мероприятий разведывательно-информационной деятельности, разведывательно-информационной работы.*

*В условиях динамичности, многогранности процессов обработки, анализа, хранения больших объемов информации ключевым остается задача уменьшения неопределенности информации вызванной факторами эволюционного развития, факторами применения сложных информационных систем в различных условиях сложной радиоэлектронной и оперативной обстановки.*

***Ключевые слова:** радиоэлектронная разведка; разведывательно-информационная деятельность; разведывательно-информационная работа; неопределенность информации.*

**MATHEMATICAL MODEL OF THE RESEARCH AND INFORMATION ACTIVITY PROCESS IN UNCERTAINTY**

*Serhii Hatsenko (Candidate of technical sciences)*

*Oleksandr Lishchenko*

*Andrii Sotnichenko*

*Yaroslav Zharkov*

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

*One of the main technical types of military intelligence of Ukraine, which is constantly carried out (conducted) in peacetime, a special period, in the interests of national security and defense of the state and the fulfillment of tasks in operations (military operations) is electronic intelligence.*

*Electronic intelligence extracts intelligence information by opening up the operation of electronic equipment and systems used to control troops (forces) and weapons, and also collects, processes, analyzes, and brings the intelligence obtained to specific consumers on time.*

*For the continuous and timely provision of consumers with certain information, information (information and analytical) bodies, a set of measures is undertaken for intelligence and information activities, intelligence and information work.*

*In the conditions of dynamism, versatility of the processes of processing, analysis, storage of large volumes of information, the key task remains to reduce the uncertainty of information caused by factors of evolutionary development, factors of the use of complex information systems in various conditions of a complex electronic and operational environment.*

**Key words:** *electronic intelligence, intelligence and information activity, intelligence and information work, information uncertainty.*

### **References**

- 1. Method** of integral estimation of channel state in the multiantenna radio communication systems S. Kalantaievska, H. Pievtsov, A. Kuvshynov, S. Hatsenko, A. Shyshatskyi, S. Yarosh, S. Zubrytskyi, R. Zhyvotovskiy, S. Petruk, V. Zulko Eastern-european journal of enterprise technologies. Vol. 5, No 9 (95) pp. 60-76, 2018: Information and controlling system. **2. Development** of methodology for complex processing of geopatronic data in the geoinformation system of special purpose in conditions of diversity and nenophynedy A. Koshlan, O. Salnikova, M. Chekhovska, R. Zhyvotovskiy, Ye. Prokopenko, T. Hurskyi, A. Yefymenko, Ye. Kalashnikov, S. Petruk, A. Shyshatskyi Eastern-european journal of enterprise technologies. Vol. 5, No 9 (95) pp. 35-45, 2019: Information and controlling system.. **3. Method** of Immunity Minimization of the Free Platform ed Inertial Navigation System of Unmanned Aircrafts R. Bieliakov, S. Hatsenko, O. Fesenko, R. Zhyvotovskiy, S. Petruk, 2nd Ukraine Conference on Electrical and Computer Engineering Lviv, Ukraine, July 2-6, rr. 803-808, 2019. **4. Zastosuvannya** InformatsIynih sistem dlya anallzu radIoelektronnoYi obstanovki Yu. I. Radkovets, V. A. Shurenok, R. V. Dzyubchuk, M. A. Rogovets, VVR # 17, 2008 r, S. 47-56. **5. Permyakov** O. Yu. Teoreticheskie osnovyi obrabotki nechetkih danyih v analiticheskikh zadachah spetsialnogo matematicheskogo obespecheniya: Diss. na sois. uch. stepeni d. t. n. K.: 1995. 198 s. **6. Gatsenko S. S.** Zuyko V. V., Zotov S. V. Metodika viroblennya ta nadannya rekomendatsIy v umovah neviznachenostiI ta superechlivostiI rozvIduvalnoYi InformatsIYi: Zblrnik naukovih prats TsNDI OVT ZSU. 2016. # 3 (62). S. 12–23. **7. VIyskoviy** standart 01.101.004, reEstratsIyniy nomer A2187/000033, s. 24. **8. Anfilatov, V. S.** Teoroticheskie Osnovyi avtomatizatsii upravleniya voyskami i svyazyu. Chast 1. (.Sistemnyie osnovyi avtomatizatsii upravleniya voyskami i svyazyu: Uchebn. posobie / V.S. Anfilatov. SPB.: VAS. 2014. 312s. **9. Moskvina B. V.** Teoriya prinyatiya resheniy: uchebnik / B.B. Moskvina. SPB.: VKA im. L.F. Mozhayskogo, 2014. 364 s. **10. Voennaya** sistemotekhnika i sistemnyiy analiz. Modeli i metodyi podgotovki i prinyatiya resheniy v slozhnyih organizatsionno-tehnicheskikh kompleksah v usloviyah neopredelennosti i mnogokriterialnosti / Pod red. B.V. Sokolova. - SPb.: VIKU im. A.F. Mozhayskogo, 1999. - 496 s. **11. Gatsenko S. S.** InformatsIyna sistema otsInyuvannya operativnoYi obstanovki v umovah neviznachenostiI: K.: NUOU, 2017. # 1 (140), S. 157–165.

*Віталій Володимирович Зуйко (кандидат військових наук, доцент)*

*Сергій Анатолійович Мельник*

*Іван Миколайович Лук'янчиков*

*Олексій Васильович Повещенко*

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

## МЕТОДИКА ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ ДОКУМЕНТІВ В ІНТЕРЕСАХ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

В статті пропонується вирішення актуального наукового завдання удосконалення науково-методичного апарату оцінювання інформаційних документів при проведенні розвідувально-інформаційної діяльності в системі воєнної розвідки. Розвідувально-інформаційна діяльність – це безперервний процес, який включає комплекс заходів з організації і ведення в загальній системі воєнної розвідки розвідувально-інформаційної, інформаційної та інформаційно-аналітичної роботи для надання розвідувальної інформації її споживачам. Зібрати у визначені терміни, оперативно обробити, проаналізувати та вчасно доповісти це є головним і вирішальним завданням розвідувально-інформаційної діяльності в інтересах забезпечення прийняття рішення. Особливістю сучасної розвідувально-інформаційної діяльності є вирішення широкого кола інтелектуальних за змістом завдань, результатами яких є розробка інформаційних документів. Оцінка якості їхнього виконання є складовою частиною оцінювання інформаційно-аналітичної діяльності в цілому.

Для вирішення завдання ефективної інформаційно-аналітичної діяльності запропоновано методику оцінювання інформаційно-звітних документів. Методика оснований на методі аналізу ієрархій, якій дозволяє прийняти рішення на основі неформалізованих показників, які неможливо описати аналітичними залежностями. Запропонована методика дозволить підвищити якість оцінювання інформаційних документів.

**Ключові слова:** розвідувально-інформаційна діяльність; воєнна розвідка; інформаційні документи; розвідувальна інформація.

### Вступ

**Постановка проблеми.** Останнім часом розвідка стає дедалі важливішою складовою функціонування Збройних Сил України та держави в цілому. Значення і сила розвідки полягає в інформації, що добувається, в її своєчасній і якісній обробці та в оперативному доведенні її до органів управління, що визначені законодавством України [1]. Тому організація та ведення ефективної інформаційно-аналітичної діяльності (ІАД) воєнною розвідкою, що передбачає етапи збору, обліку та систематизації, аналізу, оцінки, узагальнення та синтезу даних на основі інформаційних технологій у всіх сферах розвідувальної діяльності, займає провідне місце у процесі забезпечення функціонування усіх органів державної влади. Результатом ІАД є розробка інформаційних та інформаційно-аналітичних документів, а оцінювання якості їхнього виконання є складовою частиною заключного етапу процесу організації інформаційно-аналітичної діяльності.

**Аналіз останніх досліджень і публікацій.** Аналіз існуючих методик і підходів оцінки показує, що вони в цілому дозволяють проводити комплексне оцінювання якості виконання документів. Однак їм притаманні суттєві недоліки,

а саме:

не враховані вимоги [2], що стосується визначення самого поняття “розвідувальна інформація”; не визначена загальна послідовність (алгоритм) проведення оцінювання якості виконання документів; потребують уточнення показники та критерії, за якими здійснюється оцінювання інформаційних документів (ІД); не використовуються кількісно-якісні підходи до визначення якості виконання документів.

**Мета статті.** Виходячи з цього метою статті є удосконалення методики оцінювання якості виконання інформаційних документів, в інтересах розвідувально-інформаційної діяльності (РІД) в системі воєнної розвідки.

### Виклад основного матеріалу дослідження

Оцінка якості виконання ІД являє собою визначення ступеню виконання вимог, які до них висуваються керівними документами. Під ступенем виконання цих вимог будемо розуміти відповідність значень показників поточного документу значенням показників “ідеального документу”.

Проведення такого порівняння передбачає прийняття рішення на основі неформалізованих показників, які неможливо описати аналітичними

залежностями. Одним із найбільш ефективних методів вирішення завдань наведеного класу є метод аналізу ієрархій (МАІ) [3-6]. При цьому, використання МАІ для таких цілей обумовлює наступні припущення та обмеження:

обрані показники якості виконання ІД є незалежними один від одного та в повній мірі відображають вимоги, які висуваються до документів;

ступінь впливу того чи іншого показника на якість виконання документу в цілому визначається шляхом проведення парних порівнянь відносно головної мети проведення такого оцінювання;

парні порівняння показників здійснюються за допомогою шкали порівнянь, яка має 9 градаций;

отримані під час парних порівнянь числові переваги є детермінованими, а не ймовірнісними величинами;

пріоритети показників якості виконання документів встановлюються шляхом проведення експертного опитування;

перевірка узгодженості думок експертів здійснюється за процедурою, яку передбачає МАІ;

одночасно може проводитись оцінювання якості виконання тільки одного ІД.

Оцінювання якості виконання ІД пропонується здійснювати в кілька етапів (рисунок 1).

На **першому етапі** здійснюється вивчення документу та проводиться перевірка відповідності інформації, яка в ньому міститься, вимогам [2].

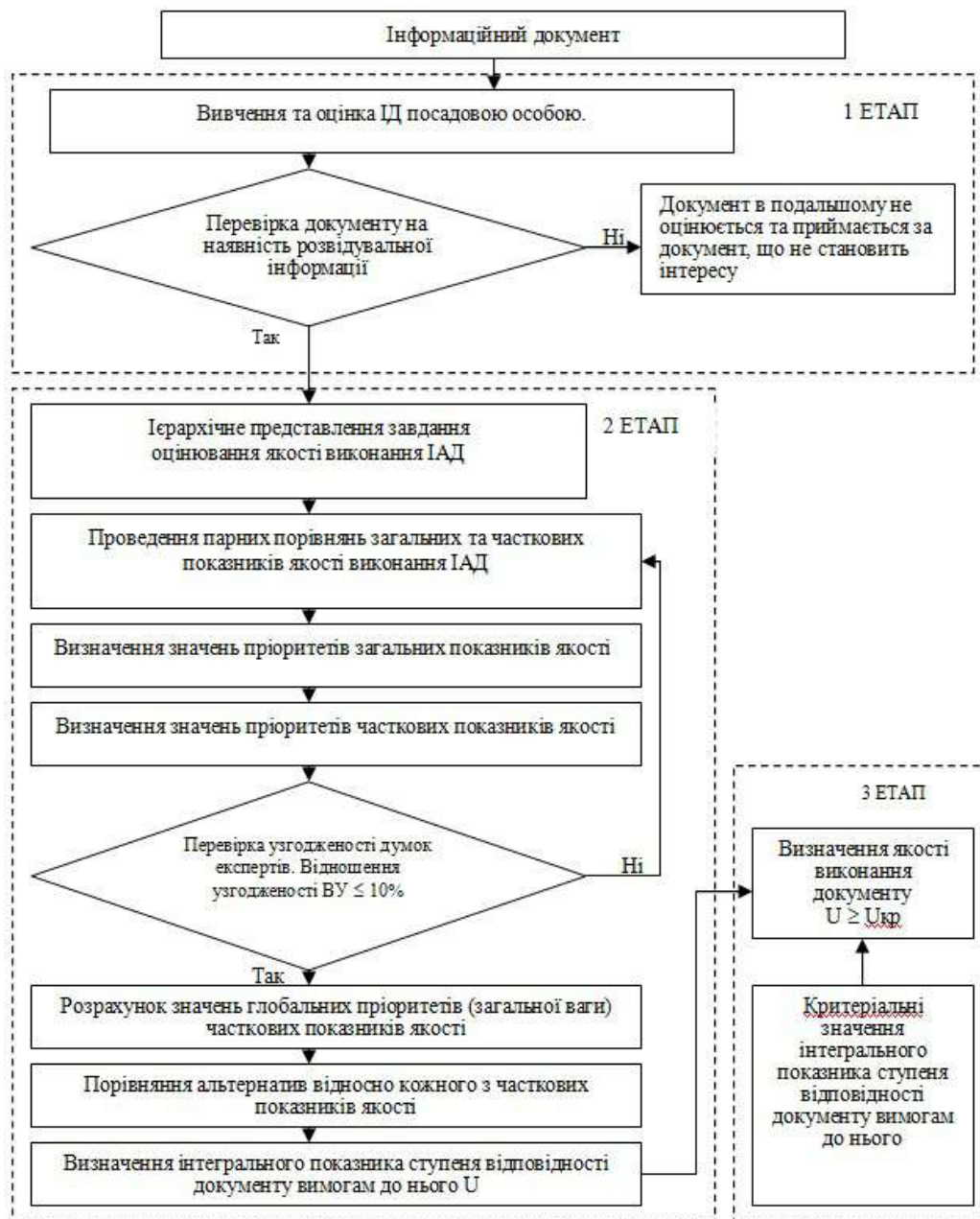


Рис. 1. Алгоритм оцінювання якості виконання інформаційних документів

**Другий етап.** За умов наявності в документі розвідувальну, здійснюється визначення інформації, яку можна класифікувати як інтегрального показника ступеня відповідності

документу  $U$  вимогам до нього за допомогою виразів:

$$U = \frac{P_{\Pi}}{P_1} 100\%, \quad (1)$$

$$P_{\Pi(i)} = \sum_{i=1}^n \alpha_i V_{\Pi(i)i}, \quad (2)$$

де  $P_{\Pi}$ ,  $P_1$  – коефіцієнти відносної ваги поточного та “ідеального” документів відповідно, які отримані шляхом порівняння альтернатив відносно кожного з часткових показників якості виконання документів;  $\alpha_i$  – глобальний пріоритет  $i$ -го показника якості виконання документу;  $V_{\Pi(i)i}$  – відносні пріоритети поточного (“ідеального”) документу, які отримані шляхом їхнього парного порівняння відносно ступеня відповідності критеріальним значенням  $i$ -го часткового показника якості виконання документів.

Використання МАІ для визначення показника  $U$  передбачає необхідність ієрархічного зображення завдання з оцінювання якості виконання документів. Таке ієрархічне зображення наведено на рисунку 2 [5].

Виходячи з рисунку 2 та визначених в [5, 7, 8] загальних та часткових показників, відповідно до МАІ проводяться їх парні порівняння і визначаються значення пріоритетів (вага) цих показників. Здійснюється перевірка думок експертів та розраховуються значення глобальних пріоритетів часткових показників якості виконання документів.

Глобальний пріоритет  $i$ -го показника якості виконання документу визначається за формулою

$$\alpha_i = \beta_j \gamma_i, \quad (3)$$

де  $\beta_j$  – пріоритет  $j$ -го загального показника відносно його впливу на загальну мету;

$\gamma_i$  – пріоритет  $i$ -го часткового показника відносно свого загального показника.

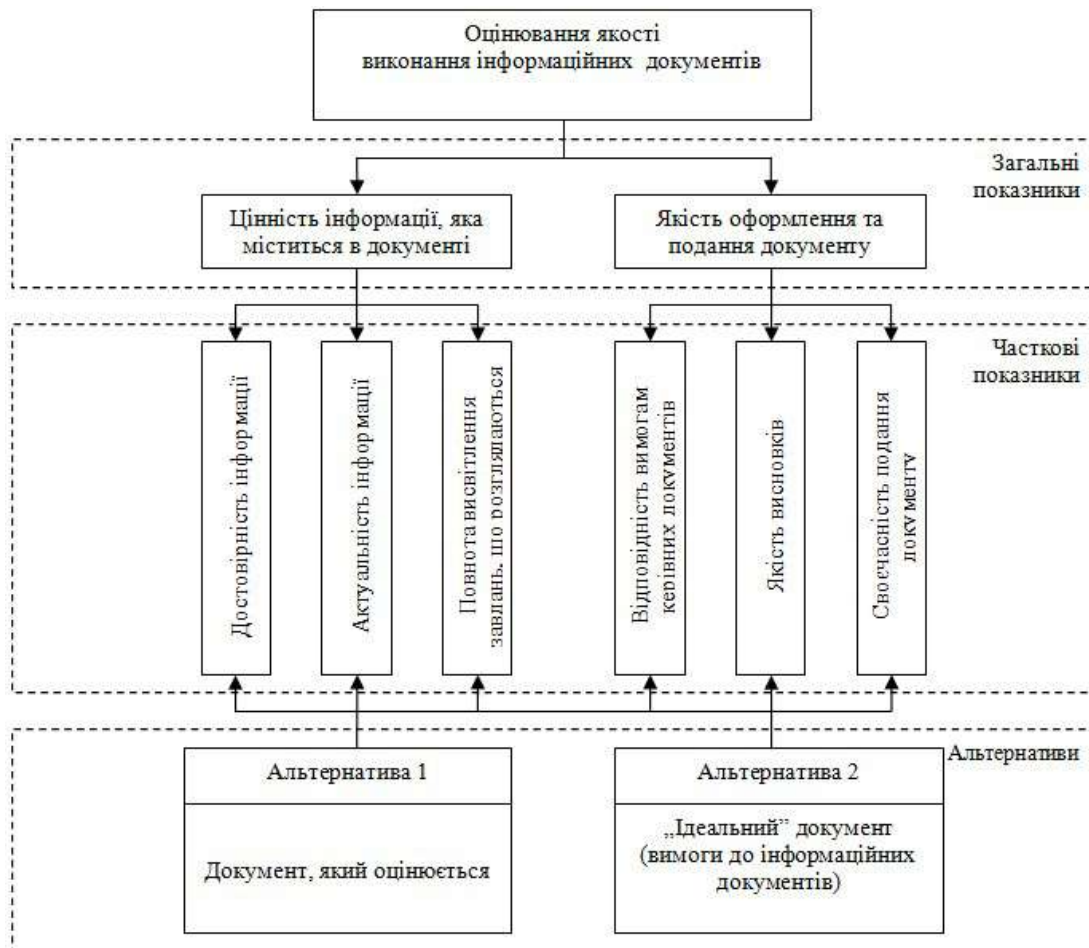


Рис. 2. Ієрархічне зображення завдання з оцінювання якості виконання інформаційних документів

Визначення значень  $\beta_j$  і  $\gamma_i$  здійснюється шляхом складання відповідних матриць парних порівнянь за допомогою шкали парних порівнянь.

Клітини матриці заповнюються експертами виходячи з таких міркувань (таблиця 1). Якщо

показник  $A_1$  домінує над показником  $A_2$ , то клітка, яка відноситься до рядка  $A_1$  і стовпця  $A_2$ , заповнюється числом  $a_{12}$ , а клітка, яка відповідає рядку  $A_2$  і стовпцю  $A_1$ , заповнюється оберненим числом, тобто  $a_{21} = 1/a_{12}$ . Якщо елементи, що

порівнюються однакові, то у клітці на перетині одиниця [6-9]:  
відповідних строки та стовпця ставиться

Таблиця 1

Матриця оцінок експертів якості виконання документу

Загальні (часткові) показники якості виконання документу	Загальний (частковий) показник $A_1$	Загальний (частковий) показник $A_2$	...	Загальний (частковий) показник $A_j$
Загальний (частковий) показник $A_1$	$a_{111}$	$a_{121}$	...	$a_{1j1}$
Загальний (частковий) показник $A_2$	$a_{211}$	$a_{221}$	...	$a_{2j1}$
.	.	.	...	.
.	.	.	...	.
.	.	.	...	.
Загальний (частковий) показник $A_i$	$a_{i11}$	$a_{i21}$	...	$a_{ij1}$

З групи одержаних матриць парних порівнянь формується набір локальних пріоритетів, які виражають відносний вплив множини елементів на елемент рівня, що примикає зверху. Для цього обчислюються власні вектори для кожної матриці парних порівнянь і результат нормується. Визначення локальних пріоритетів здійснюється у такій послідовності: для кожного рядка  $l$ -ї матриці визначається геометричне середнє:

$$b_{il} = \sqrt[n]{\prod_j a_{ijl}}, \quad j = \overline{1, n}, \quad i = \overline{1, n}, \quad (4)$$

Потім здійснюється нормування геометричних середніх, тобто розраховуються значення пріоритетів (ваги) показників якості (загальних, часткових):

$$\beta(\gamma) = \frac{b_{ij}}{\sum_i b_{ij}}, \quad i = \overline{1, n}, \quad (5)$$

Авторами були проведені дослідження, які дозволили шляхом проведення експертного опитування та застосуванні процедури МАІ для обробки суджень експертів, визначити значення пріоритетів (ваги) загальних та часткових показників оцінки якості виконання документів. Відношення узгодженості думок експертів під час опитування склало менше 10 %, що відповідає вимогам [5, 9-11]. Значення пріоритетів (ваги) загальних та часткових показників (рисунок 2) складають відповідно:

- для загального показника цінності інформації, яку містить документ,  $\beta_1 = 0,75$ ;
- для загального показника якості оформлення та подання документу  $\beta_{II} = 0,25$ ;
- для часткового показника достовірності інформації  $\gamma_D = 0,54$ ;
- для часткового показника актуальності інформації  $\gamma_A = 0,3$ ;
- для часткового показника повноти інформації  $\gamma_{II} = 0,16$ ;
- для часткового показника відповідності вимогам керівним документам  $\gamma_K = 0,12$ ;

для часткового показника якості висновків  $\gamma_B = 0,44$ ;

для часткового своєчасності подання документу  $\gamma_C = 0,44$ .

З врахуванням отриманих показників глобальні пріоритети кожного часткового показника якості виконання документів будуть дорівнювати:

для часткового показника достовірності інформації  $\alpha_D = \beta_I \times \gamma_D = 0,405$ ;

для часткового показника актуальності інформації  $\alpha_A = \beta_I \times \gamma_A = 0,225$ ;

для часткового показника повноти інформації  $\alpha_{II} = \beta_{II} \times \gamma_{II} = 0,12$ ;

для часткового показника відповідності вимогам керівним документам  $\alpha_K = \beta_{II} \times \gamma_K = 0,027$ ;

для часткового показника якості висновків  $\alpha_B = \beta_{II} \times \gamma_B = 0,11$ ;

для часткового показника своєчасності подання документу  $\alpha_C = \beta_{II} \times \gamma_C = 0,11$ .

В подальшому значення розрахованих глобальних пріоритетів  $\alpha_i$  часткових показників в методиці використовуються як константи.

Після визначення глобальних пріоритетів  $\alpha_i$  здійснюється порівняння альтернатив (поточного та

“ідеального” документів) відносно кожного з часткових показників якості та визначаються їхні відносні пріоритети  $B_{II(i)}$ :

$$B_{II} = \frac{\sqrt{1/b_i}}{\sqrt{b_i} + \sqrt{1/b_i}}, \quad (6)$$

$$B_I = \frac{\sqrt{b_i}}{\sqrt{b_i} + \sqrt{1/b_i}}, \quad (7)$$

де  $b_i$  – ступінь важливості при порівнянні за шкалою парних порівнянь [6].

Для визначення  $B_{II(i)}$  проводиться порівняння за шкалою [5] альтернатив з метою встановлення



ступеню відповідності поточного документу парних порівнянь за кожним частковим вимогам, які висуваються до документів за  $i$ -м показником (таблиця 2):  
показником якості. Для цього формуються матриці

Таблиця 2

Матриця парних порівнянь за кожним частковим показником

Альтернативи	Поточний документ	„Ідеальний” документ
Поточний документ	1	$1/b_i$
“Ідеальний” документ	$b_i$	1

Далі за формулами (1), (2) здійснюється порівняння отриманого значення інтегрального розрахунок інтегрального показника ступеня показника  $U$  з його критеріальними значеннями відповідності документу вимогам до нього. (таблиця 3) та визначається якість виконання

**Третій етап** методики. Проводиться документу, що розглядається.

Таблиця 3

Критеріальні значення інтегрального показника ступеня відповідності документу вимогам до нього

Ступінь якості виконання документу	Значення $U$	Зміст критерію	
		щодо цінності інформації, яка міститься в документі	щодо якості оформлення та подання документу
Документ особливої важливості	$U \geq 86,5\%$	PI, яка міститься в документі, достовірна, упереджувальна та повна.	Документ поданий вчасно, повністю відповідає вимогам керівних документів, висновки повні.
Документ оцінюється як цінний	$86,5\% > U \geq 65,5\%$	PI, яка міститься в документі, достовірна, повна, а її актуальність висока.	Документ поданий вчасно, повністю відповідає вимогам керівних документів якість висновків достатня.
Документ середньої цінності	$65,5\% > U \geq 39,7\%$	PI, яка міститься в документі за своєю достовірністю не нижче за вірогідну, достатньо повна, її актуальність достатня.	Документ поданий вчасно, відповідність вимогам керівних документів достатня, висновки середньої якості.
Документ становить інтерес	$39,7\% > U \geq 29,6\%$	PI, яка міститься в документі, за достовірністю не нижче за можливо правдиву, частково повна, її актуальність достатня.	Документ поданий вчасно, відповідність вимогам керівних документів посередня, висновки низької якості.
Документ малої цінності	$29,6\% > U \geq 19,5\%$	PI, яка міститься в документі, за достовірністю сумнівна, низької актуальності та повноти.	Документ поданий вчасно, відповідність вимогам керівних документів низька, висновки незадовільної якості.
Документ не становить інтересу	$U < 19,5\%$	PI, яка міститься в документі, не несе змістовного навантаження, неактуальна, а її достовірність неможливо визначити. Або документ не містить в собі PI.	Документ поданий невчасно, відповідність вимогам керівних документів та висновки незадовільні.

Розглянемо практичний приклад оцінювання якості виконання інформаційних документів за допомогою вище запропонованої методики.

Відповідно до ієрархії оцінювання якості виконання ІД (рисунок 2) здійснюємо порівняння поданого документу з документом, який повністю відповідає вимогам, тобто з “ідеальним документом”. Порівняння здійснюються окремо по відношенню до критеріальних значень кожного часткового показника якості за допомогою шкали порівнянь [5]. При цьому відповідно до [5]

найвищому критеріальному значенню виставляється 1, а найнижчому – 1/9.

Припустимо, що поточний документ оцінений: за достовірністю поданої інформації – середнє між “достовірна” та “вірогідна” (1/2); за актуальністю поданої інформації – “висока актуальність” (1/3); за повнотою інформації – середнє між “достатньо повна” та “часткова” (1/4); за відповідністю вимогам керівних документів – “висока” (1); за якістю висновків – середнє між “середньої

якості” та “низької якості” (1/6); результати порівняння поточного та “ідеального” за своєчасністю подання документу – документів за частковими показниками можна “вчасно” (1). представити у вигляді таблиці 4.  
Тому, згідно з розробленою методикою

Таблиця 4

Результати порівняння поточного та „ідеального” документів за кожним з часткових показників якості

Альтернативи (документи, що порівнюються)	“Ідеальний” документ	Поточний документ
<b>За ступенем достовірності поданої інформації</b>		
“Ідеальний” документ	1	2
Поточний документ	1/2	1
<b>За ступенем актуальності поданої інформації</b>		
“Ідеальний” документ	1	3
Поточний документ	1/3	1
<b>За ступенем повноти поданої інформації</b>		
“Ідеальний” документ	1	4
Поточний документ	1/4	1
<b>За ступенем відповідності вимогам керівним документам</b>		
“Ідеальний” документ	1	1
Поточний документ	1	1
<b>За ступенем якості висновків</b>		
“Ідеальний” документ	1	6
Поточний документ	1/6	1
<b>За своєчасністю подання документу</b>		
“Ідеальний” документ	1	1
Поточний документ	1	1

За результатами парних порівнянь (таблиця 4) визначаються відносні пріоритети поданого  $V_{Pi}$  та “ідеального”  $V_i$  документів за кожним  $i$ -м частковим показником якості:

за показником достовірності інформації

$$V_{iD} = 0,67, V_{PiD} = 0,33;$$

за показником актуальності інформації

$$V_{iA} = 0,75, V_{PiA} = 0,25;$$

за показником повноти інформації

$$V_{iP} = 0,8, V_{PiP} = 0,2;$$

за показником відповідності вимогам керівним документам

$$V_{iK} = 0,5, V_{PiK} = 0,5;$$

за показником якості висновків

$$V_{iB} = 0,86, V_{PiB} = 0,14;$$

за своєчасністю подання документу

$$V_{iC} = 0,5, V_{PiC} = 0,5.$$

Далі відповідно до формули (2) розраховуються коефіцієнти відносної ваги “ідеального” та поточного (поданого) документу:

$$P_I = 0,644; P_{Pi} = 0,298.$$

За формулою (1) розраховується значення інтегрального показника ступеня відповідності поданого (поточного) документу вимогам до інформаційних документів

$$U = \frac{P_{Pi}}{P_I} = 46\%.$$

За значенням інтегрального показника  $U$  відповідно до таблиці 3 визначається оцінка якості виконання поданого на розгляд інформаційного

документу. В даному випадку ( $U = 46\%$ ) поданий документ оцінюється як документ середньої цінності.

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

Аналіз наведених результатів дозволяє зробити висновок, що переваги запропонованої методики оцінювання якості виконання інформаційних документів полягають у наступному:

відсутність необхідності пошуку функціональної залежності якості виконання документу від показників;

використання парних порівнянь часткових критеріїв за шкалою відношень дозволяє не проводити нормування метричних критеріїв та зменшує помилку під час перетворення якісних характеристик в числові;

можливість отримання додаткової інформації за рахунок ієрархічного представлення елементів структури завдання та чіткий вираз суджень;

можливість зміни кількості показників, які використовуються для оцінювання якості виконання документів, без зміни структури моделі оцінки;

об'єднання часткових показників якості виконання документів в групи показників та проведення оцінювання за однією групою показників без врахування інших груп;

за умов визначення значень пріоритетів загальних та часткових показників якості виконання інформаційних документів за судженням 10-15 експертів може бути забезпечена

достовірність оцінки документу не нижче 0,8 [8].

Подальшим напрямком дослідження в цій галузі може бути розробка методики оцінки

інформаційно-аналітичної діяльності в цілому, одним із входних даних для якої будуть результати оцінювання інформаційних документів.

### Література

1. **Калашніков Є.М.,** Гаценко С.С., Шишацький А.В. Аналіз характеру сучасних воєнних конфліктів International scientific and practical conference “Challenges of hybrid war: information dimension”: conference proceedings, August 16–17, 2019. Vilnius: Izdevniecība “Baltija Publishing”. pages 24–27.
2. **Закон України** „Про розвідувальні органи України” // Відомості Верховної Ради, № 19, 2001. – С. 94.
3. **Івашенко Г.І.** Обґрунтування рекомендацій щодо удосконалення статутних документів Збройних Сил України для підготовки і ведення збройної боротьби в сучасних умовах: Дисертація канд. військ. наук: 20.01.05. – К., 2004. – 226 с.
4. **Василенко І.С.,** Макар А.Б. Уточнення змісту показників оцінювання виконання інформаційних (інформаційно-аналітичних) документів // Вісник воєнної розвідки, 2006. - № 12. – С. 66 – 70.
5. **Саати Т.** Принятие решений. Метод анализа иерархий / Пер. с англ. Р. Г. Вачнадзе. – М.: Радио и связь, 1993. – С. 23–69.
6. **Литвак Б. Г.** Экспертные оценки и принятия решений / Б.Г. Литвак. – М.: Патент, 1996. – 271 с.– ISBN 5-7518-0010-9.
7. **Development of methodology for complex processing of geoinformation data in the geoinformation system of special purpose in conditions of diversity and nenophynedy** A. Koshlan, O. Salnikova, M. Chekhovska, R. Zhyvotovskiy, Ye. Prokopenko, T. Hurskiy, A. Yefymenko, Ye. Kalashnikov, S. Petruk, A. Shyshatskiy Eastern-european journal of enterprise technologies. Vol. 5, No 9 (95) pp. 35-45, 2019: Information and controlling system.
8. **Яхина Е.П.** Методи оцінки інформаційних систем / Е. П. Яхина // В мире научных открытий. – 2010. – № 3 (09). – Часть 1. – С. 63–66.
9. **Method of Immunity Minimization of the Free Platform ed Inertial Navigation System of Unmanned Aircrafts** R. Bieliakov, S. Hatsenko, O. Fesenko, R. Zhyvotovskiy, S. Petruk, 2nd Ukraine Conference on Electrical and Computer Engineering Lviv, Ukraine, July 2-6, pp. 803-808, 2019.
10. **S. Kalantaievska,** H. Pievtsov, O. Kuvshynov, A. Shyshatskiy, S. Yarosh, S. Gatsenko, H. Zubrytskiy, R. Zhyvotovskiy, S. Petruk and V. Zuiko. Method of integral estimation of channel state in the multiantenna radio communication systems. // Eastern-European Journal of Enterprise Technologies. Vol 5, No 9 (95) (2018): pp 60–76. DOI: <https://doi.org/10.15587/1729-4061.2018.144085>.
11. **Ткаченко Н.О.** Розробка критеріїв для оцінки інформаційних наукових ресурсів в Інтернет / Н.О. Ткаченко// Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. - 2013. - Вип. 2 (25). - С. 136-143

## МЕТОДИКА ОЦЕНИВАНИЯ ИНФОРМАЦИОННЫХ ДОКУМЕНТОВ В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

*Виталий Владимирович Зуйко (кандидат военных наук, доцент)*

*Сергей Анатолиевич Мельник*

*Иван Николаевич Лукянчиков<sup>1</sup>*

*Алексей Васильевич Повещенко<sup>1</sup>*

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

*В статье предлагается решение актуальной научной задачи совершенствования научно-методического аппарата оценивания информационных документов при проведении разведывательно-информационной деятельности в системе военной разведки. Разведывательно-информационная деятельность - это непрерывный процесс, который включает комплекс мероприятий по организации и ведению в общей системе военной разведки разведывательно-информационной, информационной и информационно-аналитической работы для предоставления разведывательной информации ее потребителям. Собрать в определенные сроки, оперативно обработать, проанализировать и вовремя доложить это является главным и решающим задачей разведывательно-информационной деятельности в интересах обеспечения принятия решения. Особенностью современной разведывательно-информационной деятельности является решение широкого круга интеллектуальных по содержанию задач, результатами которых является разработка информационных документов. Оценка качества их выполнения является составной частью оценки информационно-аналитической деятельности в целом.*

*Для решения задач эффективной информационно-аналитической деятельности предложена методика оценивания информационных документов. Методика основана на методе анализа иерархий, который позволяет принимать решения на основе неформализованных показателей, которые невозможно описать аналитическими зависимостями. Предложенная методика позволит повысить качество оценивания информационных документов.*

**Ключевые слова:** *разведывательно-информационная деятельность; военная разведка; информационные документы; разведывательная информация.*

**METHOD OF EVALUATION INFORMATION DOCUMENTS IN INTEREST PROVIDING INFORMATION ACTIVITIES**

*Vitalii Zuiko (Candidate of Military Sciences, assistant professor)<sup>1</sup>*

*Serhii Melnyk<sup>1</sup>*

*Ivan Lukianchikov<sup>1</sup>*

*Oleksii Poveshchenko<sup>1</sup>*

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

*The article proposes the solution of the actual scientific task of improving the scientific and methodological apparatus of evaluating information documents in conducting intelligence and information activities in the military intelligence system. Intelligence is a continuous process that includes a set of measures for organizing and conducting intelligence, information and analytical work in the general military intelligence system to provide intelligence to its customers. Collect in a timely manner, promptly process, analyze and timely report is the main and decisive task of intelligence and information activities in the interests of decision-making. The peculiarity of modern intelligence-information activity is the solution of a wide range of intellectual tasks, the results of which are the development of information documents. Assessment of the quality of their implementation is an integral part of the evaluation of information and analytical activity as a whole.*

*For the decision of tasks of effective intelligence and information activities the method of evaluation of informative documents is offered. A method is based on the method of analysis of hierarchies, which allows to make a decision on the basis of unformalized indexes which it is impossible to describe analytical dependences. The offered method will allow to promote quality of evaluation of informative documents.*

**Key words:** *intelligence; reconnaissance; information documents; intelligence information.*

**References**

- 1. Kalashnikov Ye.M., Gaczenko S.S., Shishacz'kij A.V.** Anali'z kharakteru suchasnikh voyennikh konfli'kti'v International scientific and practical conference "Challenges of hybrid war: information dimension": conference proceedings, August 16–17, 2019. Vilnius: Izdevnieciba "Baltija Publishing". pages 24-27. **2. Zakon Ukrayini** „Pro rozvi'duval'ni' organi Ukrayini” // Vi'domosti Verkhovnoyi Radi, # 19, 2001. – S. 94. **3. Ivashchenko G.Г.** Obruntuvannya rekomendi'czi'j shhodo udoskonalennya statutnikh dokumenti'v Zbrojnikh Sil Ukrayini dlya pi'dgotovki i' vedennya zbrojnoyi borot'bi v suchasnikh umovakh: Disertaczi'ya kand. vi's'k. nauk: 20.01.05. – K., 2004. – 226 s. **4. Vasilenko Г.С., Makar A.B.** Utochnennya zmi'stu pokazniki'v oczi'nyuvannya vikonannya i'nformaczi'jnikh (i'nformaczi'jno-anali'tichnikh) dokumenti'v // Vi'snik voyennoyi rozvi'dki, 2006. - # 12. – S. 66 – 70. **5. Saati T.** Prinyatie reshenij. Metod analiza ierarkhij / Per. s angl. R. G. Vachnadze. – M.: Radio i svyaz', 1993. – S. 23–69. **6. Litvak B. G.** E'kspertny'e ocenki i prinyatie reshenij / B.G. Litvak. – M.: Patent, 1996. – 271 s.– ISBN 5-7518-0010-9. **7. Development** of methodology for complex processing of geopatronic data in the geoinformation system of special purpose in conditions of diversity and nenophynedy A. Koshlan, O. Salnikova, M. Chekhovska, R. Zhyvotovskiy, Ye. Prokopenko, T. Hurskiy, A. Yefymenko, Ye. Kalashnikov, S. Petruk, A. Shyshatskiy Eastern-european journal of enterprise technologies. Vol. 5, No 9 (95) pp. 35-45, 2019: Information and controlling system. **8. Yakhina E.P.** Metody' ocenki informacziyonny'kh sistem / E. P. Yakhina // V mire nauchny'kh otkry'tij. – 2010. – # 3 (09). – Chast' 1. – S. 63–66. **9. Method** of Immunity Minimization of the Free Platform ed Inertial Navigation System of Unmanned Aircrafts R. Bieliakov, S. Hatsenko, O. Fesenko, R. Zhyvotovskiy, S. Petruk, 2nd Ukraine Conference on Electrical and Computer Engineering Lviv, Ukraine, July 2-6, rr. 803-808, 2019. **10. S. Kalantaievska, H. Pievtsov, O. Kuvshynov, A. Shyshatskiy, S. Yarosh, S. Gatsenko, H. Zubrytskyi, R. Zhyvotovskiy, S. Petruk and V. Zuiko.** Method of integral estimation of channel state in the multiantenna radio communication systems. // Eastern-European Journal of Enterprise Technologies. Vol 5, No 9 (95) (2018): rr 60–76. DOI: <https://doi.org/10.15587/1729-4061.2018.144085>. **11. Tkachenko N.O.** Rozrobka kriteri'yiv dlya oczi'nki i'nformaczi'jnikh naukovikh resursi'v v I'nternet / N.O. Tkachenko// Naukovi' praczi' Donecz'kogo naczi'onal'nogo tekhnichnogo uni'versitetu. Seri'ya: Obchislyuval'na tekhnika ta avtomatizaczi'ya. - 2013. - Vip. 2 (25). - S. 136-143

*Валерій Дмитрович Сергієнко (кандидат технічних наук, доцент)*

*Микола Якович Павлушко (кандидат військових наук, професор)*

*Олександр Олександрович Шапран*

*Андрій Степанович Мулявка*

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

## ОСОБЛИВОСТІ ВПЛИВУ АКУСТИЧНОЇ ЗБРОЇ НА ОСОБОВИЙ СКЛАД ВІЙСЬКОВИХ ФОРМУВАНЬ В УМОВАХ ВЕДЕННЯ НЕ КОНВЕНЦІЙНИХ ВОЄННИХ ДІЙ

*Стаття присвячена дослідженням засад застосування зброї на нетрадиційних принципах дії, зокрема, акустичної зброї. Надана базова інформація стосовно фізіологічних ефектів, що виникають при впливі акустичної зброї на особовий склад військових формувань при виконанні ними завдань за функціональним призначенням в умовах ведення не конвенційних воєнних дій. Проведено аналіз і узагальнення можливих наслідків впливу акустичних хвиль на особовий склад, що дозволить визначити найбільш доцільні способи надання першої медичної допомоги при отриманні травм (ушкоджень тощо) від впливу акустичної зброї і дозволить зменшити безпосередні втрати особового складу та скоротити час на відновлення боєздатності людей.*

**Ключові слова:** акустична зброя; акустичні хвилі; вплив; генератор звуку.

### Вступ

**Постановка проблеми.** Досвід проведення антитерористичної операції (АТО) та операції Об'єднаних сил (ООС) на Сході України у особливих районах Донецької та Луганської областей (ОРДЛО) [1] дає підстави стверджувати, що угрупованням військ, з'єднанням, військовим частинам та підрозділам Збройних Сил (ЗС) України, іншим військовим формуванням (ІВФ) і правоохоронним органам (ПрО) при виконанні бойових завдань все частіше доводиться зіткнутися із загонами бойовиків, сепаратистів і регулярними військами Російської Федерації (РФ), які використовують сучасну зброю та озброєння. Противник постійно змінює форми, способи, а також тактичні прийоми застосування засобів ведення збройної боротьби, оснащує свої війська сучасною високоефективною бойовою технікою [5, 6].

Нарощування викликів і стратегічних загроз, у сенсі параноїдального бажання "кремлівського" керівництва щодо заволодіння геополітичним лідерством, змушує замислюватися над проблемними питаннями щодо підготовки ЗС України до ведення операцій (бойових дій) в умовах застосування противником новітньої зброї, зокрема зброї на нетрадиційних принципах дії (ЗНПД) [3,5].

**Аналіз останніх досліджень і публікацій.** У зв'язку з цим особливу актуальність набувають наукові дослідження в галузі зброї нелетальної дії (ЗНД), що спрямовані на створення зразків зброї і озброєння, призначених для вирішення бойових (спеціальних) задач при виключенні, або зведенні до мінімальних збитків навколишньому середовищу і запобіганні шкоди (загибелі, поневіченню, психічних розладів тощо) мирного населення. Важливу увагу у ході досліджень слід приділити визначенню ролі і місця ЗНПД при веденні бойових дій у ході гібридних війн і збройних конфліктів.

Серед відомих видів нелетальної зброї

особливе місце займає акустична зброя (АЗ). З давніх часів людство використовувало звук для оповіщення, попередження, відлякування, передачі сигналів, впливу на людей і тварин, на природні та штучні споруди тощо [2, 3, 5]. Акустична зброя розробляється і випробовується у провідних країнах світу, як зброя, що може використовуватись для охорони режимних і інших об'єктів у якості засобів попередження і реагування, при облозі споруд і об'єктів, для контролю над натовпом, для створення бар'єрів на периметрах або кордонах, для заборони доступу або атаки по площам, для роззброєння солдат (сепаратистів, бойовиків, терористів тощо). Акустична зброя миттєво виводить з ладу противника, але не призводить до стійких фізичних ушкоджень. Однак, надійна інформація про її характеристики і вплив вкрай обмежена і суперечна [2-5].

У зв'язку з вище означеним, особливу актуальність набувають наукові дослідження стосовно визначення і систематизації можливих фізіологічних ефектів впливу акустичної зброї на особовий склад частин і підрозділів силових структур при виконанні ними бойових завдань, розвитку й вдосконаленню способів та засобів захисту військ від акустичної зброї противника в умовах ведення гібридних, неконвенційних воєнних дій. Важливим аспектом застосування акустичної зброї є можливість її використання для звільнення будівель від бойовиків (сепаратистів) під час проведення антитерористичних і миротворчих операцій [3, 5].

Ефект і ступінь впливу акустичної зброї залежить від фізичного стану і здоров'я людини, його віку, – тобто є індивідуальним показником для кожної окремої людини. Тому доцільно розглянути фізичні ефекти впливу акустичних хвиль різних діапазонів, що дозволить визначити наслідки впливу акустичної зброї і перспективи її застосування в сучасних умовах та у майбутньому. Аналіз ефектів впливу акустичних коливань на особовий склад дозволить зробити деякі

узагальнення, на підставі яких у подальшому можливо оцінити доцільність використання певних частотних смуг акустичного діапазону для розробки акустичної зброї та розробити способи та засоби захисту від неї у разі її застосування противником.

У сучасних наукових дослідженнях і публікаціях розглянуті проблеми пов'язані з розробкою і застосуванням акустичної [2-5]. Частково інформацію за означеною тематикою можна знайти у наведеної літературі. Проте у цих джерелах не достатньо повно висвітлені і не систематизовані особливості фізичного впливу акустичної зброї на особовий склад, а також не запропоновані заходи захисту від неї.

На даний момент відсутня достовірна база даних стосовно конкретних результатів впливу акустичної зброї на особовий склад при проведенні дослідницьких випробувань і застосуванні її у бойових умовах. У відомій літературі наводяться окремі епізоди із застосування акустичної зброї, які більшою мірою мають характер поліцейських чи миротворчих дій: застосування в операціях проти Іраку; на морі проти сомалійських піратів; розгін демонстрації грузинських опозиціонерів; у зоні Арабсько-Ізраїльського конфлікту. Як правило, такий матеріал супроводжується зображенням системи LRAD встановленої на бронетранспортері або на військовому (поліцейському) позашляховику. Уся ідея впливу такої зброї зосереджена у створенні потужних звуків, під дією яких виникає біль у органах слуху [2,3].

На теперішній час не проведено повного аналізу з точки зору аспектів міжнародного гуманітарного права про дозвіл використання акустичної зброї у бойових діях. Розробка, випробування та створення акустичної зброї потребує великих фінансових витрат. Крім того, для розробки акустичної зброї необхідно мати відповідну високотехнологічну виробничу базу.

Незважаючи на небезпеку появи на озброєнні деяких країн акустичної зброї, дослідження, спрямовані на її розробку, вивчення механізмів впливу і способів захисту від такої зброї, в Україні не проводилися. Тому доцільно спланувати проведення наукових досліджень для більш точної оцінки рівня загрози від можливого застосування акустичної зброї потенційним противником.

**Метою статті** є аналіз і узагальнення ефектів впливу акустичних хвиль різних діапазонів на особовий склад військових формувань при варіюванні основних параметрів випромінювання у досяжних межах. Оцінка можливостей і напрямків використання акустичної зброї у сучасних воєнних конфліктах та у війнах наступних поколінь.

В подальшому доцільно передбачити розроблення зразків акустичної зброї у різних діапазонах частот, проведення досліджень впливу акустичного випромінювання на особовий склад і бойову техніку та розроблення рекомендацій щодо доцільності створення такої зброї і засобів захисту від неї в Україні.

### **Виклад основного матеріалу дослідження**

Акустична зброя – це засоби впливу на об'єкти ураження енергією акустичних коливань певної частоти, потужності та форми. Вражаючим

фактором акустичної зброї є перепад тиску середовища поширення акустичних коливань, що діє на об'єкт.

За частотним діапазоном акустична зброя поділяється на інфразвукову, звукову, та ультразвукову. Доречно виділити три діапазони хвиль, що можуть використовуватися для акустичної зброї: інфразвук – 0...16 Гц; звук, який чути (звуковий діапазон) – 16 Гц...20 кГц; ультразвук більше 20 кГц. Ступінь впливу акустичної зброї різних діапазонів на особовий склад і об'єкти суттєво розрізняються. Для кожного діапазону можливо виокремити головні особливості хвиль і переважні фізичні наслідки їх впливу [2-5, 7].

Таким чином доцільно розглянути фізичні ефекти впливу різних діапазонів акустичних хвиль на поведінку живих організмів, що дозволить визначити наслідки її впливу і перспективи застосування в умовах ведення збройних конфліктів, а також оцінити доцільність використання певних частотних смуг акустичного діапазону для розробки акустичної зброї.

Інфразвукова зброя застосовується у діапазоні частот менше 16 Гц.

У якості прикладу можна навести проект США по створенню гостроспрямованої “акустичної кулі” яка формується антеною діаметром 1-2 метра у вигляді пачки імпульсів акустичних хвиль. При великих потужностях випромінювання така “куля” буде викликати тимчасову втрату боєздатності особового складу військ противника.

Використання двох генераторів звуку на близьких частотах, наприклад,  $f_1 = 40$  Гц і  $f_2 = 46$  Гц дозволяє утворити биття з частотою  $f_6 = 6$  Гц, які суттєво впливають на роботу серця. При малих потужностях випромінювання виникає нудота й дзвін у органах слуху, погіршується зір, виникає панічний страх. Інфразвук середньої інтенсивності спричиняє розлад органів травлення, уражає мозок, викликає параліч, загальну слабкість, навіть сліпоту. Потужний інфразвук здатний взагалі зупинити серце, призвести до розриву внутрішніх органів людини, що свідчить про достатньо високу ефективність інфразвукової акустичної зброї [2, 3, 5].

Звукова акустична зброя використовує потужні коливання у діапазоні частот від 16 Гц до 20 кГц. Основними параметрами, які впливають на сприйняття звуку людиною є частота і потужність. Потужний звук може зменшити здатність чути (тимчасово або постійно), а також вплинути на вестибулярний апарат. При великих інтенсивностях звукових хвиль (навіть при коротких експозиціях) може відбутися ушкодження вушних органів. Особливо небезпечні для людини звукові хвилі, що мають імпульсний, переривчастий характер. Дія коротких акустичних імпульсів навіть з середньою відносною інтенсивністю може привести до повної втрати слуху, практично без можливості його відновлення. Для ефективного захисту особового складу від впливу звукової акустичної зброї можна запропонувати застосування навушників або інших засобів захисту органів слуху.

Ультразвукова зброя застосовується у діапазоні частот більше 20 кГц і має специфічні особливості впливу на особовий склад. Мала довжина ультразвукових хвиль дозволяє створювати

компактні високоенергетичні системи випромінювачів з дуже великою інтенсивністю і можливістю формування гостро направленою випромінювання хвиль. Проміньовий характер розповсюдження ультразвуку дозволяє відстежувати об'єкти, що уражаються та виключити вплив випромінювання на осіб, які обслуговують такий тип акустичної зброї [2-5].

Застосування ультразвукової зброї приводить до погіршення самопочуття, викликає втрату орієнтування у просторі і головний біль. На частотах понад 100 кГц спостерігається суттєвий вплив на нервову систему. Ультразвук на частотах до 30кГц визиває термальні ефекти: перегрівання

та опіки тканин, зневоднення організму, зміну структури крові. Основним недоліком ультразвукових хвиль є значне згасання їх інтенсивності з підвищенням частоти, що може бути усунуто за рахунок збільшення потужності і фокусування випромінювання.

Проведений вище огляд ефектів впливу акустичних коливань на людину дозволяє зробити деякі часткові узагальнення, на підставі яких у подальшому можливо оцінювати доцільність використання певних частотних смуг акустичного діапазону для розробки акустичної зброї. Зведені дані по впливу акустичних хвиль на особовий склад наведені у таблиці 1.

Таблиця 1

Вплив акустичних хвиль на особовий склад

Джерело випромінювання, параметри сигналу	Ефект впливу	Примітки
<b>Інфразвук</b> з малими рівнями потужності (на рівнях 85...110 дБ)	Беззвітне почуття жаху та групова паніка у натовпі	При влученні у відповідний інтервал частот (5...8 Гц)
Інфразвук з рівнями потужності до 130 дБ	Порушення психомоторних функцій людини, або стан, що передую епілептичному нападу (судоми з втратою свідомості).	На певних частотах
Інфразвук на рівні 90...120 дБ на низьких частотах (від 5 Гц і вище)	Біль у шлунку і сильна нудота (крайні рівні занепокоєння та розладу)	Досягається при хвилинних експозиціях
Інфразвук на рівні 140...150 дБ	Важкі фізичні травми та пошкодження тканин, травмування внутрішніх органів навіть до зупинки серця	Найбільш небезпечний діапазон частот від 0 до 9 Гц
Інфразвук на рівні приблизно 170 дБ	Миттєві травми типу травм від ударних хвиль	
Інфразвук на рівні 85...110 дБ на частоті 13 Гц	Напад «морської хвороби», ефект гипофаренксу (нестримного блювотіння)	
Інфразвук на частоті 7 Гц	Вплив на психіку (припинення будь-якої розумової діяльності)	
<b>Звук</b> на рівнях більше 120 дБ	Пошкодження слуху або глухота	
Звук з рівнем у межах від 80 дБ до 120 дБ при тривалому впливі	Різне зниження чуливості слуху	На обмежений час (хвилини, тижні, місяці), після чого слух може поновитися
Вплив коротких акустичних імпульсів з відносною інтенсивністю більше 90 дБ.	Повна втрата слуху	втрата слуху наступає миттєво
Звук з рівнем більше 140 дБ	Біль у вухах	По усьому звуковому діапазону
Звук з рівнем більше 160 дБ	Розрив барабанної перетинки	
Звукові частоти від 50 до 100 Гц при рівнях 150... 155 дБ	Слабка нудота та запаморочення	
Звукові частоти нижче 50 Гц на рівнях до 150 дБ	Вібрації грудної клітини та деякі зміни дихального ритму; кашель, тиск під грудиною, задишка при диханні	
Звукові частоти від 30 до 100 Гц при рівнях 150 дБ	Збільшення частоти пульсу, почервоніння шкіри, слиновиділення і біль при ковтанні. Поле зору мерехтить та гострота зору зменшується	У суб'єктів спостерігається наявна втома
Звукові частоти вище 10 кГц при рівнях звуку вище 160 дБ	Нагрів повітряних порожнин (у носі і роті), тканин і волосся	Вуха не захищені
<b>Ультразвук</b> на частотах до 30 кГц при рівнях більше 160 дБ	Опіки тканин і зневоднення, перегрів (навіть до смертельно високих температур)	
Ультразвук на частотах більше 30 кГц	Втрата орієнтації у просторі, нестійкість у позі «Ромберга», нестерпний головний біль, крововилив у мозок	
Гостроспрямована акустична "куля", що випромінюється антеною з діаметром 1...2 м у вигляді пачки імпульсів	Тимчасова втрата боєздатності особового складу військ противника	При достатній потужності імпульсів, що випромінюються
Генератори звуку, що випромінюють на частотах биття $f_1 = 40$ Гц і $f_2 = 46$ Гц.	Відчутний функціональний збиток серцю на частоті биття $F_6 = 6$ Гц	

### Висновки й перспективи подальших досліджень

1. Акустична зброя може бути віднесена до перспективних ефективних видів нелетальної зброї майбутнього.

2. Огляд можливих наслідків застосування акустичної зброї дозволяє заздалегідь передбачити (визначити) необхідні конкретні заходи з надання першої медичної допомоги, що значно скоротить час на відновлення боєздатності особового складу

частин і підрозділів безпосередньо у ході ведення бойових дій (на полі бою).

3. Дослідження механізмів впливу акустичної зброї на особовий склад є підґрунтям для розроблення рекомендацій для зниження ефективності такої зброї шляхом застосування способів та пристроїв захисту від неї в сучасних

умовах та у війнах наступних поколінь.

4. У подальших дослідженнях доцільно провести аналіз тактичних способів і прийомів застосування акустичної зброї у конкретних ситуаціях, а також питань підготовки особового складу по її використанню у бойових умовах.

### Література

1. Закон України від 18.01.2018 року "Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях (Відомості Верховної Ради, 2018, № 10, ст.54)". 2. Добыкин В.Д., Куприянов А.И., Пономарев В.Г., Шустов Л.Н. Радиоэлектронная борьба. Силовое поражение радиоэлектронных систем / под ред. А.И. Куприянова. Москва: Вузовская книга, 2007. 468 с. 3. Ковтуненко О.П., Богучарський В.В., Слюсар В.І., Федоров П.М. Зброя на нетрадиційних принципах дії (стан, тенденції, принцип дії та захист від неї). Полтава: Видавництво ПВІЗ, 2006. 247 с.

4. Кайно Г. Акустические системы. Москва: Мир, 1990. 425 с. 5. Сергієнко В.Д., Богучарський В.В., Дрок Л.В., Міроненко П.О. Перспективи застосування акустичної зброї в сучасних воєнних конфліктах. *Наука і оборона*. Київ. 2016. №1. С. 39-42. 6. Сергієнко В.Д., Дрок Л.В., Родіонов С.С., Богучарський В.В., Федоров П.М. Деякі аспекти застосування засобів інструментальної ольфактроніки в умовах ведення не конвенційних воєнних дій. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2016. № 1(25). С. 115-119. 7. Невідкладна військова хірургія. / пер.з англ. Київ, Наш Формат, 2015. 568 с.

### ОСОБЕННОСТИ ВЛИЯНИЯ АКУСТИЧЕСКОГО ОРУЖИЯ НА ЛИЧНЫЙ СОСТАВ ВОИНСКИХ ФОРМИРОВАНИЙ В УСЛОВИЯХ ВЕДЕНИЯ НЕ КОНВЕНЦИОННЫХ ВОЕННЫХ ДЕЙСТВИЙ

*Валерий Дмитриевич Сергиенко (кандидат технических наук, доцент)*

*Николай Яковлевич Павлушко (кандидат военных наук, профессор)*

*Александр Александрович Шапран*

*Андрей Степанович Мулявка*

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

*Статья посвящена исследованию основ применения оружия на нетрадиционных принципах действия, в частности, акустического оружия. Предоставленная базовая информация о физиологических эффектах, возникающих при воздействии акустического оружия на личный состав военных формирований при выполнении ими задач по функциональному назначению в условиях ведения НЕ конвенционных военных действий. Проведен анализ и обобщение возможных последствий влияния акустических волн на личный состав, что позволит определить наиболее целесообразные способы оказания первой медицинской помощи при получении травм (повреждений и т.д.) от воздействия акустического оружия и позволит уменьшить непосредственные потери личного состава и сократить время на восстановление боеспособности людей.*

*Ключевые слова: акустическое оружие; акустические волны; воздействие; генератор звука.*

### PECULIARITIES OF ACOUSTICAL WEAPON EFFECTS ON PERSONAL COMPOSITION OF MILITARY FORMATIONS IN CONDITIONS OF NOT CONVENTIONAL MILITARY ACTION

*Valerii Serhiienko (Candidate of Technical Sciences, assistant professor)*

*Mykola Pavlunko (Candidate of Military Sciences, professor)*

*Oleksandr Shapran*

*Andrii Muliavka*

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

*The article is devoted to the study of the principles of the use of weapons on unconventional principles of action, in particular, acoustic weapons. Basic information is provided concerning the physiological effects arising from the influence of acoustic weapons on the personnel of military formations when performing their tasks for functional purposes in the context of conducting non-conventional hostilities. An analysis and generalization of the possible effects of acoustic waves on the personnel, which will determine the most appropriate ways to provide first aid in trauma (damage, etc.) from the impact of acoustic weapons and will reduce the immediate loss of personnel and reduce the time to recover fighting.*

*Key words: acoustic weapons; acoustic waves; impact; sound generator.*

### References

1. Zakon Ukrainy vid 18.01.2018 roku "Pro osoblyvosti derzhavnoji polityky iz zabezpechennja derzhavnogho suverenitetu Ukrainy na tymchasovo okupovanykh terytorijakh u Doneckijj ta Lughanskjij oblastjakh (Vidomosti Verkhovnoji Rady, 2018, № 10, st.54)". 2. Dobyikin V.D., Kupriyanov A.I., Ponomarev V.G., Shustov L.N. Radioelektronnyaya borba. Silovoe porazhenie radioelektronnykh sistem / pod red. A.I. Kupriyanova. Moskva: Vuzovskaya kniga, 2007. 468 s. 3. Kovtunenکو O.P., Boghucharskij V.V., Sljusar V.I., Fedorov P.M. Zbroja na netradycijnykh pryncypakh diji (stan, tendenciji, pryncyp diji ta zakhyst vid nej). Poltava: Vydavnyctvo

PVIZ, 2006. 247 s. 4. Kayno G. Akusticheskie sistemyi. Moskva: Mir, 1990. 425 s. 5. Serghijenko V.D., Boghucharskij V.V., Drok L.V., Mironenko P.O. Perspektivy zastosuvannja akustychnoji zbroji v suchasnykh vojennykh konfliktakh. *Nauka i oborona*. Kyjiv. 2016. №1. S. 39-42. 6. Serghijenko V.D., Drok L.V., Rodionov S.S., Boghucharskij V.V., Fedorov P.M. Dejaki aspekty zastosuvannja zasobiv instrumentalnoji oljifaktroniky v umovakh vedennja ne konvencijnykh vojennykh dij. Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony. 2016. № 1(25). S. 115-119. 7. Nevidkladna vijsjkova khirurgija. / per.z anghl. Kyjiv, Nash Format, 2015. 568 s.



*Сергій Станіславович Гаценко (кандидат технічних наук)*

*Олег Володимирович Костенко*

*Віктор Петрович Кузьменко*

*Василь Михайлович Мазуренко*

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

## МЕТОДИКА РАНЖУВАННЯ ДЖЕРЕЛ РОЗВІДУВАЛЬНИХ ВІДОМОСТЕЙ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ ПРИ ОРГАНІЗАЦІЇ І ВЕДЕННІ РОЗВІДКИ

В статті пропонується вирішення актуального наукового завдання розробки науково-методичного апарату ранжування джерел розвідувальних відомостей, які характеризують об'єкти розвідки при оцінці оперативної обстановки та радіоелектронної обстановки в інтересах планування розвідки. Ранг джерела розвідувальних відомостей розраховується з урахуванням його якісних і кількісних характеристик. Функціонування залежності рангу джерела розвідувальних відомостей від його розвідувальної цінності і ототожнюємих з ними радіоелектронною обстановкою реалізується нечіткою нейронною мережею. Результатом виконання процедури ранжування є введення на множині джерел розвідувальних відомостей що плануються, відношення порядку. Впорядкування множини джерел розвідувальних відомостей дозволяє формалізувати і вирішити завдання квазіоптимального розподілу засобів і сил розвідки.

**Ключові слова:** ранжування, джерела розвідувальних відомостей, об'єкт розвідки, планування розвідки, нечіткі множини, застосування сил і засобів розвідки.

### Вступ

Результативність процесу функціонування сил і засобів розвідки визначається кількістю викритих об'єктів розвідки (ОР) через викриття функціонування радіоелектронних засобів (РЕЗ), радіотехнічних систем (РТС), які є джерелами розвідувальних відомостей (ДРВ) і якістю добутої про них розвідувальної інформації.

В свою чергу вказані показники залежать від ступеня відповідності результатів вирішення завдання планування застосування сил і засобів розвідки (СіЗР), у відповідності до умов радіоелектронної обстановки (РЕО).

Ключовою операцією, яка використовується при вирішенні завдання планування бойового застосування засобів розвідки є операція виявлення та розпізнавання ДРВ.

ДРВ, які виявляються засобами розвідки, характеризуються множиною якісних і кількісних характеристик, маючих різну розвідувальну цінність і відповідно с цим різну ступінь важливості.

Таким чином, виявлення та розпізнавання ДРВ потребує реалізації достовірного, науково обґрунтованого відображення множини характеристик ДРВ  $H$ , на множині дійсних чисел, які характеризують ранг  $k$ -го ДРВ  $w_k : f(h_k) \rightarrow w_k$  де  $h_k = \{h_1, \dots, h_n\}, h_i \in H$ .

Представлення відображення  $f(h_k) \rightarrow w_k$  в аналітичному вигляді в контексті завдання що розглядається на сьогоднішній день не існує. Методики які є на теперішній час реалізують

відображення  $f(h_k) \rightarrow w_k$  з використанням математичного апарату на основі методів експертних оцінок, методу нормування, або методів мультиплікативної (адитивної) згортки. Застосування вказаної групи методів для реалізації процедури ранжування ДРВ обумовлюється наявністю в існуючій методиці планування застосування сил і засобів розвідки наступних недоліків:

відсутність автоматизації процедури планування застосування засобів розвідки в заданих умовах РЕО;

аналіз результатів виконання плану застосування сил і засобів розвідки не формалізований і носить суб'єктивний характер;

облік наслідків результатів застосування засобів розвідки в ході виконання наступного планування застосування сил і засобів розвідки відсутній.

Таким чином, в умовах, коли кількість множини ранжуємих ДРВ має велику кількість, існуючий підхід ранжування ДРВ не дозволяє реалізувати адаптивне раціональне планування застосування засобів розвідки.

**Постановка проблеми.** Декомпозиція завдання планування застосування сил і засобів розвідки на ряд часткових завдань і їх взаємозв'язок представлені на рис. 1.

В формалізованому вигляді завдання ранжування ДРВ в контексті вирішення завдань планування застосування СіЗР, може бути представлена в наступному вигляді:

$$r^* = \arg \max_{\pi \in G} (F(\pi[a, r])), \quad (1)$$

де:  $F(\pi[a, r])$  – цільова функція показника ефективності функціонування СіЗР;  
 $(\pi[a, r])$  – план РЕР при використанні відповідного алгоритму планування а до ранжуемого списку ДРВ r ;

а – алгоритм планування застосування СіЗР;  
 r – ранжований список ДРВ, який складається із n елементів, значення i-го елемента r характеризує ранг i-го ОР серед n джерел;  
 G – множина обмежень які накладаються на процедуру планування в заданих умовах РЕО.

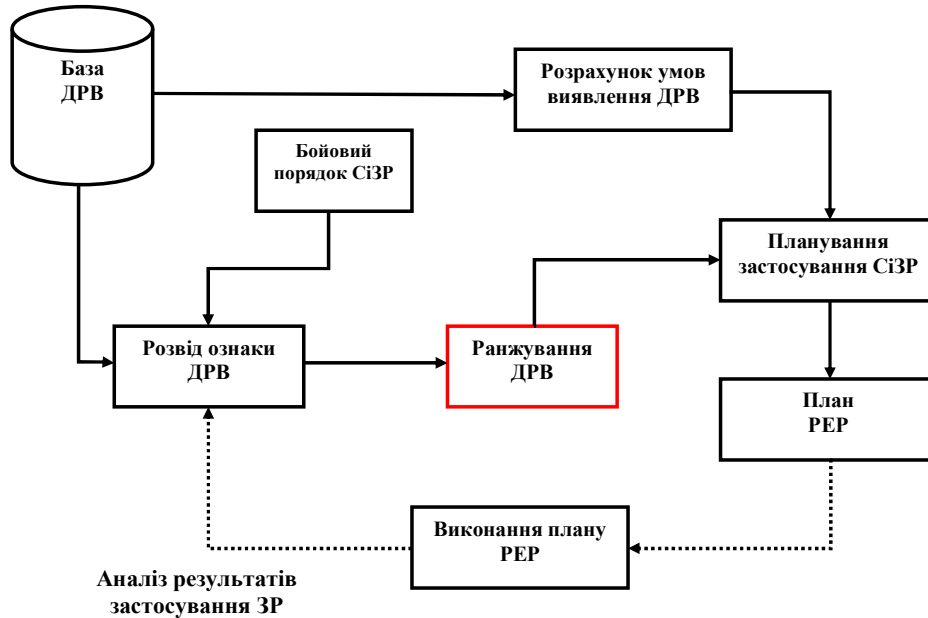


Рис. 1. Структурно-логічна схема вирішення завдання планування застосування СіЗР

В якості значення цільової функції  $F(\pi[a, r])$  виразу (1) в даній роботі розглянемо сумарний ранг ДРВ, в ході виконання плану  $\pi$ . Результативність процесу виконання плану РЕР  $\pi$  пропонується оцінити згідно наступного критерію.

$$\left( \frac{\sum_{i=1}^n k_i \cdot r_i}{n} \right) \rightarrow \min; \quad (2)$$

$$\begin{cases} k_i = 0, \text{ якщо } i\text{-й ОР не врахований;} \\ k_i = 1, \text{ якщо } i\text{-й ОР врахований.} \end{cases}$$

де  $k_i$  – бінарний коефіцієнт, який характеризує факт врахування i ДРВ в ході виконання плану  $\pi$ ;  
 $r_i$  – ранг i-го ДРВ розрахований по запропонованій методиці;  
 n – кількість ДРВ які враховуються при плануванні.

**Аналіз останніх досліджень і публікацій.** В [1, 2] автором запропонована методика визначення раціональної кількості розвідувальних ознак для визначення приналежності їх до об'єктів розвідки. Авторами робіт [3-5] було запропоновано науково-методичний апарат визначення стану об'єктів розвідки. Запропоновані підходи вимагають значних, потужних обчислювальних ресурсів. Аналіз робіт [6-8] стверджує, що завдання оцінки рангу ДРВ подібна класичній задачі класифікації (розпізнавання) образів. Найбільш поширеним і апробованим математичним апаратом, застосовуваним для вирішення подібних завдань

на сьогоднішній день, є математичних апарат нейронних мереж. Разом з тим застосування класичної нейронної мережі для вирішення завдання ранжування значної кількості ДРВ пов'язане з проблемою навчання нейронних мереж і передбачає наявність певної навчальної вибірки. Відповідно, для реалізації даної процедури потрібно множина R, що включає в якості своїх елементів пари значень і безліч характеристик. Процес формування безлічі R з обов'язковим виконанням умови узгодженості даних – складна, трудомістка процедура, що викликано неможливістю охарактеризувати складний багатокритерійний об'єкт однією чисельною величиною. Достовірне рішення даного завдання можна забезпечити, запропонувавши характеризувати ДРВ як джерело, здатне належати до трьох класів – “важливе”, “середнє”, “неважливе” – з певною функцією належності до кожного класу. Формалізацію даної процедури зручно проводити, за допомогою математичного апарату теорії нечітких множин [9, 10].

Таким чином **метою** статті є розробка методики ранжування ДРВ радіоелектронної розвідки при організації та веденні розвідки з використанням математичного апарату нечітких штучних нейронних мереж [11, 12], що дозволить враховувати наслідки застосування засобів розвідки для спостереження за ДРВ в ході планування розвідки з застосуванням принципів ранжування ДРВ з врахуванням динамічних змін РЕО.

**Виклад основного матеріалу дослідження**

Методика ранжування ДРВ з використанням нечіткої нейронної мережі складається з послідовного виконання наступних кроків.

**Крок 1.** Формується архітектура нейронної мережі, у вигляді графа  $G = (X, V)$ , де  $X$  – множина вершин нейронної мережі,  $V$  – множина зв'язків між елементами множини  $X$ . Ваги зв'язків  $w_{ij}$  між нейронами мережі ініціалізуються випадковими значеннями в інтервалі можливих значень від  $-0,5$  до  $0,5$ . Розраховується значення коефіцієнта  $w_{ij}^*$ :

$$w_{ij}^* = \sqrt{\sum_{j=1}^n w_{ij}^2} \quad (3)$$

де  $n$  – кількість вершин в  $i$ -му шарі нечіткої нейронної мережі.

Здійснюється переініціалізація ваг зв'язків між нейронами суміжних шарів:

$$w_{ij} = \frac{\beta \cdot w_{ij}}{w_{ij}^*}, \quad (4)$$

де  $\beta$  – фактор масштабування, який розраховується згідно виразу

$$\beta = 0,7 \cdot p^{-n}, \quad (5)$$

де  $p$  – кількість нейронів, у внутрішніх шарах нейронної мережі;

$n$  – кількість нейронів шару.

Для кожної вершини нейронної мережі випадковим шляхом встановлюється величина зміщення  $w_{0j}, w_{0j} \in [-\beta, \beta]$

**Крок 2.** На вхід нейронної мережі подаються об'єкти вибірки, що навчається – вектор  $x = (x_1, x_2, x_3, x_4, x_5, x_6)$ , а також відповідні еталони результатів їх обробки по приналежності до класів множини  $C$  – вектора  $d$ .

**Крок 3.** Виконання процедури фазифікації першого шару нейронної мережі. Дана процедура полягає у визначенні функції належності  $\mu(x|c_j)$  характеристик ДРВ  $x_1, x_2, x_3, x_4, x_5$ , до класів,

визначених на множині  $C - \mu(x|c_j), j \in \overline{1, |C|_5}$ .

Під функцією належності нечіткої множини розуміють узагальнену індикаторну функцію класичної множини. Реалізація даної процедури включає два етапи.

Перший етап – розрахунок центрів класів  $V_{ij}$  елементів множини  $C$  для кожної розвідувальної ознаки ДРВ.

$$V_{ij}^S = \frac{\sum_{x \in X_i} (\mu^S(x|c_j))^2 \cdot x}{\sum_{x \in X_i} (\mu^S(x|c_j))^2}, \quad (6)$$

$$\sum_{x \in X_i} (\mu^S(x|c_j))^2 \neq 0,$$

де  $S$  – номер ітерації;

$X_i$  – множина джерел вибірки що навчається, яка характеризує функцію належності значень  $i$ -ї характеристики ДРВ до елементів множини  $C$ .

Другий етап полягає у розрахунку значень функції приналежності  $i$ -ї характеристики ДРВ на  $S$ -й ітерації:

$$\mu^S(x|c_j) = \frac{1/(x - V_{ij})^2}{\sum_{j=1}^{|C|} (1/(x - V_{ij})^2)}, \quad (7)$$

якщо  $(x - V_{ij})^2 > 0$ ;

$$\mu^S(x|c_j) = 1, \text{ якщо } (x - V_{ij})^2 = 0.$$

Обидва етапи виконуються ітераційно до тих пір, доки різниця отриманих значень центрів класів не буде відповідати умові

$$|V_{ij}^S - V_{ij}^{S-1}| \leq \epsilon,$$

де  $\epsilon$  – мінімально можлива різниця значень центрів класів, отриманих на двох послідовних ітераціях.

Вираз (7) дозволяє визначити функцію належності характеристик ДРВ до елементів множини  $C$  в залежності від її кількісного значення.

Результатом проходження вектора характеристик ДРВ  $x$  через перший шар мережі є синтез другого шару мережі, активаційна функція вершин якого має вид

$$y_{2k} = \min(\mu(x|c_j)), i \in \overline{1, 6}, j \in \overline{1, 3}, \quad (8)$$

де  $\mu(x_i)$  – функція належності  $i$ -ї характеристики яка використовується в процесі навчання джерела, вибірки що навчає до  $j$ -го елементу множини  $C$ .

Аргумент виразу (8) визначається значеннями сигналів, які розповсюджуються вершинами-батьками вершини  $k$  графа нечіткої множини  $C$ .

**Крок 4.** Кожний нейрон третього і наступного шарів мережі отримують сигнал від усіх нейронів попереднього шару, перетворюючи отриманий сигнал у відповідності з активаційною функцією і транслюється кожному нейрону наступного шару.

Аргумент активації функції нейрона  $z_j$  розраховується згідно виразу

$$z_j = w_{0j} + \sum_{i=1}^n y_i \cdot w_{ij}, \quad (9)$$

де  $n$  – кількість нейронів в попередньому шарі.

На основі отриманого значення аргументу  $z_j$  розраховуємо значення активаційної функції нейрону  $y_j = f(z_j)$ .

**Крок 5.** Проводиться перевірка вимог продовження навчання нейронної мережі згідно визначеному критерію. Якщо критерій зупинки виконується, потік управління алгоритмом передається на крок 9. Помилка роботи класифікатора вираховується на останньому шарі нейронної мережі згідно виразу:

$$\varepsilon = \sum_{i=1}^n |d_i - y_i|,$$

$$\sigma_i = f'(z_i) \cdot \sum_{j=1}^n \sigma_j \cdot w_{ij}.$$

**Крок 6.** Виконується зворотне розповсюдження помилки. Кожен нейрон вихідного шару отримує цільове значення  $d_i$  обчислює величину похибки  $\sigma_i$ :

$$\sigma_i = (d_i - y_i) \cdot f'(z_i),$$

де  $f'(z_i) = f'(z_i) \cdot (1 - f(z_i))$ .

Розраховується величина коректування вісі зв'язку  $\Delta w_{ji}$ , а також величини коректування зміщення  $\Delta w_{0j}$ :

$$\Delta w_{ji} = \alpha \cdot \sigma_i \cdot z_j; \Delta w_{0i} = \alpha \cdot \sigma_i.$$

Величина  $\sigma_i$  відправляється нейронам попереднього шару.

**Крок 7.** Кожний нейрон внутрішнього шару сумує вхідні від нейронів в наступному шарі помилки  $\sigma_i$  і вираховує величину помилки, помножуючи отримане значення на похідну активуючої функції.

Обчислюючи зміни вагів зв'язків між нейронами суміжних зв'язків згідно виразу:

$$\Delta w_{ji} = \alpha \cdot \sigma_i \cdot z_j; \Delta w_{0i} = \alpha \cdot \sigma_i.$$

**Крок 8.** Кожен нейрон змінює ваги своїх зв'язків з елементами зміщення і нейронами попереднього шару:

$$w_{ji} = w_{ji} + \Delta w_{ji}.$$

**Крок 9.** Кінцевий ранг ОР за допомогою виразу

$$r_i = |y_1 \ y_2 \ \dots \ y_n| \times |c_1 \ c_2 \ \dots \ c_n|^T,$$

де  $c_i$  – коефіцієнти які характеризують кількісну міру відповідних характеристик множини  $S$ .

**Приклад реалізації методики.** Автоматизація процесу ранжування ДРВ виконана шляхом використання програмного забезпечення, який реалізує розроблену методику. Фрагмент даних, який визначає функції належності аргументів нечіткої мережі до елементів множини  $S$ , наведено в табл. 1.

Таблиця 1

Фрагмент значення функцій приналежності  $\mu$ , для аргументів  $x_1, x_2, x_3, x_4, x_5, x_6$

$x_1$	$\mu_1$	$\mu_2$	$\mu_3$	$x_2$	$\mu_1$	$\mu_2$	$\mu_3$	$x_3$	$\mu_1$	$\mu_2$	$\mu_3$
10,00	0,92	0,06	0,02	1,80	0,00	0,11	0,89	0	0,00	0,04	0,96
50,00	0,80	0,15	0,05	2,13	0,01	0,11	0,88	9	0,03	0,05	0,95
100,0	0,70	0,22	0,08	2,46	0,02	0,10	0,88	18	0,15	0,10	0,75
122,1	0,68	0,23	0,09	2,79	0,04	0,10	0,86	27	0,15	0,31	0,54
$x_4$	$\mu_1$	$\mu_2$	$\mu_3$	$x_5$	$\mu_1$	$\mu_2$	$\mu_3$	$x_6$	$\mu_1$	$\mu_2$	$\mu_3$
700	0,01	0,10	0,89	0,9	0,01	0,09	0,90	7,0	0,01	0,10	0,89
600	0,02	0,13	0,85	0,8	0,10	0,25	0,65	7,4	0,02	0,13	0,85
500	0,03	0,17	0,80	0,7	0,15	0,33	0,52	7,8	0,03	0,17	0,80
450	0,04	0,22	0,74	0,6	0,21	0,54	0,25	8,2	0,04	0,22	0,74

В табл. 1 кожна характеристика ДРВ визначається четвіркою значень  $\mu_1, \mu_2, \mu_3, \mu_4$ . Де  $x$  – величина характеристики,  $\mu_i$  – функція належності величини  $x$  до  $i$  джерела множини. Навчасма вибірка нейронної мережі визначена на

множині ОР, які характеризуються вектором виду  $o = (x_1, x_2, x_3, x_4, x_5, x_6, c_1, c_2, c_3)$ .

Фрагмент навчасмої вибірки нечіткої нейронної мережі наведений в табл. 2.

Таблиця 2

Фрагмент навчасмої вибірки нечіткої нейронної мережі

$x_1$	$x_2$	$x_3$	$x_4$	$x_5$	$x_6$	$\mu_1$	$\mu_2$	$\mu_3$
600	1,8	0	200	0,85	7,0	0,01	0,10	0,89
600	1,8	10	200	0,85	7,0	0,01	0,24	0,75
600	3,0	0	200	0,85	7,0	0,01	0,24	0,75
600	1,8	0	200	0,65	7,0	0,1	0,3	0,6
600	1,8	0	200	0,85	11,0	0,01	0,20	0,79
600	1,8	0	300	0,85	7,0	0,01	0,35	0,64
300	1,8	0	200	0,85	7,0	0,01	0,10	0,89

На основі аналізу розрахованих вище даних, можемо зробити висновок про те що, використання нечіткої нейронної мережі дозволяє реалізувати відображення  $f(h_k) \rightarrow w_k$  з високим ступенем достовірності одержаних результатів – середньоквадратична помилка навчання нейронної мережі складає 3,9 пункта рагу ДРВ.

Таким чином, результати запропонованої методики, є достовірними і можуть бути використані в ході вирішення завдання планування спостереження за ДРВ.

### Висновки й перспективи подальших досліджень

Таким чином, розроблена методика враховує в роботі ранжування ДРВ, що виконуються в рамках планування застосування засобів розвідки, фактори, впливаючі на умови викриття ДРВ і РЕО.

Використання математичного апарату нечітких штучних нейронних мереж дозволяє враховувати

наслідки застосування засобів розвідки для спостереження за ОР через функціонування ДРВ в ході планування розвідки, застосовувати принципи ранжування ДРВ під умови РЕО, динамічно змінюються.

Запропонована методика реалізовує комплексний підхід до вирішення завдання ранжування ДРВ, та забезпечує досягнення потрібного ступеня результативності процесу функціонування системи РЕР в різних умовах РЕО.

Напрямами подальших досліджень, з врахуванням проведеного в рамках дослідження експерименту бачиться, в можливості її інтеграції в існуюче розвідувально-інформаційне забезпечення, для підвищення оперативності планування збору і обробку розвідувальної інформації про ОР та ДРВ.

### Література

1. Гаценко С. С. Методика раціонального розподілу розвідувальної інформації за важливістю та кількістю розвідувальних ознак в умовах невизначеності: Збірник наукових праць НДІ ГУР Міністерства оборони України, 2017. № 43. С. 111–120. 2. Гаценко С. С. Інформаційна система оцінювання оперативної обстановки в умовах невизначеності: К.: НУОУ, 2017. № № 1 (140), С. 157–165. 3. Шуренок В. А. Методика оцінки космічної обстановки на базі нечіткої логіки: Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2003. С. 191–203. 4. Гребенюк О. П. Застосування системно-когнітивного аналізу для автоматизації управління системою радіомоніторингу / О. П. Гребенюк, М. А. Роговець, В. А. Шуренок // Вісник ЖДТУ / Технічні науки. – 2010. - № 1 (52). – С. 72 – 80. 5. Шуренок В.А., Дзюбчук Р.В., Роговець М.А. Інформаційна система підтримки прийняття рішення оцінювання радіоелектронної обстановки на командних пунктах частин та підрозділів особливого призначення в умовах невизначеності на основі концепції „м'яких обчислень”. Труды академії. – Київ: Національна Академія оборони України. 2006, № 71. с. 50-58. 6. Тэррано Т., Аса и К.. Сугено М. Прикладные нечеткие системы. - М.: Мир, 1993. -368 с. 7. Гилл Ф., Мюррей У..

Райт М. Практическая оптимизация: мер. с англ. - М.: Мир, 1985. 509 с. 8. Круглов В.В., Борисов В.В. Искусственные нейронные сети. Теория и практика. – М Горячая линия - Телеком, 2002. - 382 с. 9. Пермяков О. Ю. Теоретические основы обработки нечетких данных в аналитических задачах специального математического обеспечения: Дисс. на соис. уч. степени д. т. н. К.: 1995. 198 с. 10. Гаценко С. С. Зуйко В. В., Зотов С. В. Методика вироблення та надання рекомендацій в умовах невизначеності та суперечливості розвідувальної інформації: Збірник наукових праць ЦНДІ ОБТ ЗСУ. 2016. №3(62). С. 12–23. 11. Method of integral estimation of channel state in the multiantenna radio communication systems S. Kalantaievskia. H. Pievtsov, A. Kuvshynov, S. Hatsenko, A. Shyshatskyi, S. Yarosh, S. Zubrytskyi, R. Zhyvotovskyl, S. Petruk, V. Zulko Eastern-european journal of enterprise technologies. Vol. 5, No 9 (95) pp. 60-76, 2018: Information and controlling system. 12. Method of Immunity Minimization of the Free Platform ed Inertial Navigation System of Unmanned Aircrafts R. Bieliakov, S. Hatsenko, O. Fesenko, R. Zhyvotovskiyi, S. Petruk, 2nd Ukraine Conference on Electrical and Computer Engineering Lviv, Ukraine, July 2-6, pp. 803-808, 2019.

## МЕТОДИКА РАНЖУВАННЯ ДЖЕРЕЛ РОЗВІДУВАЛЬНИХ ВІДОМОСТЕЙ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ ПРИ ОРГАНІЗАЦІЇ І ВЕДЕННІ РОЗВІДКИ

Сергей Станиславович Гаценко (кандидат технических наук)

Олег Владимирович Костенко

Виктор Петрович Кузьменко

Василий Михайлович Мазуренко

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье предлагается решение актуальной научной задачи разработки научно-методического аппарата ранжирования источников разведывательных сведений, характеризующих объекты разведки при оценке оперативной обстановки и радиоэлектронной обстановки в интересах планирования разведки. Ранг источники разведывательных сведений рассчитывается с учетом его качественных и количественных характеристик. Функционирование зависимости ранга источники разведывательных сведений от его разведывательной ценности и отождествляемых с ними радиоэлектронной обстановкой реализуется нечеткой нейронной сетью. Результатом выполнения процедуры ранжирования является введение на множестве источников разведывательных сведений планируемых отношение порядке. Упорядочение

множества источников разведывательных сведений позволяет формализовать и решить задачу квазиоптимального распределения средств и сил разведки.

**Ключевые слова:** ранжирование, источники разведывательных сведений, объект разведки, планирования разведки, нечеткие множества, применение сил и средств разведки.

## METHODS OF ORGANIZING RESOURCES SOURCES OF RADIO ELECTRONIC INTELLIGENCE IN ORGANIZATION AND EXERCISE

*Serhii Hatsenko (Candidate of technical sciences)*

*Oleh Kostenko*

*Viktor Kuzmenko*

*Vasyl Mazurenko*

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

The article proposes a solution to the urgent scientific task of developing a scientific and methodological apparatus for ranking intelligence sources that characterize intelligence objects in assessing the operational situation and the electronic environment in the interests of intelligence planning. The rank of intelligence sources is calculated taking into account its qualitative and quantitative characteristics. The functioning of the dependence of the rank of sources of intelligence on its intelligence value and the radio-electronic environment that is associated with them is realized by a fuzzy neural network. The result of the ranking procedure is the introduction on a variety of sources of intelligence information of the planned relationship order. Streamlining the many sources of intelligence allows us to formalize and solve the problem of quasi-optimal distribution of intelligence assets and forces.

**Key words:** ranking, sources of intelligence, reconnaissance object, intelligence planning, fuzzy sets, the use of intelligence forces.

### References

- Gaczenko S. S.** Metodika raczi'onal'nogo rozpodu rozvi'doval'noyi i'nformaczi'yi za vazhlivi'styu ta ki'l'ki'styu rozvi'doval'nikh oznak v umovakh neviznachenosti': Zbi'rnik naukovikh prac' NDI' GUR Mi'ni'sterstva obroni Ukraini, 2017. # 43. S. 111–120.
- Gaczenko S. S.** I'nformaczi'jna sistema oczi'nyuvannya operativnoyi obstanovki v umovakh neviznachenosti': K.: NUOU, 2017. # 1 (140), S. 157–165.
- Shurenok V. A.** Metodika oczi'nki kosmi'chnoyi obstanovki na bazi' nechit'koyi logi'ki: Zbi'rnik naukovikh prac' Vi's'kovogo i'nstitutu Kiyivs'kogo naczi'onal'nogo uni'versitetu i'meni Tarasa Shevchenka. 2003. S. 191–203.
- Grebenyuk O. P.** Zastosuvannya sistemno-kognitivnogo analizu dlya avtomatizaczi'yi upravli'nnya sistemoyu radi'omoni'toringu / O. P. Grebenyuk, M. A. Rogovecz', V. A. Shurenok // Vi'snik ZhDTU / Tekhni'chni nauki. – 2010. # 1 (52). – S. 72 – 80.
- Shurenok V.A., Dzyubchuk R.V., Rogovecz' M.A.** I'nformaczi'jna sistema pi'dtrimki priinyattya ri'shennya oczi'nyuvannya radi'oelektronnoyi obstanovki na komandnikh punktakh chastin ta pi'drozdi'li v osoblivogo priznachennya v umovakh neviznachenosti' na osnovi koncepczi'yi „m'yakikh obchislen'". Trudi akademi'yi. – Kiyiv: Naczi'onal'na Akademi'ya obroni Ukraini. 2006, # 71. s. 50-58.
- Te'ranov T., Asa i K., Sugeno M.** Prikladny'e nechetkie sistemy'. - M.: Mir,1993. -368 s.
- Gill F., Myurrej U., Rajt M.** Prakticheskaya optimizacziya: mer. s angl. - M.: Mir, 1985. 509 s.
- Kruglov V.V., Borisov V.V.** Iskusstvenny'e neyronny'e seti. Teoriya i praktika. – M Goryachaya liniya - Telekom, 2002. - 382 s.
- Permyakov O. Yu.** Teoreticheskie osnovy obrabotki nechetkikh danny'kh v analiticheskikh zadachakh speczial'nogo matematicheskogo obespecheniya: Diss. na sois. uch. stepeni d. t. n. K.: 1995. 198 s.
- Gaczenko S. S., Zujko V. V., Zotov S. V.** Metodika viroblyennya ta nadannya rekomendaczi'j v umovakh neviznachenosti' ta superechlivosti' rozvi'doval'noyi i'nformaczi'yi: Zbi'rnik naukovikh prac' CzNDI' OVT ZSU. 2016. # 3 (62). S. 12–23.
- Method of integral estimation of channel state in the multiantenna radio communication systems** S. Kalantaievska, H. Pievtsov, A. Kuvshynov, S. Hatsenko, A. Shyshatskyi, S. Yarosh, S. Zubrytskyi, R. Zhyvotovskiy, S. Petruk, V. Zulko Eastern-european journal of enterprise technologies. Vol. 5, No 9 (95) pp. 60-76, 2018: Information and controlling system.
- Method of Immunity Minimization of the Free Platform ed Inertial Navigation System of Unmanned Aircrafts** R. Bieliakov, S. Hatsenko, O. Fesenko, R. Zhyvotovskiy, S. Petruk, 2nd Ukraine Conference on Electrical and Computer Engineering Lviv, Ukraine, July 2-6, rr. 803-808, 2019.

*Олександр Валерійович Крайнов (кандидат технічних наук, доцент)*

*Марина Федорівна Маланчук (кандидат економічних наук)*

*Роман Іванович Грозовський*

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

## МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ

*Питання безпеки інформації – важлива частина концепції впровадження нових інформаційних технологій в військову справу. “Той, хто володіє достовірною і повною інформацією, – той володіє ситуацією, а той, хто володіє ситуацією, – той здатен управляти нею у своїх інтересах, а той, хто здатен управляти, – той здатен перемагати”. Тому захист інформації у інформаційному середовищі органів управління військами на теперішній час є дуже актуальною проблемою, яка потребує свого вирішення.*

*Захист інформації в органах військового управління має низку особливостей порівняно з загальновідомими концепціями. Це обумовлено, з одного боку, специфікою роботи штабів, як носіїв таємниць державного та військового характеру, з іншого – типовим організаційно-штатною структурою з відповідними їй постійними чітко встановленими функціями. Сучасна концепція інформаційної війни також передбачає широке використання спеціальних засобів боротьби в інформаційному просторі. Це і обумовлює актуальність проблеми захисту інформації.*

*Ключові слова: автоматизована інформаційна система; інформаційно-аналітичне забезпечення; орган військового управління; ефективність.*

### Вступ

**Постановка проблеми.** Комплексна система захисту інформації (КСЗІ) є сукупністю методів і засобів, об'єднаних єдиним цільовим призначенням, які забезпечують необхідну ефективність захисту інформації в автоматизованих інформаційних системах (АІС) органів військового управління.

Комплексність системи захисту інформації досягається охопленням всіх можливих загроз і узгодженням між собою різнорідних методів і засобів, що забезпечують захист всіх елементів АІС [3].

При побудові комплексної системи захисту інформації (КСЗІ) виділяють дві групи вимог до захищеності АІС [1,2], які повинні враховуватися – формалізовані вимоги і вимоги, які формулюються на підставі існуючої статистики загроз. Неможливість в загальному випадку формалізувати вимоги другої групи не дозволяє і формалізувати порівняльний аналіз систем захисту, віднесених до одного класу захищеності (відповідно до класифікації нормативних документів).

Зокрема, дві системи захисту, віднесені до одного класу захищеності, можуть принципово розрізнятися за своїми можливостями. При цьому необхідно відзначити, що у разі передбачуваної ідентичності реалізації формалізованих вимог, для них найважливішою характеристикою стає рівень кваліфікації їх розробників.

Припущення ідентичності звичайно не відповідає дійсності, оскільки в нормативних документах не вказується, яким способом повинен бути реалізований кожний механізм захисту. Тому існуючі системи додаткового захисту, віднесені до одного класу захищеності, принципово розрізняються і в реалізації формалізованих вимог. Питання оцінки ефективності і питання проектування КСЗІ тісно пов'язані, оскільки в їх основі лежить єдиний математичний апарат рішення відповідної оптимізаційної задачі.

**Аналіз остатніх досліджень і публікацій.** Проблематиці захисту інформації в АІС приділяють увагу багато вчених як в Україні, так і за кордоном. Особливо гостро на сьогодні, з урахуванням умов постійної конкуренції не лише між недержавними структурами, а і структурами, які містять державні інформаційні ресурси, точиться боротьба за інформацію. Тому її захист завжди актуальний. Принципи побудови КСЗІ, загальні принципи інформаційної безпеки в АІС розглядали такі фахівці у сфері захисту інформації, як В. М. Богуш, М. В. Грайворонський, О. А. Довидьков, В. Г. Кривуца, В. Ф. Шаньгин, О. Г. Корченко, Г. Ф. Конахович, В. Г. Грибунін та інші вчені.

Таким чином, метою статті є удосконалення науково-методичного апарату оцінювання ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління.

**Виклад основного матеріалу дослідження**

Розглянемо загальний підхід щодо оцінки ефективності КСЗІ та визначимо критерії і параметри оптимальної системи захисту.

Оцінку захищеності системи  $Z$  будемо здійснювати кількісно залежно від вартості інформації, що захищається, ймовірності злому, вартості КСЗІ, продуктивності системи:

$$Z = f(C_{\text{інф}}, P_{\text{взл}}, C_{\text{КСЗІ}}, \Pi),$$

де:  $C_{\text{інф}}$  – вартість інформації;

$P_{\text{взл}}$  – ймовірність взлому;

$C_{\text{КСЗІ}}$  – вартість КСЗІ;

$\Pi$  – продуктивність системи.

Оптимізаційна задача полягає в функції вартості інформації при забезпеченні максимального рівня захищеності (якщо захищається і ймовірність злому) при мінімальній вартості системи захисту і мінімальному впливу її на продуктивність системи:

$$Z^{\text{opt}} = \max Z(C_{\text{інф}}, P_{\text{взл}}, C_{\text{КСЗІ}}, \Pi)$$

При цьому слід зазначити, що крім необхідного забезпечуваного рівня захищеності, повинен враховуватися ще ряд досить суттєвих характеристик системи. Наприклад, обов'язково повинен враховуватися вплив КСЗІ на завантаження обчислювального ресурсу об'єкту, що захищається.

На практиці найбільш часто оцінка рівня захищеності проводиться використовуючи теорію ризиків. Ризик ( $R$ ) – це потенційні втрати від загроз захищеності:

$$R(p) = C_{\text{інф}} P_{\text{взл}}.$$

По суті, параметр ризику тут вводиться як мультиплікативна згортка двох основних параметрів захищеності.

З другого боку, можна розглядати ризик як втрати в одиницю часу:

$$R(\lambda) = C_{\text{інф}} \lambda_{\text{взл}}$$

де:  $\lambda_{\text{взл}}$  – інтенсивність потоку зломів (під зломом розуміємо вдалу спробу несанкціонованого доступу до інформації).

Ці дві формули пов'язані наступним співвідношенням:

$$P_{\text{взл}} = \frac{\lambda_{\text{взл}}}{\Lambda},$$

де:  $\Lambda$  – загальна інтенсивність потоку несанкціонованих спроб доступу зловмисника до інформації.

Розглянемо основний критерій захищеності та загальне рішення задачі проектування оптимальної КСЗІ.

В якості основного критерію захищеності можна використовувати коефіцієнт захищеності ( $D$ ), що показує відносне зменшення ризику в

захищеній системі в порівнянні з незахищеною системою.

$$D = \left( 1 - \frac{R_{\text{зах}}}{R_{\text{незах}}} \right) \times 100\% \quad (1)$$

де:  $R_{\text{зах}}$  – ризик в захищеній системі;

$R_{\text{незах}}$  – ризик в незахищеній системі.

Таким чином, в даному випадку задача оптимізації виглядає таким чином:

$$\begin{cases} D(C_{\text{інф}}, P_{\text{взл}}) \rightarrow \max; \\ C_{\text{КСЗІ}} \rightarrow \max; \\ \Pi_{\text{КСЗІ}} \rightarrow \max. \end{cases}$$

Для вирішення цієї задачі зведемо її до однокритеріальної за допомогою введення обмежень. В результаті отримаємо:

$$\begin{cases} D(C_{\text{інф}}, P_{\text{взл}}) \rightarrow \max; \\ C_{\text{КСЗІ}} \leq C_{\text{зад}}; \\ \Pi_{\text{КСЗІ}} \geq \Pi_{\text{зад}}. \end{cases}$$

де:  $C_{\text{зад}}$  і  $\Pi_{\text{зад}}$  – задані обмеження на вартість КСЗІ та продуктивність системи.

Цільова функція вибрана виходячи з того, що саме вона відображає основне функціональне призначення системи захисту – забезпечення безпеки інформації.

Продуктивність системи  $\Pi_{\text{КСЗІ}}$  розраховується із застосуванням моделей і методів теорії масового обслуговування і теорії розкладів (залежно від того, захищається система оперативної обробки чи реального часу). На практиці можливо завдання обмеження по продуктивності (вплив на завантаження обчислювального ресурсу системи, що захищається) не безпосередньо у вигляді необхідної продуктивності системи, а як зниження продуктивності ( $d\Pi_{\text{КСЗІ}}$ ) АІС від встановлення системи захисту. В цьому випадку задача оптимізації виглядатиме таким чином:

$$\begin{cases} D(C, p) \rightarrow \max; \\ C_{\text{КСЗІ}} \rightarrow \min; \\ d\Pi_{\text{КСЗІ}} \rightarrow \min, \end{cases}$$

або після зведення її до однокритерійної:

$$\begin{cases} D(C, p) \rightarrow \max; \\ C_{\text{КСЗІ}} \leq C_{\text{зад}}; \\ d\Pi_{\text{КСЗІ}} \leq d\Pi_{\text{зад}}, \end{cases}$$

де:  $C_{\text{зад}}$  і  $d\Pi_{\text{зад}}$  – задані обмеження на вартість КСЗІ і зниження продуктивності.

Саме такий принцип зведення задачі до однокритеріальної доцільний, оскільки в будь-якому технічному завданні на розробку КСЗІ вказується, якою мірою система захисту буде впливати на продуктивність системи. Як правило, впровадження системи захисту не повинне знижувати продуктивність системи більш ніж на 10%. Крім того, звичайно вводиться обмеження на



вартість системи захисту.

Якщо розраховане значення коефіцієнта захищеності  $D$  не задовольняє вимогам до системи захисту, то в допустимих межах можна змінювати задані обмеження і вирішити задачу методом послідовного вибору уступок. При цьому задається приріст вартості і зниження продуктивності:

$$C_{\text{зад}}^* = C_{\text{зад}} \Delta C,$$

$$C_{\text{зад}}^* = C_{\text{зад}} - \Delta C, \text{ або } C_{\text{зад}}^* = dC_{\text{зад}} + \Delta dC.$$

У такому вигляді задача розв'язується внаслідок реалізації ітераційної процедури шляхом відсіювання варіантів, що не задовольняють обмежувальним умовам, і подальшому вибору з тих, що залишилися варіанту з максимальним коефіцієнтом захищеності.

Визначимо коефіцієнт захищеності через параметр загроз. В цих умовах задаємо наступні величини:

$\omega$  – кількість видів загроз, що впливають на систему;

$C_i$  – вартість (втрати) від злому  $i$ -того виду;

$\lambda_i$  – інтенсивність потоку зломів  $i$ -того виду, відповідно;

$Q_i$  – ймовірність появи загроз  $i$ -того виду в загальному потоці спроб несанкціонованого доступу до інформації:

$$Q_i = \frac{\lambda_i}{\Lambda};$$

$P_i$  – ймовірність відбиття загроз  $i$ -того виду системою захисту.

Відповідно, коефіцієнт втрат від зломів системи захисту визначається:

$$R(p) = \sum_1^{\omega} R_i(p) = \sum_1^{\omega} C_i P_{\text{взл}_i}$$

де:  $R_i(p)$  – коефіцієнт втрат від злomu  $i$ -того типу та показує, які в середньому втрати припадають на один злом  $i$ -того типу.

Для незахищеної системи  $R_{\text{загр}_i} = Q_i$ , для захищеної системи  $R_{\text{загр}_i} = Q_i(1 - p_i)$ .

Коефіцієнт втрат від зломів системи захисту в одиницю часу відповідно визначається:

$$R_i(\lambda) = \sum_1^{\omega} R(\lambda) = \sum_1^{\lambda} C_i \lambda_{\text{взл}_i}$$

де:  $R_i(\lambda)$  – коефіцієнт втрат від зломів  $i$ -того типу в одиницю часу.

Для незахищеної системи  $\lambda_{\text{загр}_i} = \lambda_i$ ; для захищеної системи  $\lambda_{\text{загр}_i} = \lambda_i(1 - p_i)$ .

Відповідно, з (1) маємо:

$$D = 1 - \frac{\sum_1^{\omega} C_i Q_i (1 - p_i)}{\sum_1^{\omega} C_i Q_i} = 1 - \frac{\sum_1^{\omega} C_i \lambda_i (1 - p_i)}{\sum_1^{\omega} C_i \lambda_i}.$$

Якщо у якості вихідних параметрів задана ймовірність появи загроз  $Q_i$ , тоді коефіцієнт захищеності зручно рахувати через ймовірності появи загроз. Якщо ж в якості вихідних параметрів задані інтенсивності потоків загроз  $\lambda_i$ , тоді коефіцієнт захищеності рахується через інтенсивність.

### Висновки й перспективи подальших досліджень

Загрози інформаційному простору не залишаються незмінними в часі. Бурхливий розвиток інформаційних технологій та засобів обробки та удосконалення систем захисту аналогічно впливає і на розвиток засобів атак та удосконалення методів їх проведення. Свідченням цього є постійний ріст кількості загроз вірусного характеру в глобальній мережі. Це вимагає створення динамічних систем захисту адаптивних відповідно змін зовнішнього оточення інформаційних систем.

В сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в умовах ведення бойових дій.

В умовах сучасної інформаційної та кібервійни, яка ведеться проти нашої країни, забезпечення безпеки АІС органів військового управління має стати державним завданням.

інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

### Література

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. Санкт-Петербург: Наука и техника, 2004.-384с. 2. Мельников В.А. Защита информации в компьютерных системах. М.: Финансы и статистика: Электроинформ, 1997.-368с. 3. Захист

**МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ  
ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ  
ВОЕННОГО УПРАВЛЕНИЯ**

*Александр Валериевич Крайнов (кандидат технических наук, доцент)*

*Марина Федоровна Маланчук (кандидат экономических наук)*

*Роман Иванович Грозовский*

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

*Вопрос безопасности информации - важная часть концепции внедрения новых информационных технологий в военном деле. "Тот, кто владеет достоверной и полной информацией - тот владеет ситуацией, а тот, кто владеет ситуацией, - тот способен управлять ею в своих интересах, а тот, кто способен управлять, - тот способен побеждать". Поэтому защита информации в информационной среде органов управления войсками в настоящее время является очень актуальной проблемой, требующей своего решения.*

*Защита информации в органах военного управления имеет ряд особенностей по сравнению с общеизвестными концепциями. Это обусловлено, с одной стороны, спецификой работы штабов, как носителей тайн государственного и военного характера, с другой - типичным организационно-штатной структуре с соответствующими ней постоянными установленными функциями. Современная концепция информационной войны также предусматривает широкое использование специальных средств борьбы в информационном пространстве. Это и обуславливает актуальность проблемы защиты информации.*

**Ключевые слова:** *автоматизированная информационная система; информационно-аналитическое обеспечение; орган военного управления; эффективность.*

**METHODOLOGY FOR ESTIMATING THE EFFECTIVENESS OF AN INTEGRATED INFORMATION  
PROTECTION SYSTEM FOR AUTOMATED INFORMATION SYSTEMS OF MILITARY  
MANAGEMENT BODIES**

*Oleksandr Krainov (Candidate of technical sciences, associate professor)*

*Maryna Malanchuk (Candidate of Economic Sciences)*

*Roman Hrozovskyi*

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

*The issue of information security is an important part of the concept of introducing new information technologies in military affairs. "The one who possesses reliable and complete information - the one who owns the situation, and the one who owns the situation - that is able to manage it in his own interests, and the one who is able to manage - that is able to win." Therefore, the protection of information in the information environment of military command and control agencies is currently a very urgent problem that needs to be addressed.*

*Information security in military command and control has a number of features compared to well-known concepts. This is due, on the one hand, to the specifics of the work of staffs as carriers of state and military secrets, and on the other, to a typical organizational and staff structure with corresponding permanent functions. The modern concept of information warfare also provides for the widespread use of special means of combat in the information space. This determines the urgency of the problem of information security.*

**Key words:** *automated information system; information and analytical support; military command body; efficiency.*

**References**

1. Scheglov A.Yu. *Zaschita kompyuternoy informatsii ot nesanksionirovannogo dostupa*. Sankt-Peterburg: Nauka i tehnika, 2004.-384s. 2. Melnikov V.A. *Zaschita informatsii v kompyuternyih sistemah*. M.: Finansy i statistika: Elektroinform, 1997.-368s. 3. *Zakhyst informacii v avtomatyzovanykh systemakh upravlinnja : navchalnyj posibnyk / Uklad. I. A. Piljkevych, N. M. Lobanchykova, K. V. Molodecjka. – Zhytomyr : Vyd-vo ZhDU im. I. Franka, 2015. – 226 s.*

*Валерій Володимирович Кузнецов (кандидат військових наук)*

*Олексій Васильович Повещенко*

*Ігор Святославович Оксенчук*

*Віктор Павлович Ніколаєнко*

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

## УДОСКОНАЛЕНА МЕТОДИКА РАЦІОНАЛЬНОГО РОЗПОДІЛУ ІНФОРМАЦІЇ ЗА ВАЖЛИВІСТЮ І КІЛЬКІСТЮ ДЖЕРЕЛ РАДІОМОНІТОРИНГУ В АСУ ВІЙСЬКАМИ ТА ЗБРОЄЮ

При проектуванні автоматизованих систем управління військами та зброєю важлива роль відводиться формі та об'єму інформації, що передається. Інформація в контур управління надходить від датчиків, що складають систему моніторингу, і ведуть безперервне спостереження за джерелами та об'єктами моніторингу.

Система управління та зв'язку групового об'єкту радіомоніторингу являє собою складну ієрархічну структуру. Кількість джерел, які функціонують в інтересах забезпечення системи управління перевищує кількість наявних сил та засобів, що здійснюють радіомоніторинг. Виникає невідповідність при розпізнаванні об'єктів та джерел радіомоніторингу: час ідентифікації об'єкту спостереження, кількість ознак. Тому необхідно розв'язати багатокритеріальну оптимізаційну задачу для ідентифікації режиму функціонування джерел радіомоніторингу для гарантованого визначення стану системи управління та зв'язку групового об'єкту радіомоніторингу, яка полягає у виборі тих джерел корисність яких найбільша.

Запропонована методика раціонального розподілу інформації в АСУ військами та зброєю, за рахунок відбору найбільш важливих джерел радіомоніторингу і раціоналізації кількості градацій об'єктів радіомоніторингу для забезпечення заданої ймовірності правильного розпізнавання та гарантованого визначення їх стану.

**Ключові слова:** автоматизована система управління; розпізнавання; ідентифікація; джерела та об'єкти; радіомоніторинг; розподіл інформації.

### Вступ

**Постановка проблеми.** Розпізнавання – основа інформаційної технології, що являє собою перетворення вхідної інформації (деякі показники, параметри, ознаки образів, об'єктів) у вихідну, представлену висновком про те, до якого класу відноситься розпізнаваний образ [1].

Сутність процесу розпізнавання в системі радіомоніторингу полягає у викритті об'єктів радіомоніторингу (оперативних ситуацій, образів) за працюючими джерелами радіомоніторингу та представленні інформації в контур управління про стан, наміри, задуми і можливості. Об'єкти, що розпізнаються визначаються ознаками [1].

З [1, 2] відомо, що зі збільшенням кількості ознак, які характеризують об'єкт збільшуються час необхідний для його ідентифікації та інші затрати, в першу чергу апаратні, в наслідок чого знижується оперативність процесу розпізнавання.

**Аналіз останніх досліджень і публікацій.** Аналіз існуючих методик визначення важливості джерел радіомоніторингу (ДРМ) для спостереження показав, що в цілому вони дозволяють здійснювати необхідний вибір але мають наступні недоліки [3-6]:

відсутність аналітичної моделі визначення важливості різних видів ДРМ;

врахування лише одного або невеликої частини об'єктивних факторів, що впливають на процес

вибору ДРМ для спостереження;

використання методик лише в умовах повної визначеності апріорної інформації щодо ДРМ та режимів їх функціонування;

залежність визначення важливості ДРМ від суб'єктивного досвіду та професійної підготовки особи, яка приймає рішення (необхідність врахування емпіричного коефіцієнту важливості);

неможливість динамічної зміни обраних ДРМ при зміні умов обстановки.

**Мета статті.** З метою усунення викладених недоліків в [7, 8], запропоновано удосконалення методики раціонального розподілу інформації за важливістю і кількістю джерел радіомоніторингу в АСУ військами та зброєю.

### Виклад основного матеріалу дослідження

Нехай ідентифікація станів об'єкту моніторингу (ОМ) здійснюється через систему управління та зв'язку (СУЗ). Позначимо множиною можливих станів СУЗ  $X$ , де  $x_1, x_2, \dots, x_n \in X$  – можливі стани які може приймати об'єкт. Зазначимо, що з погляду питання, яке розглядається, розуміння стану ОМ та режим функціонування СУЗ ОМ збігаються.

СУЗ визначається множиною розвідувальних ознак  $Y$ , де  $y_1, y_2, \dots, y_m \in Y$  – викриті

розвідувальні ознаки.

Отже необхідно обґрунтувати необхідну кількість ознак для гарантованої ідентифікації стану СУЗ.

Якість виконання плану радіомоніторингу має набір певних показників, що задаються. Показники планування якості радіомоніторингу: повнота охоплення спостереженням ОМ, витрати технічного ресурсу навантаження постів радіомоніторингу, ймовірність відстеження стану та характеру діяльності групового ОМ.

Необхідно максимізувати якість розподілу та обробки інформації при заданих вимогах до достовірності.

Обмеження, вплив метричних критеріїв є рівноцінним, тобто (немає залежності від метричних критеріїв).

Алгоритм раціонального розподілу інформації за важливістю і кількістю джерел радіомоніторингу в АСУ військами та зброєю на рисунку 1.

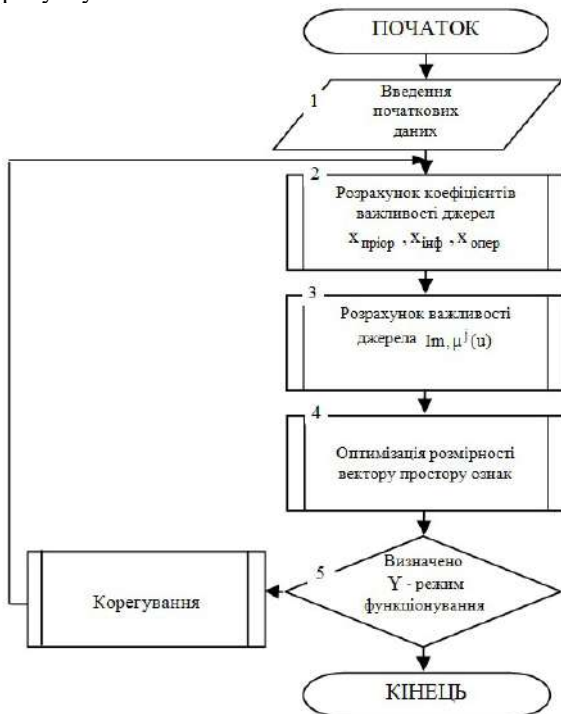


Рис. 1. Алгоритм раціонального розподілу інформації за важливістю і кількістю джерел радіомоніторингу

Для вибору варіанту плану радіомоніторингу (далі план) використовуються часткові показники якості планування радіомоніторингу [5-7]:

1. Повнота охоплення спостереженням ОМ  $\Pi$ , що розраховується як відношення суми коефіцієнтів важливості ОР  $Y_j$ , що включені в план, до суми коефіцієнтів важливості всіх ОМ:

$$\Pi = \frac{\sum_{j=1}^{\{m\}_u} Y_j}{\sum_{j=1}^J Y_j} \quad (1)$$

де:  $\{m\}_u$  – кількість ОР, вибрані для

спостереження в  $u$ -му плану.

2. Витрати технічного ресурсу навантаження постів, що визначається як сума витрат технічних ресурсів навантаження всіх постів  $S_{заг\text{РЕР}}$ .

3. Ймовірність відстеження стану та характеру діяльності усієї сукупності ОМ, що підлягають спостереженню –  $\bar{P}$ .

$$\bar{P} = \frac{1}{m} \sum_{j=1}^m P_j \quad (2)$$

де:  $P_j$  – ймовірність відстеження стану та характеру діяльності ОМ, що включені до плану.

Тоді система часткових показників якості вибору плану спостереженні за ОМ (ДРМ) буде мати вигляд:

$$\begin{cases} \Pi \rightarrow \max \\ S_{заг\text{РЕР}} \rightarrow \min \\ \bar{P} \rightarrow \max \end{cases} \quad (3)$$

З урахуванням системи часткових показників, функціонал, що відображає якість ведення моніторингу за умови вибору того чи іншого варіанту плану  $\Pi$ , можна записати у вигляді

$$F_{\Pi U_{\text{опт}}} = \max F(\Pi_{\Pi U}, S_{заг\text{РЕР}\Pi U}, \bar{P}_{\Pi U}) \quad (4)$$

Задача вибору варіанту плану спостереження відноситься до багатокритеріальних (векторних) задач. Рішення задач, що потребують векторної оптимізації, полягає у згортці окремих критеріїв якості у загальний критерій, та вибору такого варіанту рішення задачі, якому відповідало б найкраще значення загального критерію (максимальне чи мінімальне). Згортка часткових критеріїв якості до загального здійснюється з використанням певної схеми компромісів, яка визначає конкретний принцип оптимальності та стратегію дій особи, що приймає рішення [8, 9].

Однак в існуючих методах розподілу інформації за важливістю ДРМ розрахунок коефіцієнтів важливості здійснюється неявно (4), крім того, порядок їх розрахунку не визначено.

Отже, виникає актуальна наукове завдання багатокритеріальної оптимізації процесу вибору ДРМ з урахуванням їх важливості для підвищення ефективності ведення моніторингу.

Тоді (4) можна переписати у вигляді:

$$F_{\Pi U_{\text{опт}}} = \operatorname{argmax}_{im \in Im} F(Im, S_{заг\text{РЕР}\Pi U}, \bar{P}_{\Pi U}),$$

де:  $Im$  – вектор коефіцієнтів важливості (пріоритетності) ДРМ у зоні моніторингу;

$\bar{P}_{\Pi U}$  – ймовірність відстеження стану та характеру діяльності групового ОМ при виборі  $u$ -го плану спостереження.

В [8, 9] розглядаються підходи до вирішення задач багатокритеріальності і вибору альтернатив в техніці, застосовуючи математичний апарат теорії корисності, тому для розв'язання поставленого завдання пропонується скористатись відомими підходами.

Відповідно до [8] важливість ДРМ можна

розглядати як неметричний критерій корисності (НЧК). Основною складністю при розв'язанні поставленої задачі є представлення НЧК у кількісному вигляді з метою його подальшого введення до функції корисності (ФК).

Для представлення НЧК у кількісному вигляді визначені неметричні часткові критерії корисності (НЧКК), які мають характеризувати важливість ДРВ.

Відповідно [8, 9], основними НЧКК виступають ступінь пріоритетності задачі в інтересах якої ведеться моніторинг, або ступінь пріоритету ОМ ( $X_{\text{пріор}}$ ); ступінь інформативної цінності ( $X_{\text{інф}}$ ); ступінь оперативної цінності ОМ (ДРМ) ( $X_{\text{опер}}$ ).

У загальному випадку для кількісного представлення неметричних критеріїв використовується теорія експертного оцінювання. Головною причиною цього є відсутність іншого загального методу перетворення неметричних критеріїв у числові значення [8].

Позначимо  $Q(X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}})$ , як функцію корисності НЧКК.

$X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}$  незалежні системи величин. Тоді функції корисності НЧКК можна представити системою виразів

$$\begin{cases} \Psi_{\text{пріор}} = Q(X_{\text{пріор}})f(X_{\text{пріор}}), \\ \Psi_{\text{інф}} = Q(X_{\text{інф}})f(X_{\text{інф}}), \\ \Psi_{\text{опер}} = Q(X_{\text{опер}})f(X_{\text{опер}}), \end{cases} \quad (5)$$

де:  $f(X_{\text{пріор}})$ ,  $f(X_{\text{інф}})$ ,  $f(X_{\text{опер}})$  – функції залежності корисності від метричних критеріїв.

У свою чергу функція корисності ДРМ матиме вираз

$$\Psi = Q(X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}})f(X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}) \quad (6)$$

Для дослідження впливу неметричних критеріїв введемо обмеження, сутність якого полягає в тому, що вплив метричних критеріїв є рівноцінним, тобто (немає залежності від метричних критеріїв)

$$f(X_{\text{пріор}}) = f(X_{\text{інф}}) = f(X_{\text{опер}}) = 1 \quad (7)$$

Аналіз обмеження (7) показує, що показники між собою рівноцінні за метричним критерієм. В свою чергу функції залежності корисності від неметричних критеріїв змінюються за лінійним законом і визначаються нижнім і верхнім значенням прийнятих оцінок. Здійснивши операцію нормування за максимальним значенням, будь-яка перевага одного із показників виразу (7) за неметричним критерієм призведе до домінування функції корисності відповідного показника.

Враховуючи (7), вираз (6) буде представлений

$$\Psi = Q(X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}) \quad (8)$$

З метою вибору раціонального виду функції корисності  $Q(X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}})$  зручно представити  $X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}$  у вигляді нечітких

множин, а оцінки НЧКК, як їх елементи відповідно. Тоді  $Q(X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}})$  можна ототожнити з функцією належності набору вхідних значень показників основних НЧКК  $X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}$  до нечітких множин  $X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}$ , відповідно [10]. Таким чином, задачу визначення важливості ДРМ можна сформулювати як задачу прийняття рішення щодо важливості ДРМ, а результат процесу прийняття рішення можна представити у вигляді:

$$I_m = Q(X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}) \quad (9)$$

де:  $X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}$  – набір вхідних значень показників основних НЧКК;

$I_m$  – рішення щодо визначення важливості ДРМ.

Задача прийняття рішення щодо визначення важливості ДРМ полягає в тому, щоб на основі інформації про вектор вхідних показників ( $X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}$ ) визначити результат  $I_m$ . Необхідною умовою формального розв'язання поставленої задачі є наявність залежності (9). Для встановлення такої залежності необхідно розглядати вхідні показники (НЧКК) і вихідне рішення як лінгвістичні змінні, що задані на універсальних множинах [10, 11]:

Для оцінювання таких лінгвістичних змінних пропонується використовувати якісні терми, що складають терм-множину:

$$X_{\text{інф}} = \{Н, нС, С, вС, В\} \text{ – терм-множина змінної}$$

$X_{\text{інф}},$

$$X_{\text{опер}} = \{Н, нС, С, вС, В\} \text{ – терм-множина}$$

змінної  $X_{\text{опер}},$

$$X_{\text{пріор}} = \{Н, С, В\} \text{ – терм-множина змінної}$$

$X_{\text{пріор}},$

$$I_m = \{Н, нС, С, вС, В\} \text{ – терм-множина змінної}$$

$I_m,$

де Н, нС, С, вС, В – відповідно “низький”, “нижче середнього”, “середній”, “вище середнього”, “високий”;

$I_m$  – множина змінних, що характеризують важливість ДРМ.

$$X_{\text{інф}} = [1,5];$$

$$X_{\text{опер}} = [1,5];$$

$$X_{\text{пріор}} = [1,3];$$

$$I_m = [1,5]$$

(10)

Для оцінювання значень лінгвістичних змінних  $X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}$ , відповідно (10) використаємо наступну шкалу якісних термів.

У відповідності з методами когнітивної інженерії щодо синтезу бази знань, викладених в [10, 11] отримано бази знань, що характеризують важливість ДРМ. Використовуючи математичний апарат теорії нечітких множин базу знань перетворено в логічні рівняння

$$\mu^{Im_j}(X_{\text{пріор}}, X_{\text{інф}}, X_{\text{опер}}) = \max_j \left\{ \min_i \left[ \mu^j(X_{i(\text{пріор})}), \mu^j(X_{i(\text{інф})}), \mu^j(X_{i(\text{опер})}) \right] \right\}$$

$$\mu^j(Im_i) = \tilde{\mu}^j(u), u = 4 \frac{Im_i - Im}{Im - Im}, \quad (12)$$

$j = H, Hc, C, BC, B$

Таблиця 1

Числове значення важливості ДРВ (Im)	Лінгвістичне значення важливості ДРВ (Im)
12,2 ÷ 15	Висока
9,4 ÷ 12,2	Вища за середню
6,6 ÷ 9,4	Середня
3,8 ÷ 6,6	Нижче за середню
1 ÷ 3,8	Низька

Аналітична модель функції належності представлена виразом:

$$\mu^j(u) = \frac{1}{1 + \left(\frac{u-b}{c}\right)^2} \quad (13)$$

де параметри  $b$  і  $c$  задано в таблиці 2

Таблиця 2

Терм	H	Hc	C	BC	B
b	0	1	2	3	4
c	0,923	0,923	0,923	0,923	0,923

Графічне зображення ФН згідно з виразом (13) наведено на рисунку 2

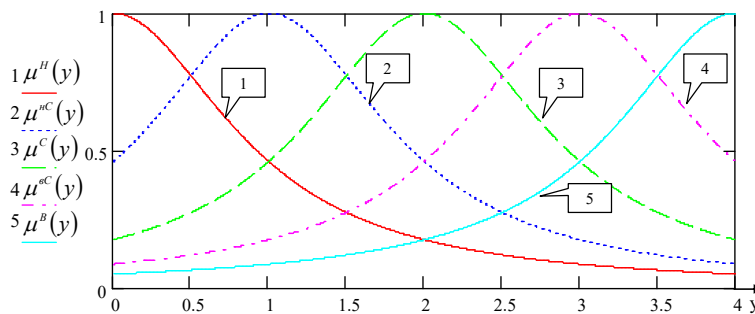


Рисунок 2 – Графічне зображення ФН нечіткої множини ступенів важливості ДРМ

**Розрахунок коеф. важливості (дія 2 рис. 1).** Визначаються коефіцієнт пріоритетності  $x_{\text{пріор}}$ , коефіцієнт ступеню інформативної цінності  $x_{\text{інф}}$ , коефіцієнт ступеню оперативної цінності  $x_{\text{опер}}$ .

**Розрахунок важливості ОМ (дія 3 рис. 1).** За допомогою (13) розраховуються значення важливості відповідного ОМ (ДРМ).

**Визначення лінгвістичного значення важливості ОМ (дія 4 на рис. 1)**

Користуючись таблицею 2 визначається лінгвістичне значення важливості ДРМ.

**Розглянемо приклад.** Нехай необхідно визначити важливість радіомережі управління та оповіщення деякого групового ОМ. Використовуючи викладене, користуючись таблицями визначаємо, що:

коефіцієнт пріоритетності  $x_{\text{пріор}}=3$ ;

коефіцієнт ступеню інформативної цінності  $x_{\text{інф}}=2$ ;

коефіцієнт ступеню оперативної цінності  $x_{\text{опер}}=3$ .

Підставляючи отримані дані до (13) отримуємо

значення важливості  $Im = 9$ . Використовуючи таблицю 3 визначаємо результат – “СЕРЕДНЯ”.

**Висновок:** дане ДРМ має “СЕРЕДНЮ” важливість.

**Оптимізація вектору розвідувальних ознак (дія 5 рис. 1)**

З [1, 2] відомо, що зі збільшенням кількості ознак, які характеризують ДРМ, збільшуються час необхідний для ідентифікації режиму його функціонування та інші затрати, в першу чергу апаратні, в наслідок чого знижується оперативність процесу оцінювання обстановки.

Нехай здійснюється оцінювання обстановки з метою викриття стану та характеру діяльності деякого складного ОМ. Припустимо, що стан бойової готовності ОМ асоціюється з режимом функціонування ДРМ, який забезпечує функціонування ОМ. Позначимо множину можливих станів ОМ, а отже і множину режимів функціонування ДРМ  $Y$ , де  $y_1, y_2, \dots, y_m \in Y$  – можливі стани ОМ.

Обстановка визначається множиною ознак  $X$ , де  $x_1, x_2, \dots, x_n \in X$  – викриті ознаки. Отже необхідно обґрунтувати необхідну кількість ознак

для ідентифікації режиму функціонування ДРМ.

В [1, 2] розглядаються методики розпізнання систем лише за умови, коли ймовірність станів складних систем відома. Таким чином, поставлена задача потребує розв'язання в умовах невизначеної ймовірності.

Виділення інформативних ознак у реальній обстановці є складним завданням, особливо при веденні радіомоніторингу систем радіозв'язку, коли набір ознак може бути дуже великим, а самі ознаки корельовані між собою. Тому постає завдання відбору й виділення групи найбільш інформативних ознак з метою зменшення розмірності вектора вихідних даних при одночасному знаходженні такої системи координат, у якій ймовірність правильного розпізнавання джерел або ОМ буде максимальною або достатньою для прийняття рішення.

Зменшення розмірності простору ознак в умовах великої кількості радіоелектронних засобів відіграє значну роль, оскільки збільшує пропускну спроможність засобів моніторингу у цілому. Досвід і теоретичні розрахунки показують, що зі збільшенням кількості ознак ймовірність ідентифікації режиму функціонування ДРМ збільшується. Однак, це справедливо тільки при відносно невеликій кількості ознак. Тому, що збільшення кількості ознак значною мірою призводить до збільшення похибок ідентифікації.

Залежність ймовірності ідентифікації ДРМ від розмірності простору ознак наведено на рис. 3.

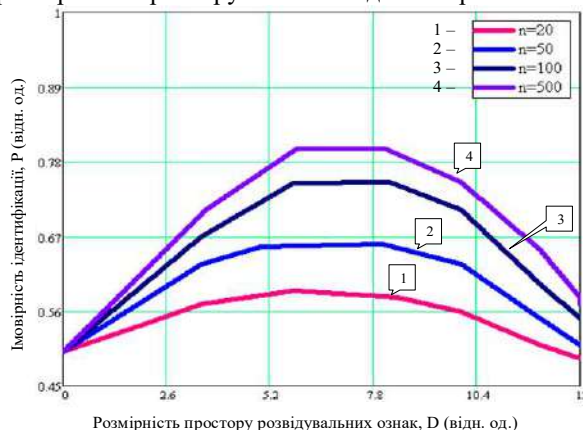


Рис. 3. Залежність ймовірності ідентифікації режиму функціонування ДРМ від розмірності простору ознак

З наведених графіків видно, що довільне збільшення розмірності простору ознак може призвести до погіршення ймовірності правильного розпізнавання.

Формування вектора ознак математично може бути представлено у вигляді:

$$Y = AX \quad (14)$$

де: X – вектор ознак;

Y – вектор можливих рішень;

A – матриця перетворень.

Для вирішення питання щодо визначення міри інформативності ознак і мінімізації їх простору скористаємось положенням теорії інформації К. Шеннона.

За Шенноном міру інформативності деякої ознаки щодо множини режимів функціонування ДРМ можна оцінити як різницю початкової ентропії ідентифікації режиму функціонування й ентропії рішення за певною ознакою

$$I_k = H_0(Y) - H(Y/x_k) \quad (15)$$

де:  $H_0(Y)$  – початкова ентропія ідентифікації;

$H(A/x_k)$  – ентропія рішення за ознакою  $x_k$ .

Припустимо, що в розглянутій предметній області ознак  $x_k$  може приймати J дискретних значень (градацій)  $x_k$  ( $j = 1, 2, \dots, J$ ).

Тоді ентропія рішення за j-м значенням ознаки  $x_k$  визначиться як

$$H(Y_m/x_{kj}) = -\sum_{i=1}^m p(Y_i/x_{kj}) \log p(Y_i/x_{kj}) \quad (16)$$

де:  $p(Y_i/x_{kj})$  – умовна ймовірність ідентифікації режиму функціонування  $Y_i$  за j-ю градацією ознаки  $x_k$ .

Умовна ймовірність за критерієм Баєса буде дорівнювати

$$p(Y_i/x_{kj}) = \frac{p(Y_i)p(x_{kj}/Y_i)}{p(x_{kj})} = \frac{p(Y_i)p(x_{kj}/Y_i)}{\sum_{i=1}^m p(Y_i)p(x_{kj}/Y_i)} \quad (17)$$

де:  $p(Y_i)$  – апіорна ймовірність режиму функціонування  $Y_i$  серед всіх m режимів;

$p(x_k)$  – ймовірність появи j-ї градації k-ї ознаки в усіх режимах функціонування;

$p(x_k/Y_i)$  – умовна ймовірність появи j-го значення k-ї ознаки в режимі функціонування  $Y_i$ .

Після підстановки цього виразу у рівняння (16) формула для розрахунків ентропії рішення буде мати вигляд:

$$H(Y_m/x_{kj}) = -\frac{1}{p(x_{kj})} \sum_{i=1}^m p(Y_i)p(x_{kj}/Y_i) \log \frac{p(Y_i)p(x_{kj}/Y_i)}{\sum_{i=1}^m p(Y_i)p(x_{kj}/Y_i)} = -\frac{1}{p(x_{kj})} \left[ \sum_{i=1}^m p(Y_i)p(x_{kj}/Y_i) \log p(Y_i)p(x_{kj}/Y_i) - \sum_{i=1}^m p(Y_i)p(x_{kj}/Y_i) \log \sum_{i=1}^m p(Y_i)p(x_{kj}/Y_i) \right] \quad (18)$$

Для одержання ентропії рішення слід знайти суму значень величин  $H(Y_m/x_{kj})$  по всіх градаціях  $j = J$  з вагами, пропорційними ймовірності появи кожної градації, тобто  $p(x_{kj})$ .

Тоді

$$\begin{aligned}
 H(Y_m / x_k) &= -\sum_{j=1}^J p(x_{kj}) H(Y_m / x_{kj}) = \\
 &= -\sum_{j=1}^J \sum_{i=1}^m p(Y_i, x_{kj}) \log p(Y_i, x_{kj}) + \\
 &+ \sum_{j=1}^J \sum_{i=1}^m p(Y_i, x_{kj}) \times \sum_{i=1}^m \log p(Y_i, x_{kj}), \quad (19)
 \end{aligned}$$

$$\begin{aligned}
 H_{j-1} &= -\sum_{i=1}^m p_i \log(p_i/P); \\
 H_j &= -\sum_{i=1}^m q_i \log(q_i/Q),
 \end{aligned} \quad (22)$$

де:  $p(Y_i, x_{kj}) = p(Y_i)p(x_{kj}/Y_i)$  – спільний розподіл ймовірностей значень ознаки  $x_k$  для режиму  $Y_k$ .

Тому початкова ентропія ідентифікації режиму функціонування дорівнює

$$H_0(A) = -\sum_{i=1}^m p(A_i) \log p(A_i), \quad (20)$$

то, після підстановки знайдених доданків, остаточний вираз для визначення інформативності  $k$ -ї ознаки буде визначатися як:

$$\begin{aligned}
 I_k &= -\sum_{i=1}^m p(Y_i) \log p(Y_i) = \\
 &= -\sum_{j=1}^J \sum_{i=1}^m p(Y_i, x_{kj}) \log p(Y_i, x_{kj}) - \\
 &- \sum_{j=1}^J \sum_{i=1}^m p(Y_i, x_{kj}) \log \sum_{i=1}^m p(Y_i, x_{kj})
 \end{aligned} \quad (21)$$

З отриманого виразу для обчислення інформативності ознак (21) випливає, що чим точніше вимірюються значення кожної розвідувальної ознаки й чим більше використовується кількість градацій ознак  $J$ , тим більшу інформацію можна отримати при її використанні. Однак при цьому неминуче збільшуються витрати пам'яті і машинного часу ЕОМ при реалізації етапів навчання й класифікації. Тому бажано знайти найменшу кількість ознак і їхніх градацій, що забезпечують необхідну ймовірність ідентифікації режиму функціонування ДРМ.

При розгляді процедури мінімізації простору ознак або знаходженні мінімального опису режимів функціонування ДРМ можна застосувати такий спосіб. Якщо на осі абсцис відкласти значення ймовірностей  $p(x_{kj})$  послідовно для всіх градацій  $j$  будь-якої ознаки  $x_k$ , а по осі ординат – відповідні їм значення  $H(Y_i / x_{kj})$ , то можна побудувати графік залежності  $H(Y_i / x_{kj}) = f[p(x_{kj})]$ .

Площа, обмежена віссю абсцис і кривою, пропорційна ентропії рішення за ознакою  $x_k$ , а площа між рівнем  $H_0(Y)$  і характеристикою – інформаційному змісту  $I_k$  ознаки  $x_k$ .

Для більш детального викладення основних принципів процедури мінімізації простору ознак розглянемо градації  $(j-1)$  та  $j$ . Відповідні їм складові ентропії рішення за  $x_k$ -ю ознакою будуть такі:

де:  $p_i = p(Y, x_{k,j-1})$ ;  $q_i = p(Y_i, x_{kj})$ ;  $P = \sum_{i=1}^m p_i$ ;

$$Q = \sum_{i=1}^m q_i.$$

Після мінімізації градацій за рахунок об'єднання складову ентропії можна знайти як

$$\begin{aligned}
 H_{j,j-1} &= -\sum_{i=1}^m (p_i + q_i) \log(p_i + q_i) + (P + Q) \times \\
 &\times \log(P + Q) = -\sum_{i=1}^m (p_i + q_i) \log \frac{p_i + q_i}{P + Q}
 \end{aligned}$$

У такий спосіб можна розрахувати втрату інформативності ознаки при мінімізації будь-якої кількості градацій ознак.

*Перевірка оптимальної розмірності вектора ознак (дія б рисунок 1).* Умовою закінчення циклу ліквідації градацій є величина порогу втрат інформативності за усіма ознаками  $(\sum \Delta I_k)_{\max}$  або за конкретною ознакою. Можна також задати максимальну кількість градацій, яку необхідно залишити в процесі мінімізації.

На рис. 4 наведені криві зміни інформативності ознак залежно від кількості їх градацій. Аналіз цих кривих за усіма ознаками дає можливість мінімізувати кількість градацій в аспекті витрат пам'яті пристрою ідентифікації і сумарних витрат інформативності параметрів ідентифікації.

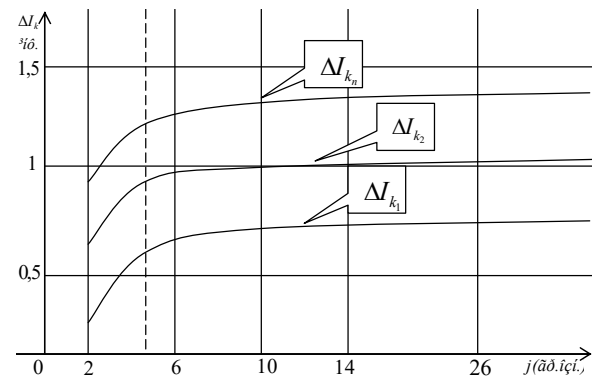


Рис. 4. Мінімізація простору ознак

Наведені залежності свідчать, що кількість градацій ознак доцільно вибрати не більше 4-6 (по точці переломлення більшості кривих), що збігається з результатами наведеними на рисунку 4

У таблиці 3 наведено результати процедури мінімізації простору ознак. При моделюванні використовувалися три режими функціонування ДРМ, які описані вектором ознак, що включає 15 ознак і їхніх градацій ( $j=30$ ). Втрата інформативності в результаті мінімізації за усіма ознаками і їхніми градаціями склала в середньому 0,1126 біт на ознаку, а економія пам'яті збільшилася у 6 разів.



Результати процедури мінімізації простору ознак

Ознака $x_k$	Інформативність $I_k$		Ознака $x_k$	Інформативність $I_k$	
	№ за порядком	Початкова при $j = 30$		Прикінцева при $j = 5$	№ за порядком
1	1,2105	1,1150	9	1,0380	0,9939
2	1,2545	1,0750	10	1,0829	0,9762
3	1,1804	1,0691	11	1,0704	0,9488
4	1,1749	1,0599	12	1,0122	0,9056
5	1,1652	1,0467	13	1,0129	0,9055
6	1,1640	1,0431	14	0,9628	0,8799
7	1,1122	1,0085	15	0,8282	0,7226
8	1,0629	1,0029			

### Висновки й перспективи подальших досліджень

Таким чином, удосконалена методика раціонального розподілу інформації в АСУ військами та зброєю, за рахунок відбору найбільш важливих джерел радіомоніторингу і раціоналізації кількості градацій об'єктів радіомоніторингу для забезпечення заданої ймовірності правильного розпізнавання та гарантованого визначення їх стану, що базуються на основних положеннях теорії інформації К. Шеннона, та дають можливість досить ефективно формалізувати й вирішити завдання визначення

інформативності ознак і мінімізувати їх простір при ідентифікації режимів функціонування ДРМ з мінімальними витратами інформативності і максимальною швидкістю виконання обчислювальних операцій за рахунок збереження обсягу пам'яті ЕОМ в АСУ військами та зброєю.

Результати проведених досліджень в подальшому планується застосовувати при розробці методики визначення пріоритетів розвідувальних ознак та створенні інформаційної системи оцінювання обстановки в умовах надлишковості інформації.

### Література

1. Аксенов Г.Н., Рубцов В.С., Радковец Ю.И. Оперативно-информационная подготовка: Информационное моделирование системы радио- и радиотехнической разведки фронта. Учебное пособие. К.: КВИРТУ ПВО, 1987. -72с. 2. Аксенов Г. Н. Рубцов В.С., Радковец Ю. И. Оперативно-информационная подготовка: часть II. Боевая работа на командных пунктах подразделений, частей и соединений радио и радиотехнической разведки: К., КВИРТУ ПВО, 1985. 72с. 3. Гаценко С. С., Пермяков О. Ю., Варламов І. Д., Удосконалення автоматизованих систем управління військами на основі раціонального розподілу інформаційних потоків в інтегрованому командному середовищі: Збірник матеріалів ХХ Всеукраїнської науково-практичної конференції "Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення". Житомир: ЖВІ, 2014. С. 49-50. 4. Варламов І.Д., Гаценко С.С., Бучинський Ю.А. Особливості побудови та практичної реалізації автоматизованої системи управління розвідкою К., НУОУ, Труді університету. 2017. - № 6(145), С. 44-54. 5. Гончаров Ю. И. Теоретические основы радио и радиотехнической разведки. Ленинград: ВАС, 1989. 374с. 6. Смірнов Ю. О. Основи радіоелектронної

розвідки. Частина 1. Розвідувально-інформаційний процес, основні моделі системи РЕР ефективність і напрями її подальшого розвитку. К.: НДІ ГУР МО України, 2009. 155с. 7. I. Alieinykov, K. A. Thamer, Y. Zhuravskiy, O. Sova, N. Smirnova, R. Zhyvotovskiy, S. Hatsenko, S. Petruk, R. Pikul, A. Shyshatskiy. Development of a method of fuzzy evaluation of information and analytical support of strategic management. Eastern-European Journal of Enterprise Technologies. Vol. 6. No. 2 (102). 2019. pp. 16-27. DOI: <https://doi.org/10.15587/1729-4061.2019.184394>. 8. Брахман Т.Р.

Многокритериальность и выбор альтернатив в технике. -М.: Радио и связь, 1984. -288с. 9. Воронин А.Н. Многокритериальные решения: модели и методы: монография А.Н. Воронин, Ю.К. Зиятдинов, М.В. Куклинский - К.: НАУ, 2011. -268с. 10. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети. Винница: "УНИВЕРСУМ", 1999. 320 с. 11. Пермяков О. Ю. Теоретические основы обработки нечетких данных в аналитических задачах специального математического обеспечения: Дис. на соис. уч. степени д. т. н. К.: 1995. 198 с.

### УСОВЕРШЕНСТВОВАНА МЕТОДИКА РАЦІОНАЛЬНОГО РАСПРЕДЕЛЕНИЯ ИНФОРМАЦИИ ПО ВАЖНОСТИ И КОЛИЧЕСТВУ ИСТОЧНИКОВ РАДИОМОНИТОРИНГА В АСУ ВОЙСКАМИ И ОРУЖИЕМ

*Валерий Владимирович Кузнецов (кандидат военных наук)  
Алексей Васильевич Повещенко  
Игорь Святославович Оксенчук  
Виктор Павлович Николаенко*

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

*При проектировании автоматизированных систем управления войсками и оружием важная роль отводится форме и объему информации, передаваемой информации. Информация в контур управления поступает от датчиков, составляющих систему мониторинга и ведут непрерывное*

наблюдение за источниками и объектами мониторинга.

Система управления и связи группового объекта радиомониторинга представляет собой сложную иерархическую структуру. Количество источников, которые функционируют в интересах обеспечения системы управления превышает количество имеющихся сил и средств, осуществляющих радиомониторинг. Возникает несоответствие при распознавании объектов и источников радиомониторинга: идентификации объекта наблюдения, количество признаков. Поэтому необходимо решить многокритериальную оптимизационную задачи для идентификации режима функционирования источников радиомониторинга для гарантированного определения состояния системы управления и связи группового объекта радиомониторинга, которая заключается в выборе тех источников полезность которых наибольшая.

Предложенная методика рационального распределения информации в АСУ войсками и оружием, за счет отбора наиболее важных источников радиомониторинга и рационализации количества градаций объектов радиомониторинга для обеспечения заданной вероятности правильного распознавания и гарантированного определения их состояния.

**Ключевые слова:** автоматизированная система управления; распознавание; идентификация; источники и объекты; радиомониторинг; распределение информации.

## THE METHODOLOGY OF RATIONAL DISTRIBUTION OF INFORMATION BY IMPORTANCE AND QUANTITY OF RADIO MONITORING SOURCES IS IMPROVED IN ACS ARMS AND WEAPONS

*Valerii Kuznetsov (Candidate of military sciences)*

*Oleksii Poveshchenko*

*Ihor Oksenchuk*

*Viktor Nikolaienko*

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

When designing automated systems for command and control of troops and weapons, an important role is given to the form and volume of information transmitted information. Information in the control loop comes from sensors that make up the monitoring system and continuously monitor the sources and objects of monitoring.

The control and communication system of a group object of radio monitoring is a complex hierarchical structure. The number of sources that operate in the interests of providing a control system exceeds the number of available forces and means that carry out radio monitoring. There is a discrepancy in the recognition of objects and sources of radio monitoring: identification of the object of observation, the number of signs. Therefore, it is necessary to solve the multicriteria optimization problem for identifying the operating mode of radio monitoring sources for guaranteed determination of the state of the control system and communication of the group object of radio monitoring, which consists in choosing those sources whose utility is greatest.

The proposed methodology for the rational distribution of information in automated control systems by troops and weapons, by selecting the most important sources of radio monitoring and rationalizing the number of gradations of radio monitoring objects to ensure a given probability of correct recognition and guaranteed determination of their condition.

**Key words:** automated control system; recognition; identification; sources and objects; radio monitoring; information distribution.

### References

1. **Aksenov G.N.**, Rubczov V.S., Radkovecz Yu.I. Operativno-informacionnaya podgotovka: Informacionnoe modelirovanie sistemy radio- i radiotekhnicheskoy razvedki fronta. Uchebnoe posobie. K.: KVIRTU PVO, 1987. -72s.
2. **Aksenov G. N.**, Rubczov V.S., Radkovecz Yu. I. Operativno-informacionnaya podgotovka: chast' II. Boevaya rabota na komandny'kh punktakh podrazdelenij, chastej i soedinenij radio i radiotekhnicheskoy razvedki: K.: KVIRTU PVO, 1985. 72s.
3. **Gazenko S. S.**, Permyakov O. Yu., Varlamov I. D., Udoskonalennyya avtomatizovanih sistem upravli'nnya vi's'kami na osnovi' raczi'onal'nogo rozpodi'lu i'nformaczi'jnikh potoki'v v i'ntegrovanomu komandnomu seredovishhi': Zbi'rnik materi'ali'v KhKh Vseukrayins'koyi naukovopraktichnoyi konferenczi'yi "Problemi stvorennyya, rozvitku ta zastosuvannyya visokotekhnologij'chnikh sistem speczi'al'nogo priznachennyya". Zhitomir: ZhVI', 2014. S. 49-50.
4. **Varlamov I.D.**, Gaczenko S.S., Buchins'kij Yu.A. Osoblivosti' pobudovi ta praktichnoyi reali'zaczi'yi avtomatizovanoi sistemi upravli'nnya rozvi'dkoyu K., NUOU, Trudi uni'versitetu. 2017. - # 6(145), S. 44-54.
5. **Goncharov Yu. I.** Teoreticheskie osnovy' radio i radiotekhnicheskoy razvedki. Leningrad: VAS, 1989. 374s.
6. **Smirnov Yu. O.** Osnovi radi'oelektronnoi rozvi'dki. Chastina 1. Rozvi'dual'no-i'nformaczi'jniy proces, osnovni' modeli' sistemi RER effektivni'st' i' napryami viyi podal'shogo rozvitku. K.: NDI' GUR MO Ukraini, 2009. 155s.
7. **I. Alieinykov, K. A.** Thamer, Y. Zhuravskiy, O. Sova, N. Smirnova, R. Zhyvotovskiy, S. Hatsenko, S. Petruk, R. Pikul, A. Shyshatskiy. Development of a method of fuzzy evaluation of information and analytical support of strategic management. Eastern-European Journal of Enterprise Technologies. Vol. 6. No. 2 (102). 2019. pp. 16-27. DOI: <https://doi.org/10.15587/1729-4061.2019.184394>.
8. **Brakhman T.R.** Mnogokriterial'nost' i vy'bor al'ternativ v tekhnike. -M.: Radio i svyaz', 1984. -288s.
9. **Voronin A.N.** Mnogokriterial'ny'e resheniya: modeli i metody': monografiva A.N Voronin, Yu.K Ziatdinov, M.V Kuklin-skiy - K.: NAU, 2011. -268s.
10. **Rotshtejn A. P.** Intel'ektual'ny'e tekhnologii identifikaczi: nechvyotkie mnozhestva, geneticheskie algoritmy', neironny'e seti. Vinnicza: "UNIVERSUM", 1999. 320 s.
11. **Permyakov O. Yu.** Teoreticheskie osnovy' obrabotki nechetkikh danny'kh v analiticheskikh zadachakh speczi'al'nogo matematicheskogo obespecheniya: Diss. na sois. uch. stepeni d. t. n. K.: 1995. 198 s.

*Олег Васильович Боровик (доктор технічних наук, професор)*

*Людмила Володимирівна Боровик (доктор педагогічних наук, доцент)*

*Олександр Васильович Андрушко*

*Національна академія Державної прикордонної служби України ім. Б. Хмельницького, Україна*

## УДОСКОНАЛЕННЯ НАУКОВО-МЕТОДИЧНОГО АПАРАТУ РОЗПІЗНАВАННЯ РІВНЯ НЕБЕЗПЕКИ СИТУАЦІЙ У РАЗІ ЗМІНИ ХАРАКТЕРИСТИК ІНФОРМОВАНOSTІ ОСОБИ, ЯКА ПРИЙМАЄ РІШЕННЯ

Дослідження системних задач розпізнавання рівня небезпеки ситуацій і запобігання критичним ситуаціям у складних системах різного призначення є актуальним завданням. Це пояснюється тим, що часткове або повне руйнування таких систем спричиняє не лише катастрофічні наслідки для них самих, а й призводить до суттєвих збитків, які часто перевищують вартість самих систем. Останні можуть бути як матеріальними, так і не матеріальними. Аналіз ряду катастроф у різних галузях людської діяльності, свідчить про те, що масштаби втрат можуть бути значно меншими, якщо в позаштатній ситуації вчасно сформувавши і реалізувавши раціональні рішення. Одним із можливих підходів до розв'язання задач розпізнавання та запобігання критичним ситуаціям у складних системах, є підхід, що базується на реалізації механізмів корегування показників інформованості особи, яка приймає рішення.

У роботі здійснено формалізацію задачі підвищення достовірності даних щодо визначення допустимого періоду часу на формування і реалізацію рішення, для якого ймовірність переходу певної ситуації в критичну, надзвичайну або катастрофічну не перевищуватиме заданого значення, а також класифікації та розпізнавання рівня небезпеки ситуацій. Також проведено аналіз існуючого підходу щодо вирішення сформульованої задачі у випадку застосування механістичного підходу визначення кількісних показників інформованості особи, яка приймає рішення, що дозволило виявити проблемні питання, які мають місце при його застосуванні. На основі застосування системи аналогії запропоновано підхід щодо підвищення ефективності розв'язування подібних задач і програмно-алгоритмічне забезпечення його реалізації.

Зазначений підхід базується на встановленні переліку причин, які обумовлюють фактори, що можуть впливати на зміну ситуації досліджуваної системи, їх ваги, варіантів впливу причин на появу фактора, та на основі цього уточнення показника достовірності інформованості особи, яка приймає рішення. Він також може застосовуватись для підвищення точності оцінки й інших кількісних показників інформованості особи, зокрема повноти та своєчасності.

Програмно-алгоритмічна реалізація авторського підходу до вирішення досліджуваної задачі дозволяє автоматизувати окремі етапи вирішення задачі та покращити рівень об'єктивності розв'язків.

**Ключові слова:** математична модель; критична ситуація; особа, яка приймає рішення; інформованість; достовірність; фактори; причини; експертна оцінка; матриці; алгоритм; програмне забезпечення.

### Вступ

Необхідність дослідження системних задач розпізнавання і запобігання позаштатним, критичним і катастрофічним ситуаціям у складних системах різного призначення (технічних, організаційних тощо) безпосередньо впливає з тенденцій та особливостей їх розвитку. Адже часткове або повне руйнування таких систем спричиняє не лише катастрофічні наслідки для них самих, а й призводить до суттєвих збитків, які часто перевищують вартість самих систем. Такі збитки можуть бути як матеріальними, так і не матеріальними (наприклад, іміджевими, політичними, безпековими). Аналіз ряду катастроф у різних галузях людської діяльності, що проведений авторами, свідчить про те, що

масштаби втрат можуть бути значно меншими, якщо в позаштатній ситуації вчасно сформувавши і реалізувавши раціональні рішення.

**Постановка проблеми.** На даний час у системному аналізі існують методи, які дозволяють з певною точністю розв'язувати ці задачі. Вони базуються на застосуванні показників інформованості особи, яка приймає рішення (ОПР). Такі показники в межах дослідження приймаються заданими. Однак результати розв'язків у ряді випадків свідчать про їх незадовільний рівень. Саме тому актуальним є завдання пошуку підходів до розв'язання задач розпізнавання та запобігання позаштатним, критичним і катастрофічним ситуаціям у складних системах різного призначення, які б забезпечували достатній рівень

об'єктивності розв'язків.

Під час формалізації і розв'язування реальних задач з описаного вище класу важливе значення мають якісні характеристики використовуваної інформації [1].

Зважаючи на це, одним із можливих підходів до розв'язання задач розпізнавання та запобігання позаштатним, критичним і катастрофічним ситуаціям у складних системах різного призначення, який би забезпечував достатній рівень об'єктивності розв'язків, є підхід, що базується на реалізації механізмів корегування показників інформованості ОПР у межах встановленого на початковому етапі періоду часу та динамічного уточнення тривалості самого періоду.

Таким чином, проблемну задачу, яка потребує вирішення, можна сформулювати так.

У процесі функціонування певної системи під впливом множини неконтрольованих факторів ризику деяка штатна ситуація може перейти в критичну, надзвичайну або катастрофічну. Такий перехід може відбуватися упродовж деякого періоду часу, тривалість якого априорі невідома, і який залежить від кількості, властивостей і тривалості впливу факторів. Потрібно визначити такий допустимий період часу на формування і реалізацію рішення, для якого ймовірність переходу ситуації в критичну, надзвичайну або катастрофічну не перевищуватиме задане значення, і який би забезпечував достатній рівень об'єктивності розв'язків.

#### Аналіз остатніх досліджень і публікацій.

Зважаючи на підхід, який пропонується для розв'язання визначеної задачі, актуальним є проведення аналізу існуючих підходів щодо оцінювання інформації у контексті задачі формування рішень.

Одним із найбільш поширених підходів є підхід, що базується на застосуванні показників оцінювання кількості інформації. Він описаний у працях Шеннона [2], Колмогорова [3], Кульбака [4]. Подальший розвиток цього підходу пов'язується з роботою основоположника кібернетики Н. Вінера [5]. Поставлені кібернетикою якісно нові проблеми, пред'явили нові вимоги до формування вихідної інформації. Одним із основних результатів робіт [2-5] стали запропоновані А. Н. Колмогоровим нові ідеї визначення кількості інформації, на основі яких були розроблені нові підходи: комбінаторний і алгоритмічний.

Однак у працях [2-5] не оцінювалися такі показники якості інформації, як повнота, достовірність, своєчасність. Зважаючи ж на те, що вирішення ряду прикладних системних задач потребувало урахування не лише кількості інформації, а й її якісних характеристик, у наступних роботах науковці почали приділяти увагу цьому аспекту. Саме цим пояснюється той факт, що окремі дослідники пропонували методи перетворення якісних характеристик в кількісні, та подальшу обробку отриманих характеристик звичними для математиків методами. Такий підхід

мав місце для фінансової галузі та відповідних прикладних задач.

У сучасній теорії інформаційного аналізу заслуговують на увагу методи та підходи, які відображені в роботі Річарда Грінольда та Рональда Кана з Каліфорнійського університету в Берклі [1], яка містить цікаві ідеї щодо формалізації процесу відбору корисної фінансової інформації для формування інвестиційного портфелю. В роботі наведені не тільки теоретичні відомості та загальна математична постановка задачі, а й результати досліджень та застосування запропонованих методів в американських фінансових компаніях. Також автори навели основні переваги й недоліки запропонованих ними методологій, описали основні принципи вибору правильних джерел інформації та методів оцінки їх релевантності.

Розвиток цих ідей знайшов відображення в роботах [6-11], які стосувалися економічних аспектів діяльності, та у працях [12-15], в яких були досліджені інформаційні аспекти забезпечення прийняття рішень в інших галузях людської діяльності.

Незважаючи на достатньо великий перелік наукових праць, які стосуються досліджуваної задачі, на сьогодні ще не до кінця сформовано універсальний підхід, який би дозволяв розв'язувати її, забезпечуючи при цьому достатній рівень об'єктивності рішення.

**Метою статті** є удосконалення науково-методичного апарату розпізнавання та запобігання позаштатним, критичним і катастрофічним ситуаціям у складних системах різного призначення.

#### Виклад основного матеріалу дослідження

Для досягнення мети вбачається за доцільне: здійснити формалізацію досліджуваної задачі; здійснити аналіз існуючого підходу щодо її вирішення; окреслити коло проблемних питань, що мають місце при його застосуванні; запропонувати механізм реалізації власного підходу щодо вирішення досліджуваної задачі; сформувати програмно-алгоритмічне забезпечення його реалізації.

#### Математична постановка задачі.

Нехай у процесі функціонування складно керованої системи під впливом множини  $\Phi = \{\Phi_j \mid j = \overline{1, n}\}$  неконтрольованих факторів

ризиків  $\Phi_j$  штатна ситуація  $S_i \left( i = \overline{1, m} \right)$  може

перейти в критичну, надзвичайну або катастрофічну. Такий перехід може відбуватися упродовж деякого періоду часу, тривалість якого невідома, і який залежить від кількості, властивостей і тривалості впливу (табл. 1) факторів  $\Phi_j \in \Phi$ .

Потрібно визначити такий допустимий період часу  $T_0$  на формування і реалізацію рішення, для

якого ймовірність переходу ситуації  $S_i$  в критичну, надзвичайну або катастрофічну не перевищуватиме задане значення  $\eta = \eta_{\text{доп}}$  (тобто визначити допустимий період часу на формування і реалізацію рішення, що запобігає катастрофічній ситуації), а також класифікувати та розпізнати рівень небезпеки ситуацій (тобто встановити чи є ситуація критичною, чи вона надзвичайна, чи катастрофічна).

Тут під критичною ситуацією розуміється позаштатний режим функціонування, за якого показники якості системи або показники зовнішнього середовища лежать поза інтервалами штатного режиму в таких межах, що виникає реальна загроза аварії або катастрофи. Аварійна ситуація – позаштатний режим функціонування, за якого система переходить із дієздатного стану в такий недієздатний, аварійний стан, що для переходу у вихідний стан необхідно здійснити певні впливи (наприклад, для технічних систем виконати певні ремонтні роботи). Тут аварія – це кінцевий результат аварійної ситуації. Катастрофічна ситуація – позаштатний режим функціонування, за якого система переходить із дієздатного стану в такий недієздатний, катастрофічний стан, що перехід у початковий стан принципово виключений. Тут катастрофа – це кінцевий результат катастрофічної ситуації.

Таблиця 1

Найменування ситуації $S_i$	Неконтрольовані фактори ризику $\Phi_j \in \Phi$ , що впливають на ситуацію			
	$\Phi_1$	$\Phi_2$	...	$\Phi_n$
$S_1$	+ або -	+ або -	...	+ або -
$S_2$	+ або -	+ або -	...	+ або -
...	...	...	...	...
$S_m$	+ або -	+ або -	...	+ або -

У табл. 1 знак «+» означає, що за впливу відповідного фактора штатна ситуація переходить у критичну, надзвичайну або катастрофічну, а знак «-» - фактор ризику не впливає на ситуацію.

Аналіз існуючого підходу щодо вирішення досліджуваної задачі.

Розглянемо насамперед першу частину задачі, що стосується визначення періоду часу  $T_0$ . Базовий метод її вирішення описаний у роботі [12]. Згідно цього методу насамперед необхідно розрахувати допоміжні коефіцієнти  $\alpha_{ij}, \beta_{ij}, \gamma_{ij}$ , що характеризують динаміку змін показників інформованості. Ці коефіцієнти знаходяться за формулами [12]:

$$\alpha_{ij} = \begin{cases} e^{\hat{I}_{\Pi}^{ij}} \hat{I}_{\Pi}^{ij} 0,5, & \text{якщо } 0 < \hat{\alpha}_{ij} \leq 1, \\ 0, & \text{якщо } \hat{\alpha}_{ij} > 1; \end{cases} \quad (1)$$

$$\beta_{ij} = \begin{cases} (\hat{\alpha}_{ij} + \gamma_{ij}) \hat{I}_{T}^{ij} 10^{-5}, & \text{якщо } 0 < \hat{\alpha}_{ij} + \gamma_{ij} \leq 1, \\ 0, & \text{якщо } \hat{\alpha}_{ij} > 1; \end{cases} \quad (2)$$

$$\gamma_{ij} = \begin{cases} e^{\hat{I}_{D}^{ij}} \hat{\alpha}_{ij} 0,05, & \text{якщо } 0 < \hat{\alpha}_{ij} \leq 1, \\ 0, & \text{якщо } \hat{\alpha}_{ij} > 1. \end{cases} \quad (3)$$

У виразах (1)-(3)  $\hat{\alpha}_{ij}$  - коефіцієнт, що характеризує рівень впливу кожного з факторів  $\Phi_j \in \Phi$  на властивості ситуації  $S_i$ :  $\hat{\alpha}_{ij} \in [0;1]$  і визначається експертно. А  $\hat{I}_{D}^{ij}, \hat{I}_{\Pi}^{ij}, \hat{I}_{T}^{ij}$  - це попередні оцінки показників  $I_{D}^{ij}, I_{\Pi}^{ij}, I_{T}^{ij}$ , які визначаються в момент виявлення позаштатного режиму функціонування системи:  $\hat{I}_{D}^{ij}, \hat{I}_{\Pi}^{ij}, \hat{I}_{T}^{ij} \in [0;1]$  і також визначаються експертно. Самі ж показники  $I_{D}^{ij}, I_{\Pi}^{ij}, I_{T}^{ij}$  - це показники, що характеризують достовірність, повноту, своєчасність інформованості ОПР про вплив факторів  $\Phi_j \in \Phi$  на властивості ситуації  $S_i$ . Їх відшукання здійснюється так:

$$I_{D}^{ij}(t) = \begin{cases} \hat{I}_{D}^{ij} (1 + \gamma_{ij} t), & \text{якщо } 0 < \hat{I}_{D}^{ij} (1 + \gamma_{ij} t) < 1, \\ 1, & \text{якщо } \hat{I}_{D}^{ij} (1 + \gamma_{ij} t) \geq 1; \end{cases} \quad (4)$$

$$I_{\Pi}^{ij}(t) = \begin{cases} \hat{I}_{\Pi}^{ij} (1 + \alpha_{ij} t), & \text{якщо } 0 < \hat{I}_{\Pi}^{ij} (1 + \alpha_{ij} t) < 1, \\ 1, & \text{якщо } \hat{I}_{\Pi}^{ij} (1 + \alpha_{ij} t) \geq 1; \end{cases} \quad (5)$$

$$I_{T}^{ij}(t) = \begin{cases} \hat{I}_{T}^{ij} (1 - \beta_{ij} t^2), & \text{якщо } 0 < \beta_{ij} t^2 < 1, \\ 0, & \text{якщо } \beta_{ij} t^2 \geq 1. \end{cases} \quad (6)$$

На основі знання значень показників  $I_{D}^{ij}, I_{\Pi}^{ij}, I_{T}^{ij}$  знаходиться значення інтегрального показника інформованості у фіксований момент часу  $t$  за співвідношенням

$$I_{ij}(t) = I_{\Pi}^{ij}(t) I_{D}^{ij}(t) I_{T}^{ij}(t). \quad (7)$$

При його відшуканні слід враховувати наступне:

1. Рівень інформованості зростає безперервно від збільшення кожного з показників  $I_{\Pi}, I_{T}, I_{D}$  або тільки одного з них.

2. Загальний рівень інформованості у разі збільшення його повноти, достовірності і своєчасності підвищується за нелінійним законом, а саме: приріст рівня інформованості поступово сповільнюється в міру наближення показників повноти, достовірності і своєчасності до їх граничних значень.

3. Рівень інтегрального показника інформованості у разі зменшення значення одного з показників нижче від деякого граничного значення не може бути компенсований за рахунок збільшення значень інших показників.

4. За нульового значення будь-якого з показників  $I_{\Pi}, I_{T}, I_{D}$  загальний рівень інформованості також дорівнює нулю.

Далі знаходиться ймовірність переходу ситуації  $S_i$  у критичну під впливом фактору  $\Phi_j \in \Phi$  у вигляді

$$\eta_{ij}(t) = 1 - \lg[1 + \alpha_{ij} I_{ij}(t)]. \quad (8)$$

Після цього для визначення тривалості допустимого періоду  $T_0$  розв'язується нерівність:

$$0 \leq 1 - \lg(1 + \alpha_{ij} I_T^{ij} I_{\Pi}^{ij} I_D^{ij} \times (1 + \alpha_{ij} t)(1 + \gamma_{ij} t)(1 - \beta_{ij} t^2)) \leq \eta_{\text{доп}}. \quad (9)$$

Результатом розв'язання нерівності (9) є проміжок  $[T_1; T_2]$ .

Слід зауважити, що проміжки  $[T_1; T_2]$  знаходяться для всіх активних пар  $(i; j)$ , що визначаються наявними факторами  $\Phi_j \in \Phi$  та можливими ситуаціями  $S_i$ . Тоді величина  $T_0 \in [0; \bar{T}_2]$ , де  $\bar{T}_2$  рівне мінімальному із значень  $T_2$  тих проміжків  $[T_1; T_2]$ , які характерні для різних факторів  $\Phi_j \in \Phi$  для конкретної ситуації  $S_i$ . Тобто тривалість  $T_0$  не може перевищувати величини  $\bar{T}_2$ .

Початковою умовою для другої частини досліджуваної задачі є проміжок  $[T^-; T^+]$ , який визначає класифікацію ситуацій  $S_i$  щодо їх критичності. Так, якщо для ситуації  $S_i$  її значення  $T_0$  таке, що  $T_0 \leq T^-$ , то ситуація  $S_i$  відноситься до класу катастрофічних ситуацій. Якщо  $T_0 \in (T^-; T^+]$ , то ситуація  $S_i$  відноситься до класу надзвичайних ситуацій. Якщо ж  $T_0 > T^+$ , то ситуація  $S_i$  відноситься до класу критичних ситуацій. Межі проміжку  $[T^-; T^+]$  встановлюються емпірично і можуть бути нечіткими.

Вирішення другої частини досліджуваної задачі передбачає встановлення для кожної ситуації  $S_i$  такого часового проміжку  $[T_{S_i}^-; T_{S_i}^+]$ , в якому  $T_{S_i}^- = \min T_j^-$  і  $T_{S_i}^+ = \max T_j^+$ , а  $T_j^-$ ,  $T_j^+$  - це значення, які знаходяться для кожного фактора  $\Phi_j \in \Phi$ , що є активними для фіксованої ситуації  $S_i$ , з нерівності [12]

$$\eta^- \leq 1 - \log_2(1 + \alpha_{ij} I_T^{ij} I_{\Pi}^{ij} I_D^{ij} \times (1 + \alpha_{ij} t)(1 + \gamma_{ij} t)(1 - \beta_{ij} t^2)) \leq \eta^+. \quad (10)$$

У нерівності (10)  $\eta^-, \eta^+$  - це допустимі межі ймовірності переходу кожної ситуації  $S_i$  в критичну, надзвичайну або катастрофічну за всіма факторами  $\Phi_j \in \Phi$ .

Далі для кожної ситуації  $S_i$  визначається місце розташування її інтервалу  $[T_{S_i}^-; T_{S_i}^+]$  на інтервалі  $[T^-; T^+]$ . Це дозволяє класифікувати всі ситуації  $S_i$  щодо їх критичності.

Проблемні питання, що мають місце при застосуванні існуючого підходу щодо вирішення досліджуваної задачі.

Аналіз алгоритму існуючого підходу щодо вирішення досліджуваної задачі, який наведений вище, дозволяє зробити висновок про те, що існують проблемні питання щодо ефективності існуючого методу. До числа таких відносяться наступні:

1. При розрахунку допоміжних коефіцієнтів  $\alpha_{ij}, \beta_{ij}, \gamma_{ij}$ , які характеризують динаміку змін показників інформованості, доводиться оперувати значеннями коефіцієнта  $\hat{\alpha}_{ij}$  та показників  $\hat{I}_D^{ij}, \hat{I}_{\Pi}^{ij}, \hat{I}_T^{ij}$ , що встановлюються за попередніми оцінками експертів, які можуть виявитися досить наближеними та неякісне встановлення яких може вплинути на об'єктивність розв'язків.

2. Технологія встановлення значень коефіцієнта  $\hat{\alpha}_{ij}$  та показників  $\hat{I}_D^{ij}, \hat{I}_{\Pi}^{ij}, \hat{I}_T^{ij}$  може загалом впливати на збільшення періоду  $T_0$ , що може змінити критичність ситуації.

Таким чином, фактор достовірності результатів і оперативності щодо формування рішення обумовлюють необхідність аналізу механізмів щодо їх забезпечення.

Авторський механізм удосконалення існуючого підходу щодо вирішення досліджуваної задачі.

Авторське бачення механізмів удосконалення існуючого підходу щодо вирішення досліджуваної задачі стосується удосконалення процедури встановлення значення показника  $\hat{I}_D^{ij}$ . Суть удосконалення полягає в наступному.

Кожен з факторів ризику  $\Phi_j \in \Phi$ , які можуть впливати на зміну критичності ситуації  $S_i$ , може мати місце за ряду причин  $P_k$  фізичного характеру. При цьому, перелік і кількість причин для кожного з факторів  $\Phi_j \in \Phi$  може бути різною. Тому позначимо причини, що впливають на появу фактора  $\Phi_j \in \Phi$ , як  $P_{jk_j}$ . Тут  $k_j$  - це кількість причин, які впливають на появу фактора саме  $\Phi_j \in \Phi$ .

Слід зауважити, що вага кожної з причин  $P_{jk_j}$ , які впливають на появу фактора  $\Phi_j \in \Phi$ , може бути різною. Позначимо її як  $\alpha_{jk_j}$ . Отже,  $\alpha_{jk_j}$  - це вага причини  $P_{jk_j}$  активності фактора  $\Phi_j \in \Phi$ .

Слід зазначити і те, що за наявності впливу фактора  $\Phi_j \in \Phi$  на різні ситуації  $S_i$  (тобто при наявності знака «+» у відповідній клітинці табл. 1) комбінація причин  $P_{jk_j}$ , які обумовлюють такий вплив на конкретну ситуацію  $S_i$ , може бути різною. Більше того, варіант впливу причини на появу фактора також може бути різним. Позначимо його так:  $V_{jk_j,i}$ . Отже,  $V_{jk_j,i}$  - це

варіант впливу причини  $P_{jk_j}$  на появу фактора  $\Phi_j \in \Phi$ , якщо він впливає на можливість зміни ситуації  $S_i$ .

При цьому, варіанти впливу причин на фактор можуть бути такими: причина безпосередньо впливає на появу фактора (БВ); причина має суттєвий вплив на появу фактора (СВ); причина має вплив на появу фактора (В); причина має незначний вплив на появу фактора (НВ).

З урахуванням наведеного, початкову умову задачі щодо встановлення значення показника  $\hat{I}_{Д}^{ij}$  можна представити у вигляді табл. 2.

Сама ж задача полягає у тому, щоб з урахуванням даних табл. 2 знайти значення показника  $\hat{I}_{Д}^{ij}$ .

З урахуванням теорії, що описана у праці [16], та стосується питань оцінки ефективності математичних моделей, загалом, та достовірності результатів моделювання, зокрема, з великим ступенем точності можна стверджувати, що для визначення величин  $V_{jk_j,i}$  можна скористатися описаним у вказаній роботі підходом. Згідно цього підходу та з урахуванням системи аналогій,

$$V_{jk_j,i} = \begin{cases} 0, & \text{якщо має місце БВ;} \\ 0.445, & \text{якщо має місце СВ;} \\ 0.6, & \text{якщо має місце В;} \\ 1.33, & \text{якщо має місце НВ.} \end{cases} \quad (11)$$

Оскільки основним змістом вимоги щодо достовірності результатів моделювання є достатньо точне відображення найбільш суттєвих сторін процесів, що моделюються і притаманних їм закономірностей, то для оцінки величини  $\hat{I}_{Д}^{ij}$  слід обов'язково приймати до уваги перелік і характер впливу причин  $P_{jk_j}$  на появу фактора  $\Phi_j \in \Phi$ , якщо він впливає на можливість зміни ситуації  $S_i$ .

За відсутності детальної моделі досліджуваної задачі значення важливості  $\alpha_{jk_j}$  причин  $P_{jk_j}$  можуть бути оцінені експертно завчасно (до початку змін ситуації).

Тоді показник  $\hat{I}_{Д}^{ij}$  з урахуванням впливу кожної з причин на появу фактора для фіксованої ситуації може бути визначений так:

$$\hat{I}_{Д}^{ij} = 1 - \sum_{k_j} (V_{jk_j,i} \cdot \alpha_{jk_j}). \quad (12)$$

У (12) коефіцієнт  $\alpha_{jk_j}$  відображає вагу причини у відносних одиницях, визначену на основі оцінки усіх причин за стобальною шкалою експертною комісією. А значення  $V_{jk_j,i}$  визначає похибку, що вноситься в розрахунки внаслідок неточного (узагальненого) врахування впливу причин.

Застосування формули (12) вирішує задачу у здійсненій постановці.

Таблиця 2

Перелік причин $P_{jk_j}$ , що впливають на появу фактора $\Phi_j \in \Phi$	Вага $\alpha_{jk_j}$ причини $P_{jk_j}$ активності фактора $\Phi_j \in \Phi$	Найменування ситуації $S_i$ , вплив на яку має фактор $\Phi_j \in \Phi$			
		$S_1$	$S_2$	...	$S_m$
$P_{j1}$	$\alpha_{j1}$	$V_{j1,1}$	$V_{j1,2}$	...	$V_{j1,m}$
$P_{j2}$	$\alpha_{j2}$	$V_{j2,1}$	$V_{j2,2}$	...	$V_{j2,m}$
...	...	...	...	...	...
$P_{jk_j}$	$\alpha_{jk_j}$	$V_{jk_j,1}$	$V_{jk_j,2}$	...	$V_{jk_j,m}$

З урахуванням наведеного, удосконалений алгоритм розв'язування початкової задачі може мати наступний вигляд:

1. Формується табл. 1.
2. Формується шаблон табл. 2.
3. Проводиться розрахунок і встановлення даних табл. 2.
4. Формується матриця даних показника  $\hat{I}_{Д}^{ij}$  на основі застосування виразів (11)-(12).
5. Експертно встановлюються матриці даних показників  $\hat{I}_{П}^{ij}, \hat{I}_{Т}^{ij}$  і матриці коефіцієнтів  $\hat{\alpha}_{ij}$ .
6. Проводиться розрахунок матриці коефіцієнтів  $\gamma_{ij}$  на основі застосування формули (3).
7. Проводиться розрахунок матриць коефіцієнтів  $\alpha_{ij}, \beta_{ij}$  на основі застосування формул (1)-(2).
8. На основі застосування формул (4)-(6) проводиться розрахунок значень показників  $I_{Д}^{ij}, I_{П}^{ij}, I_{Т}^{ij}$ .
9. Застосовується формула (7) для відшукування значення інтегрального показника інформованості у фіксований момент часу  $t$ .
10. Знаходиться ймовірність переходу ситуації  $S_i$  у критичну під впливом фактору  $\Phi_j \in \Phi$  на основі застосування формули (8).

11. На основі розв'язування нерівності (9) знаходяться проміжки  $[T_1; T_2]$  для кожної активної пари  $(i; j)$ .

12. З урахуванням описаного вище підходу знаходиться тривалість  $T_0$ .

13. Проводиться класифікація всіх ситуацій  $S_i$  щодо їх критичності на основі застосування формули (10).

Запропонований підхід до визначення показника  $\hat{I}_{Д}^{ij}$  у разі його автоматизації дозволяє одночасно усунути проблемні аспекти, що мають місце при застосуванні існуючого підходу щодо вирішення досліджуваної задачі.

Таким чином, актуальним є завдання формування програмного забезпечення реалізації

наведеного удосконаленого алгоритму.

Програмно-алгоритмічне забезпечення реалізації авторського механізму удосконалення існуючого підходу щодо вирішення досліджуваної задачі.

Для реалізації наведеного алгоритму було реалізовано відповідний програмний додаток. Серверна частина додатку виконана в середовищі Node.js із застосуванням бази даних MongoDB. Вибір середовища зумовлений швидкодією при операціях введення-виведення та роботи з даними [17-20].

Фрагмент реалізації додатку, що стосується наведеного алгоритму, наведений нижче.

```
import mongoose from "mongoose";
import _ from "lodash";
Calculator.methods = {
  calculateAlpha(i, j) {
    const alphaCircumflex = this.alphaCircumflexMatrix[i][j];
    if (!alphaCircumflex) {
      return null;
    }
    return this.alphaCircumflexMatrix[i][j] > 1
      ? 0
      : Math.exp(alphaCircumflex) *
        this.IpCircumflexMatrix[i][j] * 0.5;
  },
  calculateBeta(i, j) {
    const alpha = this.calculateAlpha(i, j);
    if (!alpha) {
      return null;
    }
    const gamma = this.calculateGamma(i, j);
    if (alpha + gamma >= 1) {
      return 0;
    }
    return (alpha + gamma) *
      this.ItCircumflexMatrix[i][j] * Math.pow(10, -4);
  },
  calculateGamma(i, j) {
    const alphaCircumflex = this.alphaCircumflexMatrix[i][j];
    if (!alphaCircumflex) {
```

```
return null;
}
if (alphaCircumflex > 1) {
  return 0;
}
const IdCircumflexMatrix =
  this.calculateIdCircumflexMatrix();
return Math.exp(IdCircumflexMatrix[i][j]) *
  alphaCircumflex * 0.05;
},
calculateIp(i, j, t) {
  const IpCircumflex = this.IpCircumflexMatrix[i][j];
  if (!IpCircumflex) {
    return null;
  }
  const result = IpCircumflex * (1 +
    this.calculateAlpha(i, j) * t);
  return result >= 1 ? 1 : result;
},
...calculateAcceptablePeriod(i, j, etaAcceptable) {
  const deltaT = 0.1;
  let t = 0,
  polynome,
  TValues = [];
  do {
    polynome = this.acceptablePeriodPolynome(i, j, t);
    if (polynome == null) {
      return null;
    }
    TValues.push({ t, polynome });
    t += deltaT;
  } while (polynome >= 0);
  TValues = TValues.filter(x => x.polynome <=
    etaAcceptable);
  TValues = TValues.map(x => x.t);
  return [0,
    parseFloat(_.max(TValues).toFixed(2))] : null;
},
```

Результати роботи додатку, що опрацьований авторами та відповідає наведеному методу, можуть бути оцінені з рис. 1-4.

**Дані для визначення  $\tilde{I}_D$   
Чинники для фактора  $\Phi_1$**

Чинники:

Перелік причин $P_{jk}$ , що впливають на появу фактора $\phi_j \in \Phi$	Вага $\alpha_{jk}$ причини $P_{jk}$ активності фактора $\phi_j \in \Phi$	Найменування ситуації $S_i$ , вплив на яку має фактор $\phi_j \in \Phi$			
		$S_1$	$S_2$	$S_3$	$S_4$
P1.1	0.1	B	CB	B	CB
P1.2	0.2	CB	CB	B	HB
P1.3	0.2	CB	CB	HB	HB
P1.4	0.2	HB	B	B	CB
P1.5	0.15	HB	B	CB	HB
P1.6	0.15	BB	CB	BB	HB



Чинники для фактора  $\Phi_2$

Перелік причин $P_{jk}$ , що впливають на появу фактора $\Phi_j \in \Phi$	Вага $\alpha_{jk}$ причини $P_{jk}$ активності фактора $\Phi_j \in \Phi$	Найменування ситуації $S_i$ , вплив на яку має фактор $\Phi_j \in \Phi$			
		$S_1$	$S_2$	$S_3$	$S_4$
P2.1	0.5	НВ	В	БВ	НВ
P2.2	0.1	СВ	СВ	БВ	В
P2.3	0.1	СВ	НВ	В	БВ
P2.4	0.05	В	СВ	В	НВ
P2.5	0.05	НВ	СВ	БВ	НВ
P2.6	0.2	БВ	СВ	В	НВ

Чинники:

Чинники для фактора  $\Phi_3$

Чинники для фактора  $\Phi_4$

Рис. 1. Введення в систему даних для визначення  $\hat{I}_D^{ij}$

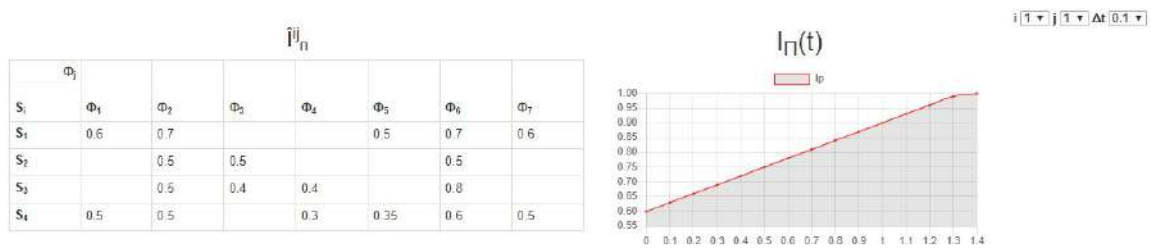


Рис. 2. Інтерфейс введення попередньо визначених показників та відображення результатів обчислення  $I_\Pi(t)$ ,  $I_T(t)$ ,  $I_D(t)$ ,  $\hat{I}_D$  з відповідними графіками

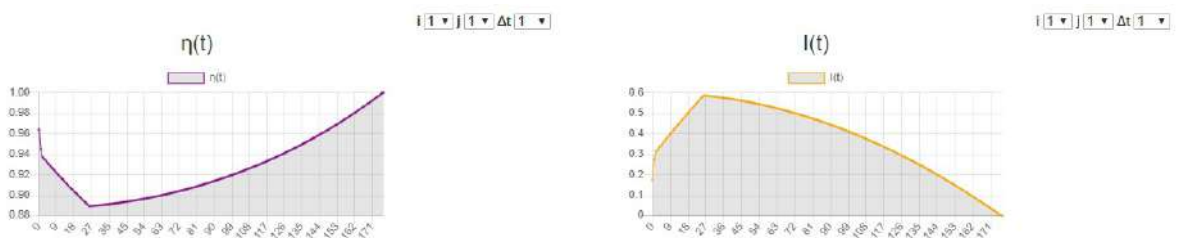


Рис. 3. Інтерфейс побудови графіків функцій інтегрального показника інформованості  $I_{ij}(t)$  та ймовірностей переходу ситуацій  $\eta_{ij}(t)$

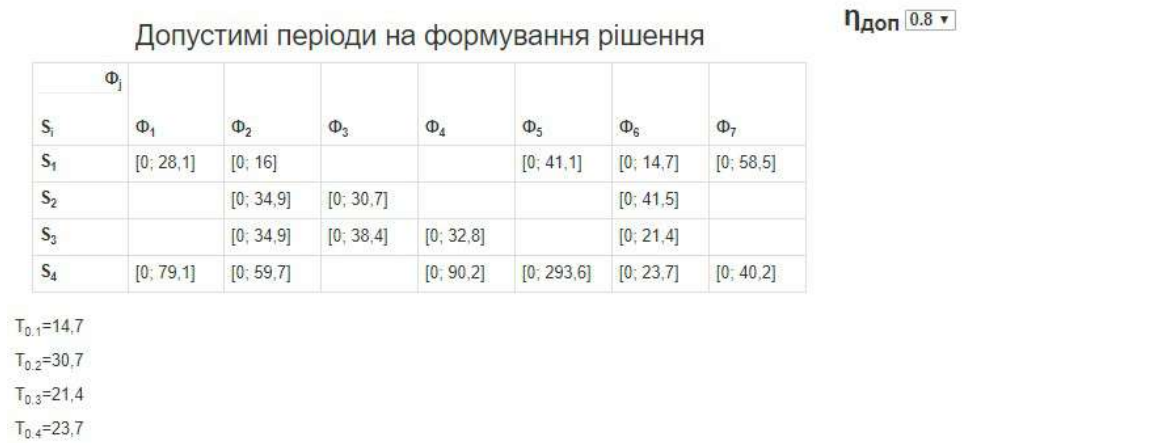


Рис. 4. Інтерфейс відображення результатів визначення допустимих періодів на формування рішення

### Висновки й перспективи подальших досліджень

За результатами проведеного дослідження можна зробити висновок про те, що запропонований підхід щодо корегування показників інформованості ОПР у межах встановленого на початковому етапі періоду часу та динамічного уточнення тривалості самого періоду забезпечує удосконалення науково-методичного апарату вирішення задачі розпізнавання та запобігання позаштатним, критичним і катастрофічним ситуаціям у складних

системах різного призначення. Слід зауважити, що підхід, який наведений вище і стосується визначення показника  $\hat{I}_{Д}^{ij}$ , може бути адаптованим і для відшукування значень матриці коефіцієнтів  $\hat{\alpha}_{ij}$ , а також встановлення матриць даних показників  $\hat{I}_{П}^{ij}, \hat{I}_{Т}^{ij}$ .

Обґрунтування механізмів реалізації наведеної ідеї, а також апробація удосконаленої у роботі моделі на основі конкретного прикладу визначає перспективи подальших досліджень.

### Література

1. Мазур М. Качественная теория информации. Мир. М. 1972. С. – 239. 2. Колмогоров А. Н. Три подхода к определению понятия «количества информации». Проблемы передачи информации. 1965. Т.1. вып.1. С. 3-11. 3. Кульбак С. Теория информации и статистика. Наука. М. 1954. С. 376. 4. Колмогоров А. Н. Теория информации и теория алгоритмов. Наука. М.1987. С. 304. 5. Винер Н. Кибернетика или управление и связь в животном и машине. Наука. М. 1983. С. 343. 6. Ілляшенко С. М. Економічний ризик: навчальний посібник. Центр навчальної літератури. 2-ге вид., доп. перероб. К. 2004. С. 220. 7. Шапкин А. С. Экономические и финансовые риски. Оценка, управление, портфель инвестиций: Монография. Изд. - Торг. корпорация «Дашков и Ко». М. 2003. С. 544 8. Балдин К. В. Информационные системы в экономике: учебник. Издательско-торговая корпорация «Дашков и Ко». М. 2006. С. 395. 9. Бережной О. А. Інформаційно-аналітичне забезпечення прийняття ефективних управлінських рішень. Актуальні проблеми економіки. 2004. №9. С. 26 – 30. 10. Бобруль Г. І. Інформація та інформаційні технології в стратегічному управлінні посередницькою організацією. Актуальні проблеми економіки. 2006. №5. С. 135-143. 11. Волков И. М.

Критерии оценки проектов. Институт экономического развития Всемирного банка. М. 2006. С. 128. 12. Згуровський М. З., Панкратова Н. Д. Основи системного аналізу. Видавнича група BVH. К. 2007. С. 544. 13. Косс В. А. Умови відповідності моделі управління системним потребам об'єкта управління. Математичні машини і системи. 2007. № 1. С. 12-18. 14. Качинський А. В. Засади системного аналізу безпеки складних систем. ДП «НБК «Євроатлантикінформ». К. 2006. С. 336. 15. Gupta J.N.D., Sharma S., Rashid M.A. Handbook of Research on Enterprise Systems. Farmington Hills: Gale Group. 2009. P. 460. 16. Городнов В. П. Моделирование боевых действий частей, соединений и объединений войск ПВО. Харьков. 1987. С. 383. 17. What is Node.js used for?. Access mode. [Electronic resource]. URL: <https://railsware.com/blog/what-is-node-js-used-for>. (date of access: 29.02.2020). 18. Математика в JavaScript. [Electronic resource]. URL: <https://habr.com/ru/post/312880> (дата звернення: 29.02.2020). 19. Документація Node.js. URL: <https://nodejs.org/ru/docs/> (дата звернення: 29.02.2020). 20. MongoDB Documentation. [Electronic resource]. URL: <https://docs.mongodb.com/> (date of access: 29.02.2020).

### УСОВЕРШЕНСТВОВАНИЕ НАУЧНО-МЕТОДИЧЕСКОГО АППАРАТА РАСПОЗНАВАНИЯ УРОВНЯ ОПАСНОСТИ СИТУАЦИЙ В СЛУЧАЙ ИЗМЕНЕНИЯ ХАРАКТЕРИСТИК ИНФОРМИРОВАННОСТИ ЛИЦА, ПРИНИМАЮЩЕГО РЕШЕНИЕ

Олег Васильевич Боровик (доктор технических наук, профессор)  
 Людмила Владимировна Боровик (доктор педагогических наук, доцент)  
 Александр Васильевич Андрушко

Национальная академия Государственной пограничной службы Украины им. Б. Хмельницкого, Украина

*Исследование системных задач распознавания уровня опасности ситуаций и предотвращение критическим ситуация в сложных системах различного назначения является актуальной задачей. Это объясняется тем, что частично или полное разрушение таких систем приводит не лишь катастрофические последствия для них самих, но и производит к существенным убыткам, которые часто превышает стоимость самих систем. Последние могут быть как материальными, так и нематериальными. Анализ ряда катастроф в различных областях человеческой деятельности, свидетельствует о том, что масштабы потерь могут быть значительно меньше, если во внештатной ситуации вовремя сформировать и реализовать оптимальные решения. Одним из возможных подходов к решению задач распознавания и предотвращения критических ситуаций в сложных системах, является подход, основанный на реализации механизмов корректировки показателей информированности лица, принимающего решение.*

*В работе осуществлено формализацию задачи повышения достоверности данных по определению допустимого периода времени на формирование и реализацию решения, для которого вероятность перехода определенной ситуации в критическую, чрезвычайную или катастрофическую не превышает заданного значения, а также классификации и распознавания уровня опасности ситуаций. Также проведен анализ существующего подхода к решению сформулированной задачи в случае применения механистического подхода определения количественных показателей информированности лица, принимающего решение, позволившее выявить проблемные вопросы, имеющие место при его применении. На основе применения системы аналогий предложен подход по повышению эффективности решения подобных задач и программно-алгоритмическое обеспечение его реализации.*

*Указанный подход базируется на установлении перечня причин, обуславливающих факторы, которые могут вытекать на смену ситуаций исследуемой системы, их веса, вариантов воздействия причин появления фактора, и на основе этого уточнении показателя достоверности информированности лица, принимающего решение.*

*Он также может применяться для повышения точности оценки и других количественных показателей информированности лица, в частности полноты и своевременности.*

*Программно-алгоритмическая реализация авторского подхода к решению исследуемой задачи позволяет автоматизировать отдельные этапы решения задачи и улучшить уровень объективности решений.*

***Ключевые слова:** математическая модель; критическая ситуация; лицо, принимающее решение; информированность; достоверность; факторы; причины; экспертная оценка; матрицы; алгоритм; программное обеспечение.*

## **IMPROVEMENT OF THE SCIENTIFIC AND METHODOLOGICAL APPARATUS BY RECOGNIZING THE LEVEL OF DANGER OF THE SITUATION IN THE CASE OF CHANGING THE CHARACTERISTICS OF THE INFORMING OF THE DECISION MAKER**

*Oleh Borovyk (Doctor of Technical Sciences, Professor)  
Liudmyla Borovyk (Doctor of Science, Associate Professor)  
Aleksandr Andrushko*

*National Academy of State Border Guard Service of Ukraine named after B. Khmelnytsky, Ukraine*

*Research on systemic problems of recognizing the level of danger of situations and preventing critical situations in complex systems of various purposes is an urgent task. This is because the partial or complete destruction of such systems causes not only catastrophic consequences for themselves, but also leads to significant losses that often exceed the cost of the systems themselves. The latter can be both material and non-material. The analysis of a number of catastrophes in different fields of human activity shows that the magnitude of losses can be much smaller if, in an emergency situation, rational decisions are made and implemented in a timely manner. One approach to addressing the challenges of identifying and preventing critical situations in complex systems is an approach based on the implementation of mechanisms for adjusting the awareness of the decision-maker.*

*The paper formalizes the problem of increasing the reliability of data to determine the permissible time period for the formation and implementation of a solution for which the probability of transition of a certain situation in a critical, emergency or catastrophic will not exceed the set value, as well as the classification and recognition of the level of danger situations. Also, the analysis of the existing approach to solving the formulated problem in the case of applying a mechanistic approach to determining quantitative indicators of the decision-maker's awareness was made, which revealed the problematic issues that occur in its application. Based on the application of the analogy system, an approach is proposed to improve the efficiency of solving such problems and to provide software and algorithmic support for its implementation.*

*This approach is based on establishing a list of reasons that determine the factors that may change the situation of the investigated system, their weight, options for the influence of causes on the appearance of the*

factor, and based on this refinement of the confidence indicator of the decision-maker. It can also be used to improve the accuracy of assessment and other quantitative indicators of a person's awareness, including completeness and timeliness.

The algorithmic implementation of the author's approach for solving the problem under study allows you to automate the individual steps of solving the problem and improve the level of objectivity of the solutions.

**Keywords:** mathematical model; critical situation; decision maker; awareness; reliability; factors; causes; expert judgment; matrices; algorithm; software.

### References

- Mazur M.** Qualitative theory of information [Kachestvennaya teoriya informatsii]. Peace. M. 1972. P. 239.
- Kolmogorov A. N.** Three approaches to the definition of the concept of "amount of information". Problems of information transfer. [Tri podhoda k opredeleniyu ponyatiya «kolichestva informatsii». Problemyi peredachi informatsii]. 1965. Vol.1. issue 1. Pp. 3-11.
- Kulbak S.** Information theory and statistics. [Teoriya informatsii i statistika] Science. M. 1954. P. 376.
- Kolmogorov A.N.** Information theory and algorithms theory.[Teoriya informatsii i teoriya algoritmov]. Science. M.1987. P. 304.
- Viner N.** Cybernetics or control and communication in animal and machine [Kibernetika ili upravlenie i svyaz v zhivotnom i mashine]. Science. M. 1983. P. 343.
- Iljashenko S.M.** Economic risk: a textbook. Center of Educational Literature [Ekonomichnyy ryzyk: navchal'nyy posibnyk.].the 2 nd ed., Suppl. republishing. K. 2004. P. 220.
- Shapkin A.S.** Economic and financial risks. Valuation, management, investment portfolio: Monograph. [Ekonomicheskie i finansovye riski. Otsenka, upravlenie, portfel investitsiy: Monografiya]. Ed. – Trade corporation. Dashkov & Co. Corporation. M. 2003. P. 544.
- Baldin K.V.** Information systems in economics: a textbook. [Informatsionnyye sistemyi v ekonomike: uchebnik]. Dashkov & Co. Publishing and Trading Corporation. M. 2006. P. 395.
- Berezhnoi O.A.** Information-analytical support for making effective management decisions [Informacijno-analitychne zabezpechennja pryjnattja efektyvnykh upravlinsjkykh rishenij]. Actual problems of the economy. 2004. №9. Pp. 26 - 30.
- Bobrulj Gh. I.** Information and informational technologies in the strategic management of an intermediary organization [Informacija ta informacijni tekhnologiji v strategichnomu upravlinni poserednyckuju orghanizacijeu]. Actual problems of the economy. 2006. №5. Pp. 135-143.
- Volkov I.M.** Criteria for project evaluation [Kriterii otsenki proektov]. World Bank Institute for Economic Development. M. 2006. P. 128.
- Zghurovsjkyj M. Z., Pankratova N. D.** Fundamentals of system analysis [Osnovy systemnogho analizu]. BHV Publishing Group. K. 2007. P. 544.
- Koss V.A.** Conditions for compliance of the management model of the system needs of the management object [Umovy vidpovidnosti modeli upravlinnja systemnym potrebam ob'jekta upravlinnja]. Mathematical Machines and Systems. 2007. № 1. Pp. 12-18.
- Kachynsjkyj A. V.** Fundamentals of system analysis of security of complex systems [Zasady systemnogho analizu bezpeky skladnykh system]. SE «Euroatlantikinform». K. 2006. P. 336.
- Gupta J.N.D. Sharma S. Rashid M.A.** Handbook of Research on Enterprise Systems. Farmington Hills: Gale Group. 2009. P. 460.
- Gorodnov V.P.** Modeling of combat operations of units, formations and unions of air defense forces [Modelirovanie boevyih deystvii chastej, soedinenij i ob'edinenij voysk PVO]. Kharkiv. 1987. P. 383.
- What is Node.js used for? Access mode. [Electronic resource]. URL: [https:// railsware.com / blog / what-is-node-js-used-for](https://railsware.com/blog/what-is-node-js-used-for). (date of access: 29.02.2020).
- Math in JavaScript. [Electronic resource]. URL: <https://habr.com/post/312880> (accessed 29/02/2020).
- Node.js documentation URL: <https://nodejs.org/en/docs/> (accessed: 02/29/2020).
- MongoDB Documentation. [Electronic resource]. URL: <https://docs.mongodb.com/> (date of access: 29.02.2020).

*Олександр Юрійович Пермяков (доктор технічних наук, професор)*

*Юрій Борисович Прібилєв (кандидат технічних наук, доцент)*

*Віктор Євгенович Бобильов (кандидат технічних наук, с.н.с.)*

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

## ПІДХІД ЩОДО ПОБУДОВИ УНІВЕРСАЛЬНОЇ АВТОМАТИЗОВАНОЇ КОНТРОЛЬНО-ВИПРОБУВАЛЬНОЇ СТАНЦІЇ ЗІ ЗАСТОСУВАННЯМ ЕКСПЕРТНИХ СИСТЕМ

У статті розробляється підхід щодо побудови універсальної автоматизованої контрольно-випробувальної станції зі застосуванням експертних систем. Показано, що найбільш складною задачею для визначення достовірного технічного стану зенітних керованих ракет є проведення контрольно-вимірювальних операцій за допомогою контрольно-випробувальних станцій.

Обґрунтована перспективність використання експертних систем у галузі технічного контролю, яка дозволяє підвищити ефективність контролю технічного стану бортового обладнання зенітних керованих ракет за рахунок урахування знань та досвіду експертів, накопичення знань та реалізації самонавчання експертної системи контролю. Запропоновано формування інформаційно-контрольних моделей поточного технічного стану зенітних керованих ракет (сукупність усіх значень параметрів, що контролюються, та зміна їх у часі, "паспорт" зенітної керованої ракети), що дозволяє зробити прогноз технічного стану зенітних керованих ракет більш достовірним за рахунок урахування тенденцій змін контрольних параметрів. Це дозволяє зробити розширений висновок за результатом роботи експертної системи контролю: зенітна керована ракета є справною (несправною) або працездатною (непрацездатною), які параметри вийшли за межі норми та рекомендований наступний міжконтрольний інтервал.

Запропонована структура контрольно-випробувальної станції реалізує завдання контролю комплексно: за програмою контролю подає стимулюючі сигнали, аналізує вихідні реакції, поповнює базу еталонних значень вимірюваних параметрів сигналів та формує інформаційно-контрольні моделі поточного технічного стану зенітної керованої ракети, які потім порівнюються за визначеним алгоритмом з інформаційно-контрольними моделями еталонного стану зенітної керованої ракети, що контролюється. Запропонований підхід щодо побудови універсальної автоматизованої контрольно-випробувальної станції зі застосуванням експертних систем забезпечить побудову універсальної уніфікованої автоматизованої контрольно-випробувальної станції зі змінною конфігурацією, яка дозволить проводити автоматизований контроль декількох зразків зенітних керованих ракет з високим рівнем достовірності та рекомендувати міжконтрольний інтервал.

**Ключові слова:** зенітний ракетний комплекс, зенітна керована ракета, контрольно-випробувальна станція, експертна система контролю, інформаційно-контрольна модель.

### Вступ

Сучасні зенітні ракетні комплекси (ЗРК) є складними технічними системами з застосуванням інформаційних технологій і радіоелектронних засобів (РЕЗ) [1]. Перспективні ЗРК мають ще більш складні РЕЗ та вимагають збільшення кількості вимірювань та якості проведення контрольно-вимірювальних операцій для отримання достовірної інформації щодо їх технічного стану (ТС) [2]. Готовність ЗРК суттєво залежить від ТС зенітних керованих ракет (ЗКР), визначення придатності яких до застосування проводиться за допомогою контрольно-випробувальних станцій (КВС) (контрольно-

вимірювальна приладна станція), що є обов'язковою складовою ЗРК.

**Постановка проблеми.** Усі КВС, що зараз знаходяться на постачанні у Збройних Силах (ЗС) України, вироблені ще у радянські часи на підприємствах, які зараз знаходяться на території Російської Федерації (РФ). Більшість з них розроблені у Рязанському конструкторському бюро "Глобус", яке спеціалізується на виробництві систем контролю. Усі ці засоби є вузькоспеціалізованими (тобто можуть бути використані для контролю тільки одного типу ЗКР, мають різні конструктивну, інформаційну та програмну бази, знаходяться в експлуатації у

середньому більш, ніж 30 років та мають незадовільний ТС внаслідок старіння елементної бази та вироблення експлуатаційного ресурсу апаратури. Внаслідок цього їх модернізація ускладнена та економічно недоцільна, а уніфікація взагалі неможлива [3].

Крім того, наявні у ЗС України на постачанні КВС виконують тільки функції саме контролю ТС ЗКР. При цьому не використовуються можливості прогнозування зміни ТС ЗКР та оптимізації міжконтрольних інтервалів, що є одним з способів зменшення витрат на проведення контролю ТС ЗКР.

Зменшити витрати на обслуговування ЗКР (особливо модернізованих та перспективних ЗКР, що зараз розробляються) дозволить побудова автоматизованої КВС, що розроблена за базово-модульним принципом із застосуванням новітніх інформаційних технологій та яка буде універсальною і здатною проводити контроль і випробування ЗКР декількох типів [4]. Існуючі зараз на постачанні ЗС України КВС при визначенні ТС ЗКР використовують тільки інформацію щодо знаходження контрольних параметрів у полі допуску. При проведенні контрольних-випробувальних робіт не фіксуються значення цих параметрів та інформація про них не використовується при наступному контролі ТС ЗКР. Але важливе значення має врахування швидкості зміни контрольних параметрів внаслідок деградації матеріалів радіоелементів, врахування важливості цих параметрів при визначенні рішення щодо справності ЗКР та визначення їх взаємозв'язку. Застосування експертних систем (ЕС) дозволяє використовувати знання і досвід фахівців-експертів у галузі контролю ТС ЗКР, що дозволить підвищити технологічний рівень КВС та забезпечити необхідний рівень достовірності контролю ТС ЗКР за допомогою КВС.

У зв'язку з цим, наукова проблема розробки моделі побудови сучасної автоматизованої системи контролю ЗКР, зі застосуванням експертних систем, для можливості накопичення знань, урахування досвіду експертів та реалізації самонавчання ЕС контролю (ЕСК) є актуальною.

**Аналіз останніх досліджень і публікацій.** Питанням використання експертних систем присвячена значна кількість робіт, у яких визначені основні терміни, що описують експертні системи, підходи до їх побудови та питання щодо їх застосування у різних сферах діяльності людини та суспільства. Експертні системи – це прикладні системи штучного інтелекту, в яких база знань являє собою формалізовані емпіричні знання висококваліфікованих експертів у будь-якій вузькій предметній області. ЕС призначені для заміни експертів при вирішенні завдань у разі їх недостатньої кількості, недостатньої оперативності

при вирішенні завдання або в умовах, що є шкідливими для них.

Зазвичай ЕС розглядаються з точки зору їх застосування у двох аспектах: для вирішення яких завдань вони можуть бути використані і в якій області діяльності. Ці два аспекти накладають свій відбиток на архітектуру експертної системи, що розроблюється. Наприклад, є посилання на ЕС при аналізі напрямків розвитку систем контролю і діагностування складних технічних систем (СТС), що проведений у [5]. Ефективність використання ЕС у галузі технічної діагностики досліджена у роботі [6]. Визначення ТС елементів комплексів засобів автоматизації за допомогою ЕС наведено у роботі [7]. У роботі [8] запропоновано застосування ЕС у галузі технічної діагностики для зменшення кількості контрольних вимірювань. У [9] зроблено спробу застосувати ЕС для технічної діагностики типових елементів заміни РЕЗ ЗРК з використанням інформації зі систем самоконтролю ТС ЗРК. Але застосування експертних систем у структури КВС ще не розглядалось.

**Мета статті** полягає у розробці підходу щодо побудови універсальної автоматизованої контрольних-випробувальної станції зенітних керованих ракет зі застосуванням експертних систем.

### Виклад основного матеріалу дослідження

Проблемним питанням системи протиповітряної оборони (ППО) України є закінчення експлуатаційного ресурсу зенітного ракетного озброєння (ЗРО), у першу чергу ЗКР та авіаційних засобів ураження, що призводить до зниження можливостей системи ППО України. На озброєнні зенітних ракетних військ знаходяться наступні основні зразки зенітного ракетного озброєння: зенітна ракетна система (ЗРС) С-300-П та ЗРК “БУК-М1”, розроблені та виготовлені ще за часів колишнього СРСР. До цих ЗРК є достатній запас ЗКР (9М38 М1 до ЗРК “БУК-М1”) та вітчизняний оборонний комплекс України має можливість проведення модернізації та продовження призначених показників ЗКР 5В55 до ЗРС С-300-П та 9М83 до С-300-В1. Але неодноразове продовження ресурсу зазначених ЗРС та ЗРК свідчить про тенденцію їх фізичного старіння, що потребує якісного (повного та достовірного) контролю ТС для підтримання готовності ЗКР на необхідному рівні, для чого зменшується періодичність контролю ЗКР. Для проведення якісного контролю та зниження експлуатаційних витрат актуальною є розробка нових методів та засобів контролю ТС ЗКР для підтримання ЗРК у готовності [10].

Аналіз технічної літератури та характеристик сучасних та перспективних ЗКР (наприклад, ЗКР у складі ЗРК “С-350”, що є заміною “С-300” у ЗС

РФ) дозволяє зробити висновок про широке використання цифрових та комп'ютерних засобів у бортовому обладнанні ЗКР [11]. Застосування сучасної цифрової елементної бази у головках самонаведення перспективних ЗКР також вимагає удосконалення ефективності існуючих та розробки принципово нових методів контролю ТС ЗКР [12]. При побудові систем (комплексів) ЗРО застосовують базово-модульний принцип, реалізація якого дозволяє при мінімальному базовому наборі модулів формувати різні за призначенням ЗРС (ЗРК), оперативно здійснювати реконфігурацію систем (комплексів) ЗРО, робити їх мобільними [13]. Базово-модульний принцип є також перспективним при побудові КВС.

Одним з найбільш значних досягнень науки у галузі штучного інтелекту є ЕС, або системи, що засновані на "знаннях". У загальному сенсі ЕС – це комп'ютерна програма, у якій застосовуються знання та досвід спеціалістів вузької галузі знань (предметної області) та яка надає рекомендації (консультації) користувачу. "Математизація" процесу пошуку відмов та розвиток ЕСК ТС об'єктів контролю (ОК) дозволяє підвищити ефективність контролю з мінімально необхідною кількістю контрольованих операцій.

Знання і досвід експертів у галузі контролю ТС дозволяють удосконалити бази даних ознак несправностей ОК та відповідних баз знань, які дозволяють зробити достовірний висновок про ТС ОК та надати рекомендації обслуговуючому персоналу щодо подальших рішень. Використання ЕС у засобах контролю ТС ЗКР дозволить вирішити важко формалізовані завдання визначення ТС та збільшити ефективність проведення його контролю. З розвитком ЕСК з'явилася можливість накопичення знань, урахування досвіду експертів та реалізація самонавчання ЕСК.

Традиційні методи технічного контролю, які конструктивно реалізовані в існуючих КВС, не завжди забезпечують необхідний рівень достовірності контролю та мають обмежені можливості щодо контролю цифрових РЕЗ, що зрозуміло, наприклад, з аналізу програми контролю АКВС 70К6 [3]. Застосування технології ЕС дозволяє підвищити технологічний рівень КВС, забезпечити необхідний рівень достовірності контролю сучасних та перспективних ЗКР та забезпечить можливість прогнозу змін ТС, що може бути підставою для корегування інтервалу проведення регламентних робіт з ЗКР.

Недосконалість алгоритмів контролю і значна кількість параметрів, що контролюються у перспективних ЗКР, значно ускладнюють рішення завдань контролю, тому традиційні способи технічного контролю (апаратний та функціональний контроль) є малоефективними. Найбільш перспективним підходом до рішення задач контролю ТС ЗКР є побудова ЕСК, які с

розвитком теорії штучного інтелекту застосовуються все частіше.

Розглянемо принцип побудови ЕСК, класична базова структурна схема якої зображена на рис. 1 та включає мінімальну кількість модулів, що необхідні для її функціонування:

програма контролю (алгоритм контролю) та генератор стимулюючих сигналів, що є обов'язковою частиною будь-якої системи контролю, як апаратно-програмного комплексу;

база знань, що становить ядро ЕСК у сукупності с базою даних еталонних параметрів ЗКР;

модуль логічного виведення, що генерує рішення за результатом контролю;

модуль редагування бази знань, що реалізує режим отримання знань системою від експерта;

модуль відображення результатів контролю.

За цією традиційною структурою ЕСК вимірюють характеристики контрольованих сигналів, що генеруються ЗКР за програмою контролю як реакція на стимулюючі сигнали, та подаються на модуль виведення рішень. База знань призначена для зберігання експертних знань про предметну область, що використовуються при вирішенні завдань експертної системою. База даних, крім зберігання інформації щодо кількісного значення параметрів об'єкта контролю, може здійснювати тимчасове зберігання проміжних рішень, що застосовуються під час прийняття остаточного рішення щодо результату контролю.

Модуль виведення рішень реалізує алгоритм порівняння результатів вимірювань характеристик контрольованих сигналів з еталонними сигналами за правилами, що є у базі знань ЕСК (які складаються та коректуються експертом).

Фактично ЕСК є апаратно-програмним комплексом, що використовує результати розумової діяльності фахівця при вирішенні завдань контролю. ЕСК виконує функції накопичення та обробки сукупності формальних і евристичних знань від фахівців для використання їх при вирішенні завдань контролю ТС.

Аналіз ЕСК традиційної структури щодо здатності вирішення завдань контролю ТС дозволяє виявити наступні її недоліки:

знання під час контролю ТС важко формалізуються, тому що більшість рішень приймається експертом на інтуїтивному рівні та не може зрозуміло їм пояснена;

значна частина знань експерта не узгоджується з базою даних еталонних значень вимірюваних параметрів сигналів;

редагування, узгодження та усунення суперечностей бази знань з базою даних здійснюється оператором у ручному режимі з низькою оперативністю;

низька оперативність контролю та невикористання інтелектуального потенціалу ЕСК щодо її самонавчання;

відсутність можливості врахування змін контрольних параметрів ЗКР, що унеможливає зробити прогноз ТС більш достовірним за рахунок врахування тенденцій змін контрольних

параметрів ЗКР та властивостей емерджентності ЗКР;

база даних з даними контролю ТС під час життєвого циклу ЗКР не складається та не використовується для прогнозу зміни ТС та корегування міжконтрольного інтервалу.



Рис.1. Базова структура класичної експертної системи контролю

Ці недоліки свідчать про низьку ефективність застосування ЕСК традиційної структури для вирішення завдань контролю ТС ЗКР. Структура удосконаленої ЕСК повинна комплексно враховувати особливості контролю ТС ЗКР та усунути вказані вище недоліки.

Комплексність завдань контролю реалізує автоматизована ЕСК, структура якої наведена на рис. 2, яка за програмою контролю подає на ЗКР стимулюючі сигнали, вимірює вихідні реакції, поповнює базу еталонних значень вимірюваних параметрів сигналів та формує інформаційно-контрольні моделі поточного ТС ЗКР, які потім порівнюються за визначеним алгоритмом з інформаційно-контрольними моделями еталонного стану ЗКР.

Ця ЕСК, крім традиційних для автоматизованої СК модулів (модулі 1 та 2 на рис. 2), включає до себе модуль 3, в якому відбувається порівняння параметрів часових еталонних інформаційно-контрольних моделей ТС, отриманих на протязі життєвого циклу еталонної ЗКР та поточних параметрів інформаційно-контрольної моделі (сукупність усіх значень параметрів, що контролюються, “паспорт” ЗКР на момент контролю), що отримані під час чергового контролю ТС ЗКР. База даних інформаційної моделі справного ТС ЗКР формується на початку експлуатації завідомо справних ЗКР і зберігається

в архівному блоці бази знань ЕСК. Застосування інформаційно-контрольних моделей еталонного ТС ЗКР дозволяє підвищити оперативність контролю поточного ТС ЗКР та зробити прогноз ТС більш достовірним за рахунок урахування тенденцій змін контрольних параметрів ЗКР та властивостей емерджентності ЗКР, як СТС.

Результатом роботи ЕСК є висновок, що відображається на модулі відображення рішень: ЗКР є справною (несправною), працездатною (непрацездатною) (які параметри, що не є критичними, вийшли за межі або знаходяться у межах норми) та рекомендований наступний міжконтрольний інтервал.

Вхідними даними для роботи ЕСК є база даних контрольних параметрів еталонного ТС ЗКР, яка формується виробником методом зняття еталонних значень контрольних параметрів завідомо справної (нової) ЗКР. Запропонована комплексна ЕСК є інтелектуальною системою, тому що вона здатна накопичувати знання, навчатись та надавати інформацію для прогнозування змін у ТС ЗКР методом апроксимації дрейфу контрольних параметрів на час прогнозу. Система запам'ятовує знайдену несправність для даного типу ЗКР та поповнює базу знань статистичних залежностей відмов даного типу ЗКР.



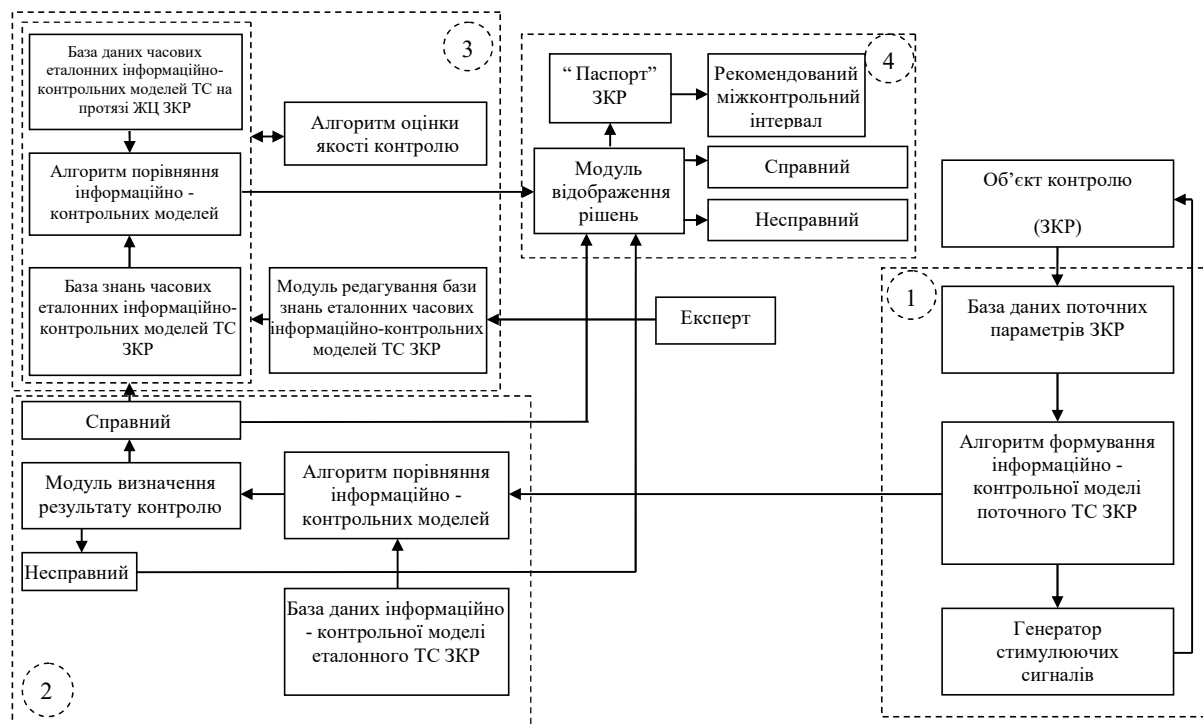


Рис.2. Удосконалена комплексна автоматизована експертна система контролю технічного стану зенітних керованих ракет

При наступному контролі іншої ЗКР цього типу вона рекомендує здійснити контроль у першу чергу параметрів, що є першими за рейтингом ймовірності несправності, якщо поточна інформаційно-контрольна модель ЗКР допускає таку несправність. ЕСК працює за аналогією з досвідченими фахівцями з контролю ЗКР на заводах-виробниках, які відновлюють ЗКР та знають типові несправності та найбільш ймовірні їх причини у конкретних ЗКР і перевіряють їх у першу чергу. Таким чином, ЕСК, що побудована за структурною схемою на рис. 2, накопичує знання щодо ймовірності несправності у базі знань, яка призначена для зберігання експертних знань про предметну область, що використовуються при вирішенні завдань експертною системою, запам'ятовує поточну інформаційно-контрольну модель ЗКР та складає їх базу даних, що дає можливість врахування змін контрольних параметрів ЗКР у часі для прогнозу зміни ТС ЗКР та рекомендувати наступний між контрольний інтервал.

### Висновки й перспективи подальших досліджень

Таким чином, КВС, що побудована за запропонованою структурою зі застосуванням ЕС буде мати наступні переваги:

можливість складання та поповнення баз даних с інформаційно-контрольними моделями ТС ЗКР, що дозволяє прогнозувати зміни ТС та корегувати інтервал проведення регламентних робіт з ЗКР;

високу достовірність визначення ТС ЗКР за допомогою використання інтелектуального алгоритму контролю з елементами самонавчання

та аналізу інформації щодо порівняння отриманих та попередніх інформаційно-контрольних моделей;

простоту уніфікації КВС з застосуванням ЕС за рахунок модульності її структури;

універсальність, тобто можливість застосування КВС на базі ЕС для контролю декількох типів ЗКР.

Запропонована універсальна ЕСК відрізняється від відомих ієрархічно модульною структурою, що дозволяє підвищити достовірність та оперативність контролю за рахунок формування та порівняння інформаційно-контрольних моделей поточного та еталонного ТС ЗКР та самонавчання ЕСК. Це дозволяє підвищити достовірність контролю ТС за рахунок аналізу інформації, що надають контрольні-інформаційні моделі, та використання сучасних інформаційних технологій у вигляді експертної системи, що включає: сформовані бази знань та даних, алгоритми логічного висновку, інтерфейс для ведення діалогу з користувачем, підсистему пояснень та підсистему придбання знань, що реалізовані в удосконаленій універсальній автоматизованій ЕСК.

Сукупність цих переваг забезпечує побудову універсальної уніфікованої високопродуктивної автоматизованої КВС зі змінною конфігурацією, яка дозволяє проводити автоматизований контроль ТС декількох типів ЗКР. Така універсальна автоматизована КВС буде відповідати технологічному рівню ЗКР, що зараз розробляються та забезпечить реалізацію стратегії експлуатації застарілих зразків ЗКР за технічним

станом з мінімально необхідними матеріальними та часовими витратами.

Перспективами подальших досліджень є розроблення алгоритму діагностування у вигляді дерева рішень ЕСК та розробка бази знань ЕСК. Перспективною є також розробка та впровадження

удосконалених методів вибіркового контролю ЗКР, та методів, що удосконалюють організацію роботи КВС, що дозволить зменшити навантаження на універсальну КВС, що побудована зі застосуванням сучасних інформаційних технологій.

### Література

**1. Коровин А.Н.** Ракетные комплексы ПВО: тенденции развития. <https://topwar.ru/2217-raketnye-kompleksy-pvo-tendencii-razvitiya.html>. **2. Карпенко Д.В.** Основні проблеми і напрями розвитку зенітного ракетного озброєння в Україні на довгострокову перспективу / Д.В. Карпенко, Д.А. Гриб, В.В. Лук'янчук, І.М. Ніколаєв // Новітні технології – для захисту повітряного простору. Тези доповідей. XIII наукова конференція ХУПС, 08-09 квітня 2015 року, Харків, 2015, с. 108. <http://www.hups.mil.gov.ua/assets/doc/science/conference/1/section06.pdf> **3. Прибілев Ю.Б.,** Сакович Л.В. Підхід до побудови уніфікованої універсальної автоматизованої контрольно-випробувальної станції ракетного озброєння. Науково-теоретичний та науково-практичний журнал "Наука і оборона", №1, 2017. С. 42-48. <http://nio.nuou.org.ua/article/view/158066/157411> **4. Прибілев Ю.Б.** Концепція побудови контрольно-випробувальної станції. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Київ: НУОУ, 2018. Вип. №2(32). С.103-106. <http://sit.nuou.org.ua/article/view/157983/157607> **5. Жердев М.К.** Напрями розвитку систем контролю технічного стану і діагностування складних технічних систем / [М.К.Жердев, В.В.Вишнівський, І.В.Пампуха, О.Ю.Скуйбіда]: зб. наук. Праць ВІКНУ імені Тараса Шевченка. 2006, № 3. С. 22–25. [http://www.library.univ.kiev.ua/ukr/host/viking/db/ftp/univ/znp\\_vi\\_knu/znp\\_vi\\_knu\\_2006\\_03.pdf](http://www.library.univ.kiev.ua/ukr/host/viking/db/ftp/univ/znp_vi_knu/znp_vi_knu_2006_03.pdf) **6. Коваленко А.С.** Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. Х.: ХУПС, 2014, № 2(38). <http://www.hups.mil.gov.ua/periodic-app/article/2387> С. 106-108. **7. Михальчук М.В.** Експертна система технічної діагностики для визначення технічного стану елементів комплексів засобів автоматизації. /

М.В. Михальчук // Системи обробки інформації. Х.: ХУПС, 2014, вип. 2 (38). С. 29-33. <http://www.hups.mil.gov.ua/periodic-app/article/11415>

**8. Шкуліпа П.А.** Проблема розробки інформаційних технологій для побудови автоматизованих систем технічного діагностування об'єктів радіоелектронної техніки // Збірник наукових праць Національної академії Державної прикордонної служби України імені Б. Хмельницького. – Хмельницький, 2012, № 58, ч. II. С. 163-166. **9. Прибілев Ю.Б.** Удосконалена комплексна автоматизована експертна система контролю технічного стану та діагностики ракетного озброєння. / Ю.Б. Прибілев // Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". К.: НУОУ, 2017, вип. №1(28). С.114-119. [file:///C:/Users/pribi/Downloads/sitsbo\\_2017\\_1\\_22.pdf](file:///C:/Users/pribi/Downloads/sitsbo_2017_1_22.pdf)

**10. Карпенко Д.В.** Стан та перспективи розвитку зенітного ракетного озброєння Повітряних Сил Збройних Сил України / Д.В. Карпенко // Науковий журнал "Наука і техніка Повітряних Сил Збройних Сил України". – 2017, № 2(27). С. 75-78. <http://www.hups.mil.gov.ua/periodic-app/article/17539>

**11. Ганин С.М.,** Карпенко А.М. Зенитная ракетная система С-300. (Невский бастион). Санкт-Петербург, 2011. 71 с. **12. Акопян 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-rakety>. **13. Лук'янчук В.В.,** Ніколаєв І.М., Опенько П.В., Дзюбенко Ю.А. Шляхи і принципи розвитку технологічного базису зенітного ракетного озброєння / Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Київ: НУОУ, 2019. Вип. №3(36). С.75-82. <https://doi.org/10.33099/2311-7249/2019-36-3-75-82>

## ПОДХОД К ПОСТРОЕНИЮ УНИВЕРСАЛЬНОЙ АВТОМАТИЗИРОВАННОЙ КОНТРОЛЬНО-ИСПЫТАТЕЛЬНОЙ СТАНЦИИ С ПРИМЕНЕНИЕМ ЭКСПЕРТНЫХ СИСТЕМ

*Александр Юрьевич Пермяков (доктор технических наук, профессор)*

*Юрий Борисович Прибылев (кандидат технических наук, доцент)*

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

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

*В статье разрабатывается подход к построению универсальной автоматизированной контрольно-испытательной станции с применением экспертных систем. Показано, что наиболее сложной задачей для определения достоверного технического состояния зенитных управляемых ракет является проведение контрольно-измерительных операций с помощью контрольно-испытательных станций.*

*Обоснована перспективность использования экспертных систем в области технического контроля, которая позволяет повысить эффективность контроля технического состояния бортового оборудования зенитных управляемых ракет за счет учета знаний и опыта экспертов, накопления*

знаний и реализации самообучения экспертной системы контроля. Предложено формирование информационно-контрольных моделей текущего технического состояния зенитных управляемых ракет (совокупность всех значений контролируемых параметров и изменение их во времени, "паспорт" зенитной управляемой ракеты), что позволяет сделать прогноз технического состояния зенитных управляемых ракет более достоверным за счет учета тенденций изменений контрольных параметров. Это позволит сделать расширенный вывод по результатам работы экспертной системы контроля: зенитная управляемая ракета является исправной (неисправной) или работоспособной (неработоспособной), какие параметры вышли за пределы нормы и какой рекомендован следующий межконтрольный интервал.

Предложенная структура контрольно-испытательной станции реализует задачи контроля комплексно: по программе контроля подает стимулирующие сигналы, анализирует выходные реакции, пополняет базу эталонных значений измеряемых параметров сигналов и формирует информационно-контрольные модели текущего технического состояния зенитной управляемой ракеты, которые затем сравниваются по определенному алгоритму с информационно-контрольными моделями эталонного состояния зенитной управляемой ракеты, которая контролируется. Предложенный подход к построению универсальной автоматизированной контрольно-испытательной станции с применением экспертных систем обеспечит построение универсальной унифицированной автоматизированной контрольно-испытательной станции с изменяемой конфигурацией, которая позволит проводить автоматизированный контроль нескольких образцов зенитных управляемых ракет с высокой степенью достоверности и рекомендовать межконтрольный интервал его проведения.

**Ключевые слова:** зенитный ракетный комплекс, зенитная управляемая ракета, контрольно-испытательная станция, экспертная система контроля, информационно-контрольная модель.

## APPROACH TO BUILDING A UNIVERSAL AUTOMATED CONTROL AND TEST STATION WITH USE OF EXPERT SYSTEMS

*Alexander Permjakov (Doctor of Technical Sciences, Professor)*

*Yurii Pribyliev (Candidate of Technical Sciences, Associate Professor)*

*Viktor Bobyluov (Candidate of Military Sciences, Senior Research Officer)*

*National Defense University of Ukraine named by Ivan Cherniakhovsky, Kyiv, Ukraine*

*The article develops an approach to building a universal automated control and testing station using expert systems. An analysis of the airborne equipment of anti-aircraft guided missiles of methods and means of their control showed that the most difficult task to determine a reliable technical condition is to conduct, using test stations, the control and measurement operations of electronic anti-aircraft guided missiles.*

*The prospects of using expert systems in the field of technical control is shown, which allows to increase the effectiveness of monitoring the technical condition of airborne equipment of anti-aircraft guided missiles by taking into account the knowledge of experts, accumulating knowledge, taking into account the experience of experts and implementing self-training of an expert control system. The formation of information-control models of the current technical condition of anti-aircraft guided missiles (the set of all values of controlled parameters and their change in time, the "passport" of anti-aircraft guided missiles) is proposed, which makes it possible to make the forecast of the technical condition of anti-aircraft guided missiles more reliable by taking into account trends in changes in control parameters. This allows us to draw an extended conclusion on the results of the expert monitoring system: the anti-aircraft guided missile is operational (malfunctioning) or operational (inoperative), the parameters are outside the normal range and the following intercontrol interval is recommended.*

*The proposed structure of the control and testing station implements the control tasks in a comprehensive manner: according to the control program it provides stimulating signals, analyzes output reactions, replenishes the base of reference values of the measured signal parameters and forms information-control models of the current technical condition of the anti-aircraft guided missile, which are then compared using an algorithm with information -controlled models of the reference state of the anti-aircraft guided missile, which is controlled. The proposed approach to the construction of a universal automated control and test station using expert systems will ensure the construction of a universal unified automated control and test station with a variable configuration, which will allow automated control of several samples of anti-aircraft guided missiles with a high degree of reliability and recommend an intercontrol interval for it.*

**Key words:** anti-aircraft missile system, anti-aircraft guided missile, control and testing station, expert control system, information-control model.

## References

- 1. Korovyn A.N.** Raketnyie kompleksi PVO: tendentsii razvitiya. <https://topwar.ru/2217-raketnye-komplekisy-pvo-tendentsii-razvitiya.html>. **2. Karpenko D.V.** Osnovni problemy i naprjamy rozvytku zenitnogo raketnogo ozbrojennja v Ukraini na dovghostrokovu perspektivu / D.V. Karpenko, D.A. Ghryb, V.V. Luk'janchuk, I.M. Nikolajev // Novitni tekhnologhiji – dlja zakhystu povitrijanogho prostoru. Tezy dopovidej. XIII naukova konferencija KhUPS, 08-09 kvitnja 2015 roku, Kharkiv, 2015, s. 108. <http://www.hups.mil.gov.ua/assets/doc/science/conference/1/1/section06.pdf> **3. Pribyljev Ju.B.,** Sakovyh L.V. Pidkhid do pobudovy unifikovanoj universalnoj avtomatyzovanoj kontroljno-vyprobuvalnoj stanciji raketnogo ozbrojennja. Naukovo-teoretychnyj ta naukovo-praktychnyj zhurnal "Nauka i oborona", #1, 2017. S. 42-48. <http://nio.nuou.org.ua/article/view/158066/157411>. **4. Pribyljev Ju.B.** Konceptija pobudovy kontroljno-vyprobuvalnoj stanciji. Naukovyj zhurnal "Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony". Kyjiv: NUOU, 2018. Vyp. #2(32). S.103-106. <http://sit.nuou.org.ua/article/view/157983/157607> **5. Zherdjev M. K.** Naprjamy rozvytku system kontrolju tekhnichnogho stanu i diagnostuvannja skladnykh tekhnichnykh system / [M.K.Zherdjev, V.V.Vyshnivs'kyj, I.V.Pampukha, O.Ju. Skujbida]: zb. nauk. Pracj VIKNU imeni Tarasa Shevchenka. – 2006. – №3. – S.22–25. [http://www.library.univ.kiev.ua/ukr/host/viking/db/ftp/univ/znp\\_vi\\_knu/znp\\_vi\\_knu\\_2006\\_03.pdf](http://www.library.univ.kiev.ua/ukr/host/viking/db/ftp/univ/znp_vi_knu/znp_vi_knu_2006_03.pdf) **6. Kovalenko A.S.** Analiz effektivnosti ispolzovaniya ekspertnoj sistemyi tehnikeskoy diagnostiki s traditsionnoj strukturoj / A.S. Kovalenko, A.A. Smirnov, A.V. Kovalenko // Sistemi ozbroEnnja I vlyskova tehnlka. H.: HUPS, 2014. – # 2(38). – S. 106-108. <http://www.hups.mil.gov.ua/periodic-app/article/2387> **7. Mykhaljchuk M.V.** Ekspertna sistema tekhnichnoj diagnostyky dlja vyznachennja tekhnichnogho stanu elementiv kompleksiv zasobiv avtomatyzaciji. / M.V. Mykhaljchuk // Systemy obrobky informaciji. - Kh.: KhUPS, 2014. – Vyp. 2 (38). – S. 29–33. <http://www.hups.mil.gov.ua/periodic-app/article/11415> **8. Shkulipa P.A.** Problema rozrobky informacijnykh tekhnologhij dlja pobudovy avtomatyzovanykh system tekhnichnogho diagnostuvannja ob'ektiv radioelektronnoj tekhniki // Zbirnyk naukovykh pracj Nacionalnoj akademiji Derzhavnoj prykordonnoj sluzhby Ukrainy imeni B. Khmeljnyckogho. – Khmeljnyckyj, 2012. – №58, ch.II. – S.163 – 166. **9. Pribyljev Ju.B.** Udoskonalena kompleksna avtomatyzovana ekspertna sistema kontrolju tekhnichnogho stanu ta diagnostyky raketnogo ozbrojennja. / Ju.B. Pribyljev // Naukovyj zhurnal "Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony". K.: NUOU, 2017, vyp.#1(28). S.114-119. [file:///C:/Users/pribi/Downloads/sitsbo\\_2017\\_1\\_22.pdf](file:///C:/Users/pribi/Downloads/sitsbo_2017_1_22.pdf) **10. Karpenko D.V.** Stan ta perspektyvy rozvytku zenitnogo raketnogo ozbrojennja Povitrijanykh Syl Zbrojnykh Syl Ukrainy / D.V. Karpenko // Naukovyj zhurnal "Nauka i tekhnika Povitrijanykh Syl Zbrojnykh Syl Ukrainy". – 2017, # 2(27). S. 75-78. <http://www.hups.mil.gov.ua/periodic-app/article/17539> **11. Ganin S.M.,** Karpenko A.M. Zenitnaya raketnaya sistema S-300. (Nevskiy bastion). Sankt-Peterburg, 2011. 71 s. **12. Akopyan I.** Mozg rakety: osobennosti postroeniya i tendentsii razvitiya golovok samonavedeniya dlya raket klassa "poverhnost-vozduh" i "vozduh-vozduh". Vozdushno-kosmicheskaya oborona, #3 (28) 2006. <http://militaryarticle.ru/voenno-kosmicheskaya-oborona/2006/12386-mozg-rakety>. **13. Luk'janchuk V.V.,** Nikolajev I.M., Openjko P.V., Dzubenko Ju.A. Shljakhy i pryncypy rozvytku tekhnologhichnogho bazysu zenitnogo raketnogo ozbrojennja / Naukovyj zhurnal "Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony". Kyjiv: NUOU, 2019. Vyp. #3(36). S.75-82. <https://doi.org/10.33099/2311-7249/2019-36-3-75-82>

Олександр Миколайович Правдивець<sup>1</sup>  
Віктор Васильович Козлов<sup>2</sup>

<sup>1</sup>Генеральний штаб Збройних Сил України, Київ, Україна

<sup>2</sup>Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

## МЕТОДИКА ВИЗНАЧЕННЯ КІЬКОСТІ КОМПЛЕКТІВ КЛІЄНТСЬКОЇ ЧАСТИНИ ЄДИНОГО ДЕРЖАВНОГО РЕЄСТРУ ВІЙСЬКОВОЗОВОБ'ЯЗАНИХ

У статті запропоновано методику визначення кількості комплектів клієнтської частини Єдиного державного реєстру військовозобов'язаних.

Методика відображає логічну послідовність дій, яка складається з трьох етапів: формування вихідних даних, визначення основних показників та визначення кількості комплектів клієнтської частини Єдиного державного реєстру військовозобов'язаних, при цьому вихідні дані методики за призначенням розподілені на шість груп.

Запропонована методика охоплює усі напрямки робіт, які виконуються підрозділами військових комісаріатів, що дає змогу:

визначити кількість комплектів клієнтської частини Єдиного державного реєстру військовозобов'язаних для виконання операції з ведення військового обліку призовників та військовозобов'язаних у військових комісаріатах;

розрахувати необхідну чисельність операторів Єдиного державного реєстру військовозобов'язаних з урахуванням завдань, які покладаються на структурні підрозділи військових комісаріатів, в межах визначеного ліміту чисельності військовослужбовців і працівників та провести перерозподіл обов'язків між існуючими посадовими особами військових комісаріатів.

Отримані результати дослідження можуть бути використані під час проведення розрахунків кількості комплектів клієнтської частини Єдиного державного реєстру військовозобов'язаних для удосконалення організаційно-штатної структури військових комісаріатів та розроблення керівних документів з питань визначення відповідних норм їх забезпечення та постачання відповідними зразками озброєння та військової техніки.

**Ключові слова:** військовий облік; клієнтська частина; Єдиний державний реєстр військовозобов'язаних.

### Вступ

**Постановка проблеми.** На сучасному етапі свого будівництва та розвитку Збройні Сили України (далі – ЗС України) проводять заходи щодо впровадження в їх діяльність автоматизованих інформаційно-телекомунікаційних систем (далі – АІТС), зокрема АІТС Єдиного державного реєстру військовозобов'язаних (ЄДРВ).

Відповідно до [1] АІТС ЄДРВ була прийнята на постачання ЗС України у 2019 року.

Аналіз результатів впровадження в діяльність ЗС України зазначеної АІТС викрило ряд проблемних питань, зокрема відсутності методики визначення кількості комплектів клієнтських частин (далі – КЧ) АІТС для її нарощування та розгортання в районних (міських) військових комісаріатах (далі – Р(М)ВК).

У свою чергу відповідно до [2] Р(М)ВК є органами ведення реєстру, на які згідно з [2 – 4] покладається виконання таких завдань:

1) ведення військового обліку громадян України - військовозобов'язаних (призовників);

2) планування та виконання заходів з мобілізації, призову на строкову військову службу, прийняття на військову службу за контрактом;

3) інформаційне забезпечення осіб, звільнених з військової служби, які мають право на пенсію, та членів сімей загиблих військовослужбовців відомостями щодо військового обліку.

Крім того, відповідно до [5] ефективне функціонування всієї системи військового обліку громадян України в цілому залежить від роботи Р(М)ВК.

У зв'язку з цим, виникла необхідність подальшого дослідження, що вимагає вирішення актуального наукового завдання, яке полягає в розробці методики визначення кількості комплектів КЧ АІТС “Оберіг” в Р(М)ВК.

**Аналіз остатніх досліджень і публікацій.** Результати аналізу останніх досліджень і публікацій присвячених ЄДРВ [6-8] показав, що

проблеми формування методичного апарату щодо визначення кількості комплектів клієнтських частин зазначеної АІТС в Р(М)ВК не досліджувались та не розглядалися.

**Метою** даної статті є розробка методики визначення кількості комплектів КЧ АІТС ЄДРВ у Р(М)ВК.

### Виклад основного матеріалу дослідження

Вихідні дані методики визначення кількості комплектів КЧ АІТС ЄДРВ у Р(М)ВК за призначенням можливо розподілити на наступні групи:

група 1 – дані щодо дійсного часу роботи комплекту КЧ АІТС;

група 2 – дані необхідні для підрахунку витрат часу на проведення операцій робіт із взяття призовника (військовозобов'язаного) на військовий облік;

група 3 – дані необхідні для підрахунку витрат

часу на проведення операцій із відновлення на військовому обліку призовника (військовозобов'язаного);

група 4 – дані необхідні для підрахунку витрат часу на проведення операцій із зміни в облікових даних призовника (військовозобов'язаного);

група 5 – дані необхідні для підрахунку витрат часу на проведення операцій із зняття з військового обліку призовника (військовозобов'язаного);

група 6 – дані необхідні для підрахунку витрат часу на проведення операцій із довідково-інформаційної та архівної роботи.

Час на виконання тих чи інших операцій з базою даних в основному визначено у [6].

Методика визначення кількості комплектів КЧ АІТС ЄДРВ у Р(М)ВК відображає логічну послідовність дій, яка складається з трьох етапів. Загальна схема послідовності дій наведена на рисунку 1.

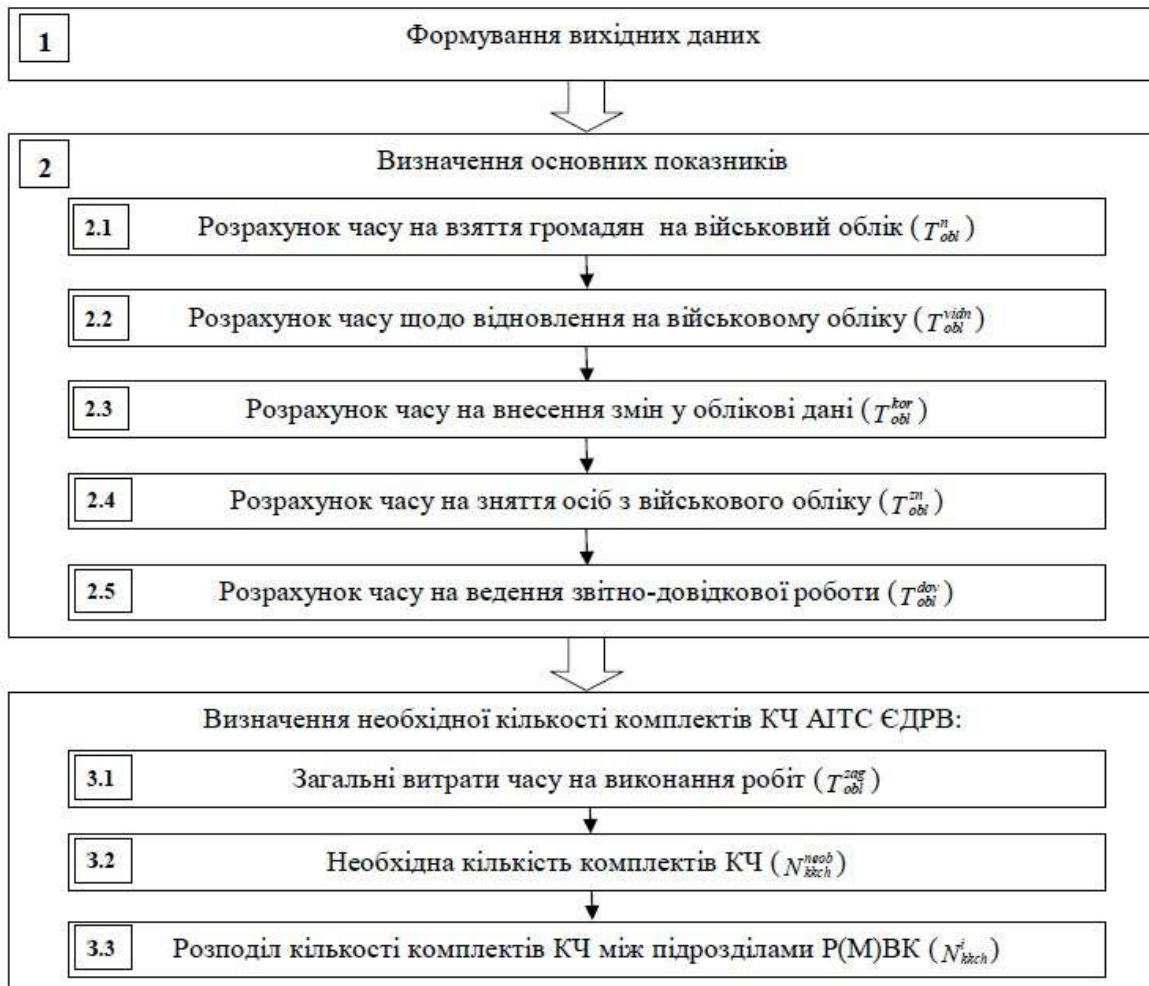


Рис. 1. Послідовність дій визначення комплектів КЧ АІТС ЄДРВ

**На першому етапі (блок 1)** забезпечується формування вихідних даних, до яких належать:

середньостатистичні дані щодо: кількості призовників, які протягом року підлягають взяттю на ВО ( $Q_{prin}^{priz}$ ), зняттю з військового обліку чи внесенню змін до їх облікових даних; кількості військовозобов'язаних, які набули громадянства

України чи з інших причин протягом року підлягають первинному взяттю на військовий облік ( $Q_{prin}^{grom}$ ), зняттю з військового обліку чи внесенню змін до їх облікових даних; кількості інформаційно-довідкових матеріалів;

нормативні показники [9] витрат часу на проведення тих чи інших операцій;

дійсний річний фонд роботи комплексу КЧ АІТС ЄДРВ ( $F_d^{kkch}$ ), який обраховується в машиногодинах як здобуток різниці між річним фондом робочого часу оператора ( $F_{fond}^{oper}$ ), та часу, який не пов'язаний з веденням бази даних АІТС ЄДРВ {участь у заняттях ( $F_{zan}^{oper}$ ) та нарадах ( $F_{nar}^{oper}$ ), несення служби у добовому наряді ( $F_{st}^{oper}$ ), відпустки ( $F_{vp}^{oper}$ ), лікувально-профілактичні заходи ( $F_{lik}^{oper}$ ) та відрядження ( $F_{vidr}^{oper}$ )} у днях та денною нормою роботи комплексу КЧ АІТС ЄДРВ ( $T_{d-n}^{kkch}$ ) у годинах:

$$F_d^{kkch} = (F_{fond}^{oper} - F_{zan}^{oper} - F_{nar}^{oper} - F_{st}^{oper} - F_{vp}^{oper} - F_{lik}^{oper} - F_{vidr}^{oper}) T_{d-n}^{kkch} \quad (1)$$

При цьому денна норма ( $T_{d-n}^{kkch}$ ) комплексу КЧ АІТС ЄДРВ обраховується як різниця між здобутком денної норми робочих годин ( $T_{d-n}$ ) на астрономічну тривалість години ( $t_a$ ) (хв.) та нормами часу на перерви ( $t_p$ ) (хв.) для відпочинку оператора з перерахунком ( $T_{d-n}^{kkch}$ ) у машиногодинах:

$$T_{d-n}^{kkch} = \frac{T_{d-n} * t_a - \sum t_p}{60 \text{ хв}}, \quad (2)$$

На **другому етапі (блок 2)** визначають основні показники необхідні для проведення подальших розрахунків, а саме:

розраховується (**блок 2.1**) час роботи комплексу КЧ АІТС ЄДРВ щодо взяття громадян на військовий облік.

Спочатку розраховується у хвиликах час необхідний для введення в базу даних АІТС ЄДРВ записів щодо взяття однієї особи на військовий облік, яка досягла призовного віку ( $T_{obl}^{priz}$ ) або військовозобов'язаного, дані на якого з тих чи інших причин не були введені в базу даних раніше ( $T_{obl}^{grom}$ ):

$$T_{obl}^{priz} = t_{norm}^{stv} + t_{norm}^{vz} + t_{norm}^{cifr} + T_{vsi}^{priz}, \quad (3)$$

$$T_{obl}^{grom} = t_{norm}^{stv} + t_{norm}^{vz} + t_{norm}^{cifr} + T_{vsi}^{vzob}, \quad (4)$$

де:  $t_{norm}^{stv}$  – час, який витрачається на створення облікового запису (хв.);

$t_{norm}^{vz}$  – час, який витрачається на взяття на облік створеного запису (хв.);

$t_{norm}^{cifr}$  – час, який витрачається на отримання відцифрованого образу обличчя (хв.);

$T_{vsi}^{priz}$  – сумарні витрати часу на первинне внесення службової інформації про призовника (хв.);

$T_{vsi}^{vzob}$  – сумарні витрати часу на первинне внесення службової інформації про військовозобов'язаного (хв.);

З урахуванням отриманих даних розраховується у машиногодинах загальний час

( $T_{obl}^n$ ), який протягом року витрачається на внесення нових записів щодо взяття на військовий облік призовників і військовозобов'язаних:

$$T_{obl}^n = \frac{T_{obl}^{priz} * Q_{priz}^{priz} + T_{obl}^{grom} * Q_{priz}^{grom}}{t_a}, \quad (5)$$

Далі (**блок 2.2**) розраховується у машиногодинах час ( $T_{obl}^{vidn}$ ), який протягом року витрачається на коригування записів у базу даних АІТС ЄДРВ стосовно осіб, які були внесені у загальну базу даних ЄДРВ раніше та відновлюються в на військовому обліку після звільнення в запас зі строкової військової служби ( $Q_{vidn}^{vsl}$ ) або військової служби за контрактом ( $Q_{vidn}^{kont}$ ), прибули з інших місцевостей ( $Q_{vidn}^{migr}$ ), звільнені з органів та підрозділів національної поліції ( $Q_{vidn}^{N-P}$ ), повернулися з тривалого (понад 3 місяці) перебування за кордоном ( $Q_{vidn}^{zak}$ ), припинили альтернативну службу ( $Q_{vidn}^{alt}$ ):

$$T_{obl}^n = \frac{T_{vidn}^{vsl} + T_{vidn}^{kont} + T_{vidn}^{migr} + T_{vidn}^{N-P} + T_{vidn}^{zak} + T_{vidn}^{alt}}{t_a} = \frac{Q_{vidn}^{vsl} * \sum_{i=1}^k t_{i,norm}^{vsl} + Q_{vidn}^{kont} * \sum_{i=1}^k t_{i,norm}^{kont} + Q_{vidn}^{migr} * \sum_{i=1}^k t_{i,norm}^{migr} + Q_{vidn}^{N-P} * \sum_{i=1}^k t_{i,norm}^{N-P} + Q_{vidn}^{zak} * \sum_{i=1}^k t_{i,norm}^{zak} + Q_{vidn}^{alt} * \sum_{i=1}^k t_{i,norm}^{alt}}{t_a} \quad (6)$$

де:  $T_{vidn}^{vsl}$  – час необхідний для коригування даних для відновлення на військовому обліку осіб звільнених в запас після проходження строкової військової служби (хв.);

$\sum_{i=1}^k t_{i,norm}^{vsl}$  – сумарний час на виконання k і-тих нормативів з уведення даних на одну особу звільненої з військової служби за призовом;

$T_{vidn}^{kont}$  – час необхідний для коригування даних для відновлення на військовому обліку осіб звільнених в запас після військової служби за контрактом (хв.);

$\sum_{i=1}^k t_{i,norm}^{kont}$  – сумарний час на виконання k і-тих нормативів з уведення даних на одну особу звільненої з військової служби за контрактом (хв.);

$T_{vidn}^{migr}$  – час необхідний для коригування даних на відновлення на військовому обліку осіб, які прибули з іншої місцевості поза межами відповідальності Р(М)ВК (хв.);

$\sum_{i=1}^k t_{i,norm}^{migr}$  – сумарний час на виконання k і-тих нормативів з уведення даних на одну особу, яка прибула з іншої місцевості (хв.);

$T_{vidn}^{N-P}$  – час необхідний для коригування даних на відновлення на військовому обліку осіб, які звільняються зі служби у Національній поліції, МВС, оперативно-рятувальній службі цивільного захисту, Державній кримінально-виконавчій службі, центральному органі виконавчої влади, що реалізує державну податкову і митну політику,

виключені з військового обліку СБУ та служби зовнішньої розвідки і підлягають відновленню (взяттю) на ВО військовозобов'язаних (хв.);

$$\sum_{i=1}^k t_{i\text{norm}}^{N-P} - \text{сумарний час на виконання } k \text{ і-тих}$$

нормативів з уведення даних на одну особу звільненої із служби з Національної поліції, МВС, оперативно-рятувальної служби цивільного захисту, Державної кримінально-виконавчої служби, центрального органу виконавчої влади, що реалізує державну податкову і митну політику, виключені з військового обліку СБУ та служби зовнішньої розвідки (хв.);

$T_{\text{vidn}}^{\text{zak}}$  – час необхідний для коригування даних на відновлення на військовому обліку осіб, які прибувають із-за кордону (хв.);

$$\sum_{i=1}^k t_{i\text{norm}}^{\text{zak}} - \text{сумарний час на виконання } k \text{ і-тих}$$

нормативів з уведення даних на одну особу, яка прибула зі-за кордону після тривалої (понад три місяці) відсутності в Україні (хв.);

$T_{\text{vidn}}^{\text{alt}}$  – час необхідний для коригування даних на відновлення на військовому обліку осіб, які припинили альтернативну службу (хв.);

$$\sum_{i=1}^k t_{i\text{norm}}^{\text{alt}} - \text{сумарний час на виконання } k \text{ і-тих}$$

нормативів з уведення даних на одну особу, яка припинила альтернативну службу (хв.).

Наступним (блок 2.3) розраховується з переведенням у машинодини час, який протягом року витрачається на коригування записів у базу даних АІТС ЄДРВ ( $T_{\text{obl}}^{\text{kor}}$ ) стосовно осіб, які заброньовані за підприємствами (установами, закладами, організаціями) на період мобілізації та на военний час ( $Q_{\text{obl}}^{\text{bron}}$ ), мають мобілізаційні розпорядження ( $Q_{\text{obl}}^{\text{mob}}$ ), уклали контракт на проходження служби у військовому резерві ( $Q_{\text{obl}}^{\text{rez}}$ ), а також осіб, у яких змінилися облікові дані щодо місця проживання, сімейного стану, місця роботи, стану здоров'я тощо ( $Q_{\text{obl}}^{\text{zm}}$ ):

$$T_{\text{obl}}^n = \frac{Q_{\text{obl}}^{\text{bron}} * t_{\text{norm}}^{\text{bron}} + Q_{\text{obl}}^{\text{mob}} * t_{\text{norm}}^{\text{mob}} + Q_{\text{obl}}^{\text{rez}} * t_{\text{norm}}^{\text{rez}} + Q_{\text{obl}}^{\text{zm}} * \sum_{i=1}^k t_{i\text{norm}}^{\text{zm}}}{t_a}, \quad (7)$$

де:  $t_{\text{norm}}^{\text{bron}}$  – нормативний час на внесення записів щодо бронювання однієї особи за підприємством (закладом, установою) (хв.);

$t_{\text{norm}}^{\text{mob}}$  – нормативний час на внесення записів щодо видачі одній особі мобілізаційного розпорядження (хв.);

$t_{\text{norm}}^{\text{rez}}$  – нормативний час на внесення записів щодо укладення особою контракту на проходження служби у військовому резерві (хв.);

$t_{i\text{norm}}^{\text{zm}}$  – нормативний час на внесення і-того запису стосовно зміни сімейного положення, народження дітей, зміни місця роботи чи

домашньої адреси тощо (хв.).

У блоці 2.4 розраховується час ( $T_{\text{obl}}^{\text{zn}}$ ), який протягом року витрачається на зняття (виключення) з військового обліку осіб, які вибули на постійне місце проживання поза межі відповідальності даного Р(М)ВК ( $Q_{\text{zn}}^{\text{migr}}$ ), призвані на строкову військову службу ( $Q_{\text{zn}}^{\text{priz}}$ ) чи прийняті на військову службу за контрактом ( $Q_{\text{zn}}^{\text{kont}}$ ), прийняті на службу до органів і підрозділів національної поліції ( $Q_{\text{zn}}^{N-P}$ ), вибули за межі України на термін понад три місяці ( $Q_{\text{zn}}^{\text{zak}}$ ), вибувають за кордон на постійне місце проживання ( $Q_{\text{zn}}^{\text{grom}}$ ), за рішенням суду визнані неідездатними, оголошені померлими чи пропалими безвісти ( $Q_{\text{zn}}^{\text{pom}}$ ), признані непридатними до військової служби у мирний та военний час ( $Q_{\text{zn}}^{\text{med}}$ ), досягли граничного віку перебування у запасі ( $Q_{\text{zn}}^{\text{vik}}$ ), засуджені до позбавлення волі ( $Q_{\text{zn}}^{\text{sud}}$ ):

$$T_{\text{obl}}^{\text{zn}} = \frac{(Q_{\text{zn}}^{\text{migr}} + Q_{\text{zn}}^{\text{priz}} + Q_{\text{zn}}^{\text{kont}} + Q_{\text{zn}}^{N-P} + Q_{\text{zn}}^{\text{zak}} + Q_{\text{zn}}^{\text{grom}} + Q_{\text{zn}}^{\text{pom}} + Q_{\text{zn}}^{\text{med}} + Q_{\text{zn}}^{\text{vik}} + Q_{\text{zn}}^{\text{sud}}) * t_{\text{norm}}^{\text{zn}}}{t_a}, \quad (8)$$

де:  $t_{\text{norm}}^{\text{zn}}$  – нормативний час на зняття особи з військового обліку (хв.);

У блоці 2.5 розраховується час, який протягом року витрачається на архівно-довідкову роботу  $T_{\text{obl}}^{\text{dov}}$  за зверненнями громадян та згідно з табелем термінових донесень, з приведенням до машиногодин:

$$T_{\text{obl}}^{\text{dov}} = \frac{Q_{\text{dov}}^{\text{grom}} * t_{\text{rozr}}^{\text{dov}} + Q_{\text{dov}}^{\text{zvit}} * t_{\text{rozr}}^{\text{zvit}}}{t_a}, \quad (9)$$

де:  $Q_{\text{dov}}^{\text{grom}}$  – середньостатистичні дані щодо кількості громадян, які звертаються за отриманням довідок

$t_{\text{rozr}}^{\text{dov}}$  – середньостатистичні дані щодо часу, який витрачається на надання однієї довідки (хв.);

$Q_{\text{dov}}^{\text{zvit}}$  – Кількість донесень за рік згідно з табелем термінових донесень;

$t_{\text{rozr}}^{\text{zvit}}$  – усереднені дані щодо часу, який витрачається на підготовку одного донесення (хв.);

На третьому етапі (блок 3) визначають необхідну кількість комплектів КЧ АІТС ЄДРВ при цьому:

Після отримання часткових показників часу, який витрачається на виконання тих чи інших операцій, розраховуються (блок 3.1) загальні витрати часу  $T_{\text{obl}}^{\text{zag}}$  на виконання робіт із залученням бази даних АІТС ЄДРВ:

$$T_{\text{obl}}^{\text{zag}} = T_{\text{obl}}^n + T_{\text{obl}}^{\text{vidn}} + T_{\text{obl}}^{\text{kor}} + T_{\text{obl}}^{\text{zn}} + T_{\text{obl}}^{\text{dov}}, \quad (10)$$

І на завершення етапу (блок 3.2) визначається кількість комплектів КЧ АІТС ЄДРВ ( $N_{\text{kkch}}^{\text{neob}}$ ) з урахуванням виділення одного комплекту



військовому комісару для здійснення контролю та отримання довідкової інформації в реальному часі, без залучення посадових осіб Р(М)ВК:

$$N_{kkch}^{neob} = \frac{T_{zag}^{obl}}{F_{d}^{kkch}} + 1, \quad (11)$$

Під час проведення розрахунків розподілу комплектів КЧ АІТС ЄДРВ ( $N_{kkch}^i$ ) між підрозділами враховується коефіцієнт участі ( $k_{uch}^i$ ) і-того підрозділу у загальному навантаженні на АІТС ЄДРВ цього Р(М)ВК (отримані розрахунки округляються до цілих одиниць):

$$N_{kkch}^i = (N_{kkch}^{neob} - 1) * k_{uch}^i, \quad (12)$$

### Висновки й перспективи подальших досліджень

Запропонована методика охоплює усі напрямки робіт, які виконуються підрозділами Р(М)ВК, що дає змогу:

визначити кількість комплектів КЧ АІТС ЄДРВ для виконання операцій з ведення військового обліку призовників та військовозобов'язаних в

АІТС “Оберіг”;

розрахувати необхідну чисельність операторів АІТС ЄДРВ з урахуванням завдань, які покладаються на структурні підрозділи Р(М)ВК, визначеного ліміту чисельності військовослужбовців і працівників та провести перерозподіл обов'язків між існуючими посадовими особами.

Забезпечення Р(М)ВК необхідною кількістю комплектів КЧ АІТС ЄДРВ дозволить:

прискорити роботу Р(М)ВК з формування бази даних ЄДРВ;

відмовитися від зайвої роботи з ведення військового обліку військовозобов'язаних і призовників на паперових носіях.

Отримані результати дослідження можуть бути використані під час проведення розрахунків кількості комплектів КЧ АІТС ЄДРВ, удосконалення організаційно-штатної структури Р(М)ВК та розроблення керівних документів з питань визначення відповідних норм забезпечення та постачання.

### Література

1. **Наказ Міністерства оборони України** від 15.04.2019 № 180 “Про прийняття на постачання та введення в експлуатацію Збройних Сил України автоматизованої системи Єдиного державного реєстру військовозобов'язаних, шифр “Оберіг”. 2. **Закон України** “Про Єдиний державний реєстр військовозобов'язаних”. 3. **Постанова Кабінету Міністрів України** від 07.12.2016 № 921 “Про затвердження Порядку організації та ведення військового обліку призовників і військовозобов'язаних”. 4. **Наказ Міністерства оборони України** від 08.08.2017 № 418 “Про затвердження Порядку ведення Єдиного державного реєстру військовозобов'язаних”. 5. **Правдивець О.М.**, Аналіз чинників, які впливають на функціонування системи військового обліку громадян України, Збірник наукових праць Національної академії прикордонної служби України 2016, № 1(67), С.223-229. 6.

**Правдивець О.М.**, “Нормативно-правове забезпечення створення та функціонування інформаційної автоматизованої системи військового обліку громадян України”, Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ, 2015, № 3 (55), С. 130-132. 7. **Правдивець О.М.**, Челобітченко О.О., Бабенко С.В. “Модель системи військового обліку громадян”. Труді університету, НУОУ, 2017, № 6 (145), ін. № 48028, с. 114 – 120. 8. **Правдивець О.М.**, Челобітченко О.О., Якименко С.В., Хардель Р.З. “Методика підготовки операторів єдиного державного реєстру військовозобов'язаних районних (міських) військових комісаріатів”, Труді університету, 2018, № 3 (148), ін. № 48275С. 142-150. 9. **Наказ командувача Сухопутних військ Збройних Сил України** від 12.04.2019 № 188 “Про затвердження доповнень до Збірника нормативів бойової підготовки Сухопутних військ Збройних Сил України 2002 року”.

## МЕТОДИКА ОПРЕДЕЛЕНИЯ КОЛИЧЕСТВА КОМПЛЕКТОВ КЛИЕНТСКОЙ ЧАСТИ ЕДИНОГО ГОСУДАРСТВЕННОГО РЕЕСТРА ВОЕННООБЯЗАННЫХ

*Александр Николаевич Правдивец<sup>1</sup>  
Виктор Васильевич Козлов<sup>2</sup>*

*<sup>1</sup>Генеральный штаб Вооружённых Сил Украины, Киев, Украина*

*<sup>2</sup>Центральный научно-исследовательский институт ВС Украины, Киев, Украина*

*В статье предложена методика определения количества комплектов клиентской части Единого государственного реестра военнообязанных.*

*Методика отражает логическую последовательность действий, которая состоит из трех этапов: формирование исходных данных, определение основных показателей и определения количества комплектов клиентской части Единого государственного реестра военнообязанных, при этом исходные данные методики по назначению разделены на шесть групп.*

*Предложенная методика охватывает все направления работ, выполняемых подразделениями военных комиссариатов, что позволяет:*

*определить количество комплектов клиентской части Единого государственного реестра военнообязанных для выполнения операций по ведению воинского учета призывников и военнообязанных в военных комиссариатах;*

рассчитать необходимую численность операторов Единого государственного реестра военнообязанных с учетом задач, которые возлагаются на структурные подразделения военных комиссариатов, в пределах определенного лимита численности военнослужащих и работников и провести перераспределение обязанностей между существующими должностными лицами военных комиссариатов.

Полученные результаты исследования могут быть использованы при проведении расчетов количества комплектов клиентской части Единого государственного реестра военнообязанных для совершенствования организационно-штатной структуры военных комиссариатов и разработка руководящих документов по вопросам определения соответствующих норм их обеспечения и снабжения соответствующими образцами вооружения и военной техники.

**Ключевые слова:** методика; клиентская часть; Единый государственный реестр военнообязанных.

## METHOD OF DETERMINATION OF THE NUMBER OF CLIENTS'S PART KITS OF THE UNIFIED STATE RESERVERS REGISTER

Oleksandr Pravdyvets<sup>1</sup>  
Viktor Kozlov<sup>2</sup>

<sup>1</sup>General Headquarters of the Armed Forces of Ukraine, Kyiv, Ukraine  
<sup>2</sup>Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

The article proposes a method for determining the number of sets of the client part of the Unified State Register of Conscripts.

The methodology reflects a logical sequence of actions, which consists of three stages: formation of initial data, determination of basic indicators and determination of the number of sets of the client part of the Unified State Register of Conscripts, with the initial data of the methodology divided into six groups.

The proposed methodology covers all areas of work performed by units of military commissariats, which allows:

determine the number of sets of the client part of the Unified State Register of Conscripts for military registration of conscripts and conscripts in military commissariats;

calculate the required number of operators of the Unified State Register of Conscripts, taking into account the tasks assigned to the structural units of military commissariats, within a certain limit of the number of servicemen and employees and redistribute responsibilities between existing officials of military commissariats.

The results of the study can be used to calculate the number of sets of the client part of the Unified State Register of Conscripts to improve the organizational and staffing structure of military commissariats and develop guidelines for determining appropriate standards for their provision and supply of appropriate weapons and military equipment.

**Key words:** methodology; client unit; Unified State Reserves Register.

### References

1. Nakaz Ministerstva obrony Ukrainy vid 15.04.2019 №180 "Pro pryjnjattja na postachannja ta vvedennja v ekspluataciju Zbrojnykh Syl Ukrainy avtomatyzovanoji systemy Jedynogho derzhavnogho rejestrju vijsjkovozobov'jazanykh, shyfr "Oberigh".
2. Zakon Ukrainy "Pro Jedynyj derzhavnyj rejestr vijsjkovozobov'jazanykh".
3. Postanova Kabinetu Ministriv Ukrainy vid 07.12.2016 №921 "Pro zatverdzhennja Porjadku orghanizaciji ta vedennja vijsjkovogho obliku pryzovnykiv i vijsjkovozobov'jazanykh".
4. Nakaz Ministerstva obrony Ukrainy vid 08.08.2017 №418 "Pro zatverdzhennja Porjadku vedennja Jedynogho derzhavnogho rejestrju vijsjkovozobov'jazanykh".
5. Pravdyvecj O.M., Analiz chynnykiv, jaki vplyvajutj na funkcionuvannja systemy vijsjkovogho obliku ghromadjan Ukrainy, Zbirnyk naukovykh pracj Nacionalnoji akademiji prykordonnoji sluzhby Ukrainy 2016, №1(67), S.223-229.
6. Pravdyvecj O.M., "Normatyvno-pravove zabezpechennja stvorennja ta funkcionuvannja informacijnoji avtomatyzovanoji systemy vijsjkovogho obliku ghromadjan Ukrainy", Zbirnyk naukovykh pracj Centru vojenno-strategichnykh doslidzhenj NUOU, 2015, №3 (55), S. 130-132.
7. Pravdyvecj O.M., Chelobitchenko O.O., Babenko S.V. "Modelj systemy vijsjkovogho obliku ghromadjan". Trudy universytetu, NUOU, 2017, № 6 (145), s. 114-120.
8. Pravdyvecj O.M., Chelobitchenko O.O., Jakymenko S.V., Khardelj R.Z. "Metodyka pidghotovky operatoriv jedynogho derzhavnogho rejestrju vijsjkovozobov'jazanykh rajonnykh (misjkykh) vijsjkovykh komisariativ", Trudy universytetu, 2018, №3 (148), S. 142-150.
9. Nakaz komanduvacha Sukhoputnykh vijsjk Zbrojnykh Syl Ukrainy vid 12.04.2019 №188 "Pro zatverdzhennja dopovnenj do Zbirnyka normatyviv bojovoji pidghotovky Sukhoputnykh vijsjk Zbrojnykh Syl Ukrainy 2002 roku"

Лариса Миколаївна Дегтярєва (кандидат технічних наук, доцент) <sup>1</sup>

Сергій Володимирович Волошко (кандидат технічних наук, с.н.с.) <sup>2</sup>

Володимир Вікторович Лоза <sup>2</sup>

Анна Олександрівна Буланкіна <sup>3</sup>

<sup>1</sup>Полтавська державна аграрна академія, Полтава, Україна

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

<sup>3</sup>Луганський центр професійно-технічної освіти Державної служби зайнятості, Україна

## ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ОБРОБКИ ДАНИХ В СУЧАСНИХ СИСТЕМАХ ТРАНСПОРТНОЇ ЛОГІСТИКИ

В статті виконаний аналіз застосування інформаційних технологій та сучасних методів обробки даних для підвищення ефективності роботи персоналу системи транспортної логістики. Обґрунтовано актуальність та необхідність створення логістичної інформаційної системи в рамках побудови системи оперативного (бойового) управління, зв'язку, розвідки та спостереження (C4ISR) у Збройних Силах України. Визначено напрямки впровадження інформаційних технологій, використання комунікаційного забезпечення та інтеграції інформаційних потоків на транспорті. Сформовано основні важливі проблеми та завдання в транспортній логістиці. На основі проведених досліджень визначені основні технологічні процеси обробки даних з використанням інформаційних технологій. Сформульовано вимоги інформаційної безпеки, необхідні для забезпечення коректної роботи інформаційних систем транспортної логістики. За результатами аналізу інформаційних процесів обробки даних з використанням сучасних інфотелекомунікаційних технологій зроблено висновки про переваги їх впровадження та застосування. Визначено напрямки подальших досліджень для побудови логістичної інформаційної системи Збройних Сил України.

**Ключові слова:** логістична система, інформаційні технології, комунікаційне забезпечення, телекомунікаційні канали, обробка даних.

### Вступ

**Постановка проблеми.** Створення ефективної системи оперативного (бойового) управління, зв'язку, розвідки та спостереження (C4ISR) у Збройних Силах України, відповідно до Стратегічного оборонного бюлетеню [1], висуває сучасні вимоги до використання сучасних інформаційних технологій та цифрових методів обробки даних у різних складових сил оборони.

Складовою загальної системи C4ISR є інформаційна система управління логістичною системою на транспорті. Для підвищення ефективності роботи такої системи необхідно активно застосовувати інформаційні технології та сучасні методи обробки даних, що потенційно можуть підвищити якість та динамічність транспортного обслуговування, недовантаження рухомого складу, вирішити складності організації взаємодії декількох видів транспорту, сповільнити зношення транспорту завдяки інформаційній підтримці та переходу на цифрові технології у всіх напрямках документообігу, у тому числі заміні паперових перевізних документів електронними для аналізу планування та підтримки прийняття управлінських рішень.

Для забезпечення паритету Збройних Сил України та можливості подальшої інтеграції інших

інформаційних систем доцільно впроваджувати такі інформаційні системи в підприємствах усіх форм власності.

**Аналіз останніх досліджень і публікацій.** Сучасні інформаційні технології, побудовані на основі використання ідей інформаційних сховищ з можливістю інтелектуальної обробки даних, сприяють створенню інформаційної інфраструктури, що дозволяє організовувати, збирати та обробляти інформацію усім об'єктам та суб'єктам логістичного ланцюга. Дослідженню впливу інфотелекомунікаційних технологій на розвиток систем транспортної логістики присвячено цілий ряд робіт, а саме: Алесинська Т.В., Беспалов Р.С., Губин С.В., Боярчук А.В., Сергєєв В.І. та ін. [2-10].

Результати досліджень в області використання інформаційних технологій на транспорті показали, що програмні продукти для їх реалізації постійно удосконалюються, збільшується кількість і якість інформаційних систем, враховуючи апаратні та мережеві складові. При цьому у зазначених роботах приділяється недостатня увага щодо методів аналізу, структурування даних та формування вихідних баз даних для подальшого

використання у інформаційних та автоматизованих системах.

**Мета статті.** Аналіз і структурування даних в транспортній логістиці з використанням інформаційних технологій обробки даних для збільшення швидкості їх обробки і отримання дієвих та коректних управлінських рішень органами військового управління.

### Виклад основного матеріалу дослідження

Сучасне спрямування сталих методів управління підрозділами, військовими частинами та підприємствами, які ґрунтувались на паперовому діловодстві, – до цифрових методів створення, передачі, обробки та зберігання інформації, призводить до широкого впровадження мобільних (інтерактивних) баз даних, організації зв'язку для доступу до інформації через телекомунікаційні канали з використанням наземних мереж та супутникових можливостей. Відповідно і у логістичних системах спостерігається перехід на цифрові технології у всіх напрямках документообігу, у тому числі заміні паперових перевізних документів електронними. Під транспортною логістикою розуміють функціональну сферу логістики, що оптимізує логістичні операції на шляху матеріального потоку від постачальника до кінцевого споживача, що здійснюється із застосуванням транспортних засобів [3].

У Збройних Силах України також створено структуру «J-4» (Головне управління логістики), зараз триває етап набуття нею спроможностей. У процесі відбувається розмежування стратегічних і оперативних функцій логістичного забезпечення органів військового управління, а також прийняття системи класів постачання НАТО. Тобто, відбувається злиття напрямів тилового забезпечення і забезпечення озброєнням в одну цілку структуру.

Впровадження інформаційних технологій, використання комунікаційного забезпечення та інтеграція інформаційних потоків реалізуються на транспорті за декількома напрямками:

активне впровадження та використання автоматизованих систем керування транспортним підприємством;

високий рівень інформативності та аналіз отриманої інформації для формування управлінського рішення;

комплексне використання технічних, математичних, інформаційних та організаційних засобів.

Кожний підрозділ або військова частина (підприємство), в тому числі і транспортне, повинне зберігати дані про свою діяльність, які можна використовувати в якості архівної інформації, а також даних, що забезпечують безпосередньо його діяльність і ефективну роботу особового складу (персоналу) та техніки в реальному режимі часу. Тому будь-яка організація

(підприємство) на сьогоднішній день прагне використовувати інформаційну систему опрацювання даних [4].

Інформаційна технологія обробки даних передбачає наявність завдань, що містять початкові дані, які мають певну структурну організацію, і метод їх розв'язання. Використання інформаційної технології обробки даних дає можливість допускати різні рівні кваліфікації персоналу, глибоко аналізувати зміст отриманої інформації, робити вибірки, звіти, статистичні та математичні розрахунки, забезпечувати введення і обробку даних з мінімізацією помилок при виконанні постійно повторюваних операцій. До переліку завдань, які потрібно вирішувати при використанні інформаційних технологій, можна віднести введення і обробку даних про клієнтів, техніку, вантажі, оптимізація маршрутів перевезення, формування різноманітних запитів, які можуть відобразити інтерактивні звіти з можливістю їх оформлення та роздрукування документів, які можуть бути оформлені згідно вимог сучасних нормативів як всередині країни, так і (при необхідності) за її межами.

Для доступу особового складу (персоналу) до інформаційної системи, яка відповідає за узгодження дій окремих модулів системи, створюється локальна розгалужена комп'ютерна мережа, по якій кожний фахівець може отримувати необхідну йому інформацію і використовувати її для своїх професійних потреб.

Операція обробки даних передбачає будь-яку дію, яка призводить до зміни початкових даних, виконання розрахунків, що призводить до появи нових даних, виконання сортування, яке дозволяє упорядкувати записи та згрупувати їх по певним параметрам; укрупнення або агрегування, що служить для зменшення кількості даних і реалізоване в формі розрахунків підсумкових або середніх значень.

Одна з важливіших проблем та завдань в транспортній логістиці це моніторинг транспортних засобів та оптимізація маршруту пересування, а саме: контроль за місцезнаходженням і станом транспортних засобів, вантажів або водіїв з використанням комп'ютерних систем, які встановлено на пересувний засіб, використання інтерфейсів для можливості роботи в локальних мережах.

Можливо вбудовування модуля для використання глобальної системи визначення місцезнаходження транспортних засобів на основі супутникового зв'язку GPS. Інформація, використовуючи телекомунікаційні канали, потрапляє до організаторів перевезень та/або до інших ланок логістичного ланцюга. Саме моніторинг на базі інформаційних технологій дозволяє значно поліпшити якість роботи транспортного каналу, підвищити безпеку перевезень та контролювати безпеку руху та стан водіїв: людина, яка контролює маршрут, у будь-який проміжок часу може відзначити

місцезнаходження транспорту (при цьому можна використовувати інтерактивну фіксацію транспортного засобу на карті з планом маршруту), його швидкість, стан вантажу тощо.

Аналізуючи особливості функціонування систем навігації (супутникового зв'язку GPS) [5] можна зазначити, що вони спираються на наступні принципи визначення координат: використання принципу беззапитних віддалених вимірювань між навігаційними супутниками і споживачем, коли споживачеві передається інформація про координати супутників і одночасно проводиться вимірювання відстані до навігаційних супутників. Спосіб вимірювань відстані спирається на порівняння розрахункових даних, які стосуються тимчасових затримок сигналу від супутника з сигналом, сформованим апаратурою споживача. При цьому сам супутниковий сигнал містить оперативну (оцифровку міток часу, зсув шкали часу супутника відносно шкали системи, відносну відміну несучої частоти супутника від номінального значення та ін.) та неоперативну (дані про стан всіх супутників системи, параметри орбіт всіх супутників системи, поправку до шкали часу супутникової системи та ін., тобто данні альманаху) інформацію [6].

У цьому випадку можна створити внутрішню систему визначення місцезнаходження транспортних засобів IPS (Indoor Positioning System) з використанням транспондерів в якості носіїв інформації при радіочастотній технології

ідентифікації.

При виникненні форс-мажорних обставин (аварія, несправність, погане почуття водія, аварійний стан шляху та ін.), інформація щодо стану ситуації дозволяє прийняти оптимальне управлінське рішення.

В Збройних Силах України на різних рівнях управління потрібні свої типи інформаційних систем. Сучасні системи керування базами даних забезпечують як фізичну (незалежність від способу зберігання і методу доступу), так і логічну незалежність даних (можливість зміни однієї програми без зміни інших додатків, що працюють з цими ж даними).

Один з основних принципів створення інформаційної системи полягає в тому, щоб збирати дані на найнижчому рівні агрегування і коректно представляти їх у якісному вигляді для порівняння та аналізу, тому для використання ефективної логістичної системи необхідний комплексний набір даних, за допомогою якого можна проводити аналіз, а система повинна мати у своєму розпорядженні можливості для проведення детального аналізу з подальшою можливістю прийняття управлінських рішень.

З урахуванням вищезазначеного, авторами пропонується використання наступних основних технологічних процесів обробки даних з використанням інформаційних технологій (представлено на рис. 1).

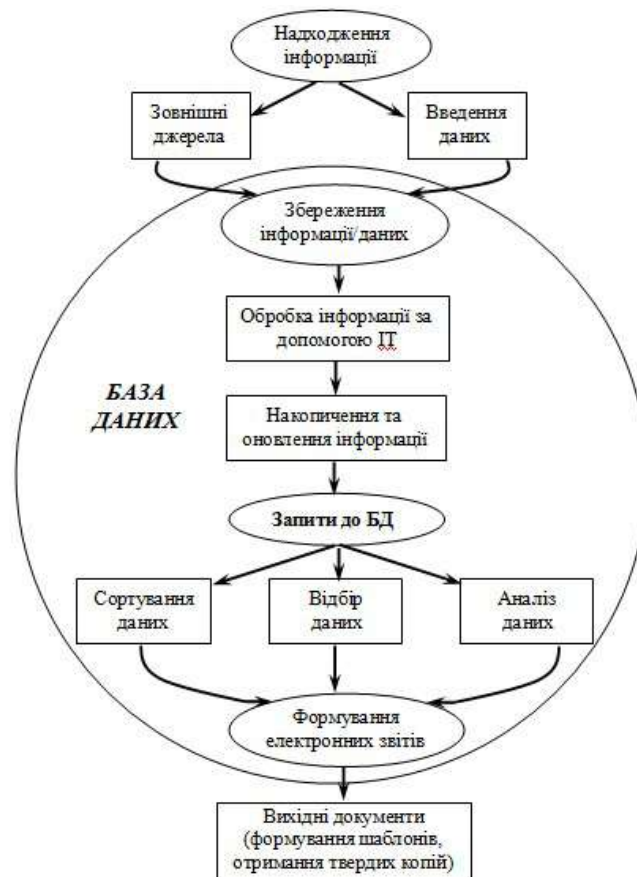


Рис. 1. Основні технологічні процеси обробки даних з використанням інформаційних технологій

Для відображення кінцевого результату обробки доцільно реалізувати процедуру створення звітів (документів). В інформаційній технології обробки даних ці документи створюються для внутрішнього вжитку – для керівництва і підлеглого особового складу, а також для взаємодіючих і приданих підрозділів.

Документи можуть створюватися за двома формами: за запитом або за шаблоном, який сформовано як періодичний звіт, який повинен бути сформовано наприкінці звітного періоду: кожного місяця, кварталу або року, сформований маршрутний лист, або надання обґрунтованих варіантів можливих управлінських рішень.

Але далеко не всі зміни інформаційного потоку даних, які «курсують» в інформаційній системі, потрібно надсилати до безпосереднього керівництва, інакше інформаційний канал

виявиться перевантаженим. Основні взаємодії виконуються на рівні виконавців, які, як правило, функціонують в автономному режимі. Відповідна комп'ютерна техніка, програмні продукти, що створені з метою здійснити обробку даних в сфері транспортної логістики, та електронні комунікації повинні замінити традиційний інформаційний обмін, спираючись на гнучкий зворотний зв'язок.

В системах транспортної логістики Збройних Силах України, які в якості інструментарію використовують засоби інформаційних систем та технологій, особлива увага приділяється заходам безпеки, які можуть забезпечити збереження даних або мінімізувати втрати від можливих сторонніх втручань.

Для забезпечення стабільної роботи інформаційної логістичної системи пропонується дотримання вимог, які перераховані в табл. 1

Таблиця 1

**Вимоги інформаційної безпеки до властивостей систем транспортної логістики**

Властивість	Опис
Ідентифікація та авторизація користувачів	Адміністрування систем транспортної логістики (з точки зору інформаційної безпеки), можливість використовувати механізм забезпечення рівнів доступу.
Цілісність системи	Необхідність використання програмних та/чи апаратних засобів, які дозволяють з вказаною (завчасно зазначеною) періодичністю перевіряти коректність роботи системи в цілому і її окремих компонентів, зокрема.
Внутрішній системний контроль	Інформаційна система транспортної логістики повинна самостійно (без зовнішнього втручання) підтримувати власну працездатність та роботу окремих системних модулів, на предмет їх злагодженої роботи. Визначається інтерфейс користувача, який гарантує зрозумілість, зручність, структурованість та ергономічність.
Опис підходів організації/ підприємства до безпеки систем транспортної логістики	Опис загальної архітектури та взаємодії між окремими модулями системи; архівація даних (періодичність та час зберігання архівованих даних). Забезпечення надійності системи від зовнішнього проникнення з дотриманням чіткого розподілу функцій адміністратора та користувачів/операторів ПК.
Аудит системи	Обов'язкова реєстрація подій: ідентифікації та аутентифікації користувачів, час роботи програми (її запуск та припинення роботи); опис моделі політики безпеки; можливість видалення об'єктів; фіксація дати та часу подій, які пов'язані з виконанням повного (затребуваного) апаратного та програмного функціоналу системи; опис функціональних можливостей користувачів в залежності від рівнів доступу та рівнів секретності, а також обмежень, які залежать від цієї рівня доступу.

Слід зазначити, що розглядаючи вимоги до захисту та збереження інформації в системах транспортної логістики в даному випадку не розглядалась можливість захисту системи від вірусів, негативних впливів програмних закладок, використання криптографічних засобів захисту даних, але всі ці компоненти можуть бути використані для забезпечення високої працездатності та захищеності системи для обробки, збереження та передавання конфіденційної інформації.

**Висновки й перспективи подальших досліджень**

Виконаний аналіз інформаційних процесів обробки даних з використанням сучасних інфотелекомунікаційних технологій дозволяє зробити висновок, що їх застосування дозволяє одержати істотну економію інших ресурсів: енергетичних, матеріальних, трудових, а також дає можливість оптимізувати процеси управління, здійснюючи організацію, контроль, регулювання та аналіз для прийняття та впровадження управлінського рішення.

Авторами пропонується визначений перелік основних технологічних процесів обробки даних з використанням інформаційних технологій, який доцільно використання при побудові не тільки

логістичних інформаційних систем військового призначення, але й в інформаційних (автоматизованих) системах цивільного призначення для забезпечення можливості їх інтеграції в єдину логістичну систему сил оборони держави.

Подальші дослідження будуть направлені на розробку методичного апарату системи підтримки

прийняття рішення органами військового управління, визначення економічно обґрунтованого переліку датчиків та параметрів для забезпечення роботи системи, а також формування рекомендацій щодо практичної реалізації такої системи з використанням програмно-апаратних комплексів.

### Література

1. Рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України". Введено в дію Указом Президента України від 6 червня 2016 року № 240/2016.  
2. Тридід О.М., Азаренкова Г.М., Мішина С.В., Борисенко І.І. Логістика. Навч. посіб. – К.: Знання, 2008. – 566 с.  
3. Безштанько В. Аналіз існуючих програмних засобів та методик оцінки стану інформаційної безпеки організації // *Бизнес и безопасность*. – 2007. – № 1. – С. 32-35.  
4. Корнієцький О.В. Розвиток логістики підприємства на основі інноваційного підходу/ О.В. Корнієцький // *Науковий вісник Херсонського державного університету* – Серія: Економічні науки. – 2014. Вип. 9, Ч. 4. – С. 109-111.  
5. Jean-Marie Zogg, Краткое руководство Основы спутниковой навигации. Теории и принципы. Системы и обзор приложений // GPS-X-02007-C, Швейцария, 2007. – С. 18-47.  
6. Харисов В.Н., Перов А.И., Болдин В.А. (ред.). Глобальная спутниковая радионавигационная система ГЛОНАСС. - М.: ИПРЖР, 1998. — 400 с.

7. Беспалов Р.С. Транспортная логистика. Новейшие технологии построения эффективной системы доставки. / Р.С. Беспалов // – М.: Вершина, 2007. – 384 с.  
8. Алесинская Т.В. Основы логистики. Функциональные области логистического управления. Ч. 3. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – 116 с.  
9. Губин С.В., Боярчук А.В. Информационные технологии в логистике – Киев: «Миллениум», 2009. – 60 с.  
10. Сергеев В.И., Григорьев М.Н., Уваров С.А. Логистика: информационные системы и технологии: Учебно-практическое пособие. – М.: Издательство «Альфа-Пресс», 2008. – 608 с.  
11. Дегтярева Л.М., Мірошникова М.В., Волошко С.В. Аналіз структури системи захисту інформації. // *Системи управління, навігації та зв'язку*. – Полтава: ПолтНТУ, 2019 – № 2 (54). – С. 78-83.  
12. Емельянова Н.З., Партыка Т.Л., Попов И.И. Основы построения автоматизированных информационных систем – М.: ФОРУМ: ИНФРА-М, 2007. – 416 с.

### ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ОБРАБОТКИ ДАННЫХ В СОВРЕМЕННЫХ СИСТЕМАХ ТРАНСПОРТНОЙ ЛОГИСТИКИ

*Лариса Николаевна Дегтярева (кандидат технических наук, доцент)<sup>1</sup>*

*Сергей Владимирович Волошко (кандидат технических наук, с.н.с.)<sup>2</sup>*

*Владимир Викторович Лоза<sup>2</sup>*

*Анна Александровна Буланкина<sup>3</sup>*

<sup>1</sup>*Полтавська державна аграрна академія, Полтава, Україна*

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

<sup>3</sup>*Луганський центр професійно-технічного освіти Державної служби зайнятості, Сєвєродонецьк, Україна*

*В статті виконано аналіз застосування інформаційних технологій і сучасних методів обробки даних для підвищення ефективності роботи персоналу системи транспортної логістики. Обґрунтовано актуальність і необхідність створення логістичної інформаційної системи в рамках побудови системи оперативного (бойового) управління, зв'язку, розвідки і спостереження (C4ISR) в Збройних Силах України. Визначено напрямки впровадження інформаційних технологій, використання комунікаційного забезпечення і інтеграції інформаційних потоків на транспорті. Сформульовано основні важливі проблеми і завдання в транспортній логістиці. На основі проведених досліджень визначено основні технологічні процеси обробки даних з використанням інформаційних технологій. Сформульовано вимоги інформаційної безпеки, необхідні для забезпечення коректної роботи інформаційних систем транспортної логістики. По результатам аналізу інформаційних процесів обробки даних з використанням сучасних інформатико-комунікаційних технологій, зроблено висновки про переваги їх впровадження і застосування. Визначено напрямки подальших досліджень для побудови логістичної інформаційної системи Збройних Сил України.*

**Ключові слова:** логістична система, інформаційні технології, комунікаційне забезпечення, телекомунікаційні канали, обробка даних.

### THE USE OF INFORMATION TECHNOLOGY FOR DATA PROCESSING IN MODERN TRANSPORT LOGISTICS SYSTEMS

*Larysa Degtyaryova (Candidate of Technical Sciences, Associate Professor)<sup>1</sup>*

*Sergiy Voloshko (Candidate of Technical Sciences, Senior Researcher)<sup>2</sup>*

*Volodymyr Loza<sup>2</sup>*

*Anna Bulankina<sup>3</sup>*

<sup>1</sup>*Poltava State Agrarian Academy, Poltava, Ukraine*

<sup>2</sup>*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

<sup>3</sup>*Lugansk center of the professional technical education of the State employment service, Severodonetsk, Ukraine*

*The article analyzes the use of information technology and modern data processing methods to increase the efficiency of the personnel of the transport logistics system. The relevance and necessity of creating a logistic information system within the framework of building an operation (combat) command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) system in the Armed Forces of Ukraine is substantiated. Defined areas for the implementation of information technology, the use of communication support and the integration of information flows in transport. The main important problems and tasks in transport logistics are formed. Based on the studies, the main technological processes of data processing using information technology are determined. The information security requirements are formulated that are necessary to ensure the correct operation of transport logistics information systems. According to the results of the analysis of data processing information processes using modern information and telecommunication technologies, conclusions are drawn about the advantages of their implementation and application. The directions of further research for the construction of a logistics information system of the Armed Forces of Ukraine are identified.*

**Keywords:** *logistics system, information technology, communications support, telecommunications channels, data processing.*

### **References**

- 1. The decision** of the Council of national security and defense of Ukraine from 20 may 2016 "Strategic defense Bulletin of Ukraine". Promulgated by the decree of the President of Ukraine of 6 June 2016 № 240/2016.
- 2. Trydid O.M.,** Azarenkova G.M., Mishyna S.V., Borysenko I.I. Logistics. Textbook. – Kyiv: Knowledge, 2008. – 566 p.
- 3. Bezshanko V.** Analysis of existing software tools and methods to assess the state of information security organizations // Business and security. – 2007. – № 1. – P. 32-35.
- 4. Kornietskiy O.** The development of logistics enterprises through an innovative approach // Scientific Bulletin of Kherson state University – Series: Economic science. – 2014. Issue 9, Part 4. – P. 109-111.
- 5. Jean-Marie Zogg,** Korotkyy posibnyk Osnovy suputnykovoyi navihatsiyi. Teoriyi i pryntsyipy. Systemy i ohlyad prohram // GPS-X-02007-C, Shveysariya, 2007. - S. 18-47.
- 6. Kharysov V.N.,** Perov A.I., Boldin V.A. (Red.). Hlobal'na suputnykova radionavihatsiyana systema HLONASS. - M.: IPRZHR, 1998. - 400 s.
- 7. Bespalov R.** Transport logistics. The newest technologies for building an efficient delivery system / R. Bespalov // – Moscow: Verzhina, 2007. – 384 p.
- 8. Алесинская Т.В.** Fundamentals of logistics. Functional area of logistics management. Part 3. – Taganrog: Publishing House of the TTI SFU, 2010. – 116 p.
- 9. Gubin S.V.,** Bojarchuk A.V. Information technology in logistics – Kyiv: "Millennium", 2009. – 60 p.
- 10. Sergeev V.I.,** Grigoryev M.N., Uvarov S.A. Logistics: information systems and technology: Training manual. – Moscow: Publishing House "Alpha-Press", 2008. – 608 p.
- 11. Degtyaryova L.M.,** Miroshnykova M.V., Voloshko S.V. Analysis of the structure of information security system // Control systems, navigation and communication. – Poltava: PoltNTU, 2019 – № 2 (54). – P. 78-83.
- 12. Jemeljanova N.Z.,** Partyka T.L., Popov I.I. Fundamentals of automated information systems – Moscow: FORUM: INFRA-M, 2007. – 416 p.



*Микола Миколайович Биченок (доктор технічних наук, с.н.с.)*

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

## ОЦІНЮВАННЯ РИЗИКІВ ЖИТТЄДІЯЛЬНОСТІ ЛЮДИНИ І НАСЕЛЕННЯ У ПРИРОДНО-ТЕХНОГЕННОМУ СЕРЕДОВИЩІ В УМОВАХ ОСОБЛИВОГО ПЕРІОДУ

*Зростання антропогенного впливу на навколишнє середовище разом з інтенсивним використанням природних ресурсів зумовлюють стійку тенденцію до збільшення негативних наслідків для життєдіяльності населення від надзвичайних ситуацій природного та техногенного походження на території України. Крім того, в умовах економічної скрути, а також гібридної війни на сході України з боку РФ зменшуються витрати на впровадження новітніх технологій, модернізацію виробничих процесів і ремонтно-профілактичні заходи, зростає кількість зношеного обладнання, знижується рівень технологічної дисципліни.*

*У даній роботі на основі узагальнення досвіду оцінювання та прогнозування ризиків виникнення надзвичайних ситуацій у різних регіонах України, в першу чергу на територіях підвищеної природної і техногенної небезпеки, розробляються методологічні основи оцінки ризиків життєдіяльності в цих умовах.*

**Ключові слова:** *надзвичайні ситуації, ризики життєдіяльності, техногенні і природні загрози.*

### Вступ

Обмежений обсяг ресурсів для проведення захисних заходів визначає необхідність їхнього використання для нейтралізації загроз на найбільш пріоритетних напрямках. Серед найактуальніших природних загроз в умовах України проявляються небезпечні екзогенні геологічні процеси (НЕГП), насамперед підтоплення, зсуви, карст, просідання лесових ґрунтів [1,2].

Що стосується техногенних загроз, то найактуальнішими для умов України можна вважати аварії на хімічно небезпечних об'єктах (ХНО) [3,4].

Хімічні, нафтохімічні і нафтопереробні виробництва в Україні характеризуються зношенням основних фондів, а також погіршенням інженерно-геологічних умов промислових майданчиків внаслідок природної і техногенної активізації НЕГП. Упродовж останніх десятиріч відбувається активний процес зниження міцності верхньої зони порід внаслідок порушення режиму їхнього водо- та теплообміну, геохімічних параметрів ландшафтів та гідрогеохімічного режиму зони активного водообміну.

Значна частина потенційно небезпечних об'єктів в Україні, в тому числі ХНО, розташована в зонах імовірної активізації природних і техногенних НЕГП. Площинний характер розвитку більшості НЕГП суттєво збільшує ризики

виникнення аварій на ХНО за рахунок деформацій і руйнувань відповідальних конструктивних елементів.

**Постановка проблеми.** В умовах особливого періоду, враховуючи військові дії на сході нашої країни, актуальною проблемою є оцінювання ризиків життєдіяльності людини і населення від впливу природних і техногенних загроз. Ці загрози потребують оперативного оцінювання і адекватного реагування, оскільки їх наслідки усугубляються під дією військових факторів.

**Аналіз останніх досліджень і публікацій.** Розробкою методів оцінювання природних і техногенних ризиків життєдіяльності займалось багато вчених, зокрема, Б.М. Данілишин [1] і С.О. Яковлев [2] розробляли методи оцінювання природних ризиків. Техногенні ризики досліджувались С.П. Іванютою [3], А.Б. Качинським [6] та ін.

Але у розглянутих авторів питання, які пов'язані з обґрунтуванням комплексного оцінювання ризиків життєдіяльності у природно-техногенному середовищі не розглядалися.

**Метою статті** є розробка моделей і методів комплексного оцінювання ризиків життєдіяльності в умовах негативних природних і техногенних загроз.

## Виклад основного матеріалу дослідження

Регіональна природно-техногенна активізація НЕГП на сучасному етапі функціонування численних просторово розосереджених техногенно-геологічних систем "техногенний об'єкт – геологічне середовище" зумовлює двоєдину структуру формування ризиків життєдіяльності в зонах впливу потенційно небезпечних об'єктів, у першу чергу хімічно небезпечних:

погіршення інженерно-геологічної стійкості середовища внаслідок природно-техногенної активізації НЕГП;

локальний вплив потенційно небезпечних об'єктів на зміни інженерно-геологічних показників порід підгрунтя (міцність, агресивність до будівельних конструкцій та ін.).

В цілому спостерігається суттєве відхилення інженерних параметрів промислових майданчиків від початкових проектних, що зумовлює додаткові деформації технологічно важливих споруд, водота теплопостачальних систем, порід підгрунтя, фундаментів та ін. [ 2 ]

На підприємствах хімічного комплексу понад 900 будівель і споруд на контрольованому періоді не мали капітальних ремонтів, близько 125 будівель і споруд не відповідають вимогам будівельних норм і правил, понад 40 – знаходяться в аварійному стані. Все це суттєво підвищує негативний вплив НЕГП і збільшує ризик аварійних ситуацій.

Внесок природних факторів у формування ризику можна враховувати за експертною оцінкою шляхом введення відповідних підвищуючих коефіцієнтів, оскільки вплив цих процесів на зростання ризику аварії відбувається за кумулятивною моделлю взаємодії. Значення підвищуючого коефіцієнта за рахунок негативних змін інженерно-геологічних умов для різних типів прояву цих процесів обґрунтовано на основі експертної оцінки: при просіданні  $K^p = 2$ ; при підтопленні  $K^f = 5$ ; при комплексній дії підтоплення і просідання  $K^k = 5 * 2 = 10$ .

Ймовірність прояву НЕГП у природному режимі їхнього розвитку  $P_1(H_1)$  залежить від двох основних чинників, що впливають на її формування: просторової ураженості території об'єктами НЕГП  $K_s$  та часової динаміки розвитку об'єктів НЕГП  $K_d$  як частоти їхньої активізації за певний проміжок часу (випадків/рік). Таким чином, річна ймовірність природного прояву НЕГП на території оцінки визначатиметься

$$P_1(H_1) = K_s * K_d,$$

де  $K_s$  – просторова ураженість території НЕГП;

$K_d$  – часова динаміка розвитку НЕГП.

З урахуванням зазначеного природний ризик життєдіяльності на території можливого прояву НЕГП оцінюється за співвідношенням

$$R_1(H_1) = P_1(H_1) * V_1(H_1) * K_1(H_1) * N,$$

де  $R_1(H_1)$  – колективний ризик життєдіяльності (втрати здоров'я чи загибелі населення) на даній території в результаті активізації екзогенних геологічних процесів (чол/рік);

$P_1(H_1)$  – ймовірність прояву НЕГП на досліджуваній території (випадків/рік);

$V_1(H_1)$  – уразливість території від прояву НЕГП, що визначається відношенням ураженої частини території до її загальної площі (частки одиниці);

$K_1(H_1)$  – просторова уразливість населення (частки одиниці);

$N$  – чисельність населення на території дослідження (чол.).

Під аварією з викидом небезпечних хімічних речовин розуміється надзвичайна ситуація техногенного характеру, що сталася на ХНО внаслідок виробничих, конструктивних, технологічних чи експлуатаційних причин або від зовнішніх впливів і призвела до пошкодження технологічного обладнання, пристроїв, споруд, транспортних засобів з формуванням зони хімічного зараження, яка становить реальну загрозу для здоров'я і життєдіяльності людей [ 4 ]. Ризик життєдіяльності в цій зоні визначається як вірогідність загибелі чи захворювання людей внаслідок отруєння.

Оцінювання ризиків життєдіяльності від можливих аварій на ХНО базується на результатах прогнозування наслідків аварійного викиду небезпечних хімічних речовин, що здійснюється з урахуванням: обсягів викиду та метеорологічних умов для визначення параметрів зони хімічного зараження і відпрацювання необхідних дій у цій зоні.

Прогнозування наслідків аварійного викиду передбачає відповідно до [ 7 ] визначення таких параметрів можливої зони хімічного зараження:

кут сектора зони з урахуванням стійкості напрямку вітрового потоку та швидкості вітру;

глибина зони  $R$ , км;

розрахункова (можлива) площа зони  $S$ , км<sup>2</sup>;

кількість населення в зоні (визначається за кількістю мешканців населених пунктів, що потрапляють у цю зону)  $N_2$ , чол.;

площа максимально можливого поширення токсичної хмари  $S_{max} = \pi * R^2$ , км<sup>2</sup>;

Ймовірність виникнення аварії  $P_2(H_2)$  на ХНО з викидом токсичних речовин визначається як середньорічна частота хімічно небезпечних аварій, від яких можуть постраждати (захворіти або загинути) люди внаслідок ураження

$$P_2(H_2) = N_a / N_h$$

де  $N_a$  – кількість аварій на ХНО з викидом небезпечних хімічних речовин, внаслідок яких можуть постраждати люди;

$N_h$  – загальна кількість ХНО на території дослідження.

З урахуванням цього максимально можливий колективний техногенний ризик життєдіяльності  $R_2 (H_2)$  в умовах можливої аварії на заданому ХНО в межах прогнозованої площі зони визначається за формулою

$$R_2 (H_2) = P_2 (H_2) * V_2 (H_2) * K_2 (H_2) * N,$$

де  $R_2 (H_2)$  – колективний ризик втрати здоров'я чи загибелі населення на даній території при можливій аварії на ХНО з викидом небезпечних хімічних речовин (чол/рік);

$P_2 (H_2)$  – ймовірність виникнення аварії на ХНО (випадків/рік);

$V_2 (H_2)$  – уразливість території від можливої аварії на ХНО (частки одиниці);

$K_2 (H_2)$  – просторова уразливість населення (частки одиниці);

$N$  – чисельність населення на території дослідження (чол.).

Уразливість території від можливої аварії на ХНО  $V_2 (H_2)$  визначається відношенням площі ураженої частини території до її загальної площі

$$V_2 (H_2) = S_2 / S,$$

де  $S_2$  – площа зони, що формується в результаті аварії з викидом небезпечних хімічних речовин (км<sup>2</sup>);

$S$  – площа території дослідження: області, району, промислового майданчика тощо (км<sup>2</sup>).

Просторова уразливість населення  $K_2 (H_2)$  визначається співвідношенням кількості населення, що перебуває в зонах можливого ураження, до чисельності населення на території дослідження

$$K_2 (H_2) = N_2 / N,$$

де  $N_2$  – чисельність населення, що перебуває в зонах можливого ураження (чол.);

$N$  – чисельність населення на території дослідження (чол.).

Вплив регіонально розповсюджених екзогенних геологічних процесів у рамках природно-техногенної системи “хімічно небезпечний об’єкт – геологічне середовище” зумовлює формування техногенно-природного ризику, який визначається з урахуванням коефіцієнта впливу відповідних НЕГП на ХНО.

#### Комплексне оцінювання ризиків життєдіяльності

Метод комплексного оцінювання природно-техногенних ризиків життєдіяльності, обумовлених спільною дією небезпечних природних і техногенних чинників, що проявляються у вигляді НЕГП та аварій на ХНО, розроблено виходячи з наступних міркувань.

При функціонуванні складної техногенно-геологічної системи «хімічно небезпечний об’єкт – геологічне середовище» можливі різні небажані події природного ( $H_1$ ) і техногенного ( $H_2$ ) походження, які характеризуються різними за своїми масштабами і негативними наслідками для життєдіяльності населення.

Вважається, що будь-які з цих небажаних подій  $H_1$  і  $H_2$  мають певні природні чи техногенні прояви, а саме  $H_1$  – активізацію небезпечних екзогенних геологічних процесів,  $H_2$  – аварії на ХНО з викидом токсичних речовин. Причому прояв однієї з цих подій не виключає прояву іншої, тобто на потенційно небезпечній території може відбутися як активізація НЕГП, так і хімічно небезпечна аварія з викидом токсичних речовин.

За таких умов будемо вважати, що функціонування природно-техногенної системи може призвести до виникнення незалежних чи сумісних негативних подій природного і техногенного походження у вигляді проявів НЕГП та аварій на ХНО.

Оцінювання природно-техногенного ризику життєдіяльності, який враховує комплексну дію природних і техногенних факторів, базується на визначенні комбінованої ймовірності прояву подій природного ( $H_1$ ) і техногенного ( $H_2$ ) походження, що представлені відповідно у вигляді активізації НЕГП та аварій на ХНО. Припускаючи, що ці події є незалежними, комбінована ймовірність їхньої реалізації на даній території визначається за законом складання ймовірностей незалежних подій [8]

$$P_3 (H_3) = P_1 (H_1) + P_2 (H_2) - P_1 (H_1) * P_2 (H_2),$$

де  $P_3 (H_3)$  – комбінована ймовірність виникнення подій природного і техногенного походження (прояву НЕГП та аварії на ХНО);

$P_1 (H_1)$  – ймовірність прояву НЕГП;

$P_2 (H_2)$  – ймовірність виникнення аварії на ХНО.

Таким чином, оцінювання природно-техногенного ризику життєдіяльності можна здійснювати за наступним співвідношенням:

$$R_3 (H_3) = P_3 (H_3) * V_3 (H_3) * K_3 (H_3) * N,$$

де  $R_3 (H_3)$  – комплексний ризик загибелі чи втрати здоров'я населення на даній території в умовах можливих аварій на ХНО і проявів НЕГП (чол/рік);

$P_3 (H_3)$  – комбінована ймовірність виникнення аварії на ХНО і прояву НЕГП;

$V_3 (H_3)$  – уразливість території (частки одиниці);

$K_3 (H_3)$  – просторова уразливість населення (частки одиниці);

$N$  – чисельність населення на території дослідження (чол.).

Пропонований метод комплексного оцінювання ризиків життєдіяльності розглядається

далі на методичному прикладі можливої аварії на Мелітопольському ДКП “Водоканал”. Для моделювання використано такі вхідні параметри:

- вид небезпечної хімічної речовини – хлор;
- обсяг викиду – 300 т;
- температура повітря - + 20° C;
- напрямок вітру - північний;
- швидкість вітру - 3 м/с;
- ступінь вертикальної стійкості повітря – ізотермія;

фактори впливу природної небезпеки на ХНО – підтоплення і просідання лесових ґрунтів.

Відповідно до методики [ 7 ] визначаються параметри можливої зони хімічного зараження:

кут сектора зони з урахуванням стійкості напрямку вітрового потоку і швидкості вітру  $\alpha = 45^0$ ;

глибина зони  $R = 26,8$  км;

можлива площа зони  $S = \pi * R^2 * 45^0 / 360^0 = 281,8$  км<sup>2</sup>;

чисельність населення в зоні  $N = 18722$  чол.;

площа максимально можливого поширення токсичної хмари  $S_{max} = \pi * R^2 = 2255$  км<sup>2</sup>.

**Оцінювання техногенного ризику життєдіяльності** в умовах можливих аварій на ХНО здійснюється за наведеною вище формулою:

$$R_2(H_2) = P_2(H_2) * V_2(H_2) * K_2(H_2) * N.$$

Ймовірність виникнення аварії на ХНО з викидом токсичних речовин визначається як середньорічна частота хімічно небезпечних аварій у заданому регіоні, від яких можуть постраждати (захворіти або загинути) люди внаслідок отруєння. За даними МНС України у 2005 році зареєстровано 4 аварії на ХНО з викидом токсичних речовин, унаслідок яких постраждало 6 чоловік [4] загальна кількість ХНО в Україні складає 1575 об’єктів.

Таким чином, статистична ймовірність аварії  $P_2(H_2)$  на ХНО з викидом токсичних речовин, які становить загрозу для життєдіяльності населення, визначається співвідношенням:

$$P_2(H_2) = 4 / 1575 = 2,5 * 10^{-3}.$$

Уразливість території  $V_2(H_2)$  від можливої аварії на ХНО визначається відношенням ураженої частини території Запорізької області до її загальної площі

$$V_2(H_2) = 281,8 / 27200 = 0,01036.$$

Просторова уразливість населення регіону  $K_2(H_2)$  в умовах можливої аварії на ХНО визначається співвідношенням кількості населення в зоні можливого ураження (оцінюється засобами ГІС) до загальної кількості населення Запорізької області

$$K_2(H_2) = 71781 / 1929200 = 0,0372.$$

Таким чином, індивідуальний ( $N=1$ ) техногенний ризик життєдіяльності в регіоні при

повномасштабному прояві можливої аварії становитиме

$$R_2(H_2) = P_2(H_2) * V_2(H_2) * K_2(H_2) = 2,5 * 10^{-3} * 0,01036 * 0,0372 = 9,63 * 10^{-7} \text{ чол/рік.}$$

**Природний ризик життєдіяльності** на території можливого прояву НЕГП оцінюється за вище наведеним співвідношенням:

$$R_1(H_1) = P_1(H_1) * V_1(H_1) * K_1(H_1) * N.$$

Ймовірність прояву НЕГП у природному режимі їхнього розвитку  $P_1(H_1)$  залежить від двох головних чинників:

просторової уразливості території  $V_1(H_1)$  об’єктами НЕГП (частина сумарної площі зон підтоплення і просідань  $S_1$  у межах площі області  $S$ ):  $V_1(H_1) = S_1 / S$ .

часової динаміки розвитку  $K_t$  об’єктів НЕГП як частоти їхньої активізації за визначений проміжок часу  $T$  (років), унаслідок впливу швидко змінюваних гідрометеорологічних факторів активізація відбувається із середньою частотою 1 раз від 3-4 до 11-30 років:

$$K_t = 1/T = 1/(3-4) \div 1/(11-30) \approx 3 * 10^{-1} \div 3 * 10^{-2}, 1/\text{рік.}$$

Просторова уразливість території Запорізької області процесами підтоплення визначається наступним чином:

$$V_1(H_1) = 96,3 / 27200 = 0,00354.$$

Коефіцієнт часової динаміки розвитку процесів підтоплення за експертною оцінкою спеціалістів Державної геологічної служби України приймається  $K_t = 0,3$ , що відповідає середньостатистичній частоті активізації цих процесів: 1 раз у 3 роки.

З урахуванням цього визначається ймовірність прояву процесів підтоплення у можливій зоні хімічного зараження

$$P_1(H_1) = V_1(H_1) * K_t = 0,00354 * 0,3 = 0,00106.$$

Просторова уразливість населення  $K_1(H_1)$  визначається співвідношенням кількості населення на територіях можливого прояву НЕГП (оцінюється засобами ГІС) до загальної кількості населення регіону:

$$K_2(H_2) = 463008 / 1929200 = 0,24.$$

Таким чином, індивідуальний ( $N = 1$ ) природний ризик життєдіяльності на території можливого прояву НЕГП становитиме:

$$R_1(H_1) = P_1(H_1) * V_1(H_1) * K_1(H_1) = 0,0012 * 0,00354 * 0,24 = 9,02 * 10^{-7} \text{ чол/рік.}$$

**Оцінювання природно-техногенного ризику життєдіяльності**, який враховує комплексну дію природних і техногенних факторів, базується на визначенні комбінованої ймовірності прояву подій природного ( $H_1$ ) і техногенного походження ( $H_2$ ), що представлені відповідно у вигляді активізації НЕГП та аварій на ХНО. Припускаючи, що ці події є незалежними, комбінована ймовірність їхньої реалізації на даній території визначається за

відомим законом складання ймовірностей незалежних подій [ 8 ]

$$P_3 (H_3) = P_1 (H_1) + P_2 (H_2) - P_1 (H_1) * P_2 (H_2) = \\ = 2,5 \cdot 10^{-3} + 1,06 \cdot 10^{-3} - 2,5 \cdot 10^{-3} * 1,06 \cdot 10^{-3} \\ = 3,55 \cdot 10^{-3} / \text{рік}.$$

Оцінювання природно-техногенного ризику життєдіяльності здійснюється за співвідношенням:

$$R_3 (H_3) = P_3 (H_3) * V_3 (H_3) * K_3 (H_3) * N,$$

де  $R_3 (H_3)$  – комплексний ризик загибелі чи втрати здоров'я населення на даній території в умовах можливих аварій на ХНО та проявів НЕГП (чол/рік);

$P_3 (H_3)$  – комбінована ймовірність виникнення аварій на ХНО та прояву НЕГП;

$V_3 (H_3)$  – уразливість території (частки одиниці);

$K_3 (H_3)$  – просторова уразливість населення (частки одиниці);

$N$  – чисельність населення на території дослідження (чол.).

З урахуванням викладеного індивідуальний (N=1) природно-техногенний ризик життєдіяльності

$$R_3 (H_3) = P_3 (H_3) * V_3 (H_3) * K_3 (H_3) = 3,55 \cdot 10^{-3} * \\ 0,01036 * 0,0372 = 2,4 \cdot 10^{-6} \text{ чол} / \text{рік}.$$

### Висновки і перспективи подальших досліджень.

Для підвищення обґрунтованості рішень з упереджувачого реагування на техногенну небезпеку потрібно завчасно оцінювати ризики життєдіяльності від можливих аварій з урахуванням взаємодії техногенних і природних чинників, зумовлених проявами НЕГП як у межах промислових майданчиків, так і в зонах можливого впливу викидів небезпечних хімічних речовин. Це зумовлює необхідність в умовах особливого періоду у місцях розташування ХНО досліджувати і враховувати небезпеку прояву НЕГП.

### Література

1 Данилишини Б.М. Природно-техногенні катастрофи: проблеми економічного аналізу та управління.-К.: НІЧЛАВА, 2001.-260 с. 2. Биченок М.М., Іванюта С.П., Яковлев Є.О., Про вплив екзогенних геологічних процесів на рівень техногенних ризиків життєдіяльності // Збірник наукових праць УкрДІГРІ 2006- №1.- С..85-91 3. Буравлев Є.П., Гетман В.В. Управління техногенною безпекою України. – К.: ПНБ, 2006. – 248 с. 4. Національна доповідь про стан техногенної та природної безпеки в Україні у 2006 р. – К.: ДП «Чорнобильінтерінформ, 2007. – 236 с.5 Іванюта С.П. ПС реалізація оцінки ризику життєдіяльності від аварій на хімічно небезпечних об'єктах. // Екологія і ресурси. –

К.: ПНБ, 2005. – № 11. – С. 95-101.6 Качинський А.Б. Безпека, загрози і ризик: наукові моделі та математичні методи. – К.: ПНБ, НАСБУ, 2004.- 472 с. 7.Наказ іністерства з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, Міністерства аґарарної політики, Міністерства економіки, Міністерства екології і природних ресурсів №73/82/64/122 від 27 березня 2001 року "Про затвердження Методики прогнозування наслідків впливу (викиду) небезпечних хімічних речовин при аваріях на промислових об'єктах і транспорті". 8 Мушик Э., Мюллер П. Методы принятия технических решений. – М.: Мир, 1990. – 206 с.

## ОЦЕНИВАНИЕ РИСКОВ ЖИЗНЕДЕЯТЕЛЬНОСТИ ЛЮДЕЙ В ПРИРОДНО-ТЕХНОГЕННОЙ СРЕДЕ В УСЛОВИЯХ ОСОБОГО ПЕРИОДА

*Николай Николаевич Быченко (доктор технических наук, с.н.с.)*

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

*Возрастание антропогенного воздействия на окружающую среду вместе с интенсивным использованием природных ресурсов вызывают устойчивую тенденцию к увеличению негативных последствий для жизнедеятельности населения от чрезвычайных ситуаций природного и техногенного происхождения на территории Украины. Кроме того, в неблагоприятных экономических условиях, а также гибридной войны на востоке Украины со стороны РФ, снижается уровень технологической дисциплины, уменьшаются затраты на внедрение новейших технологий, модернизацию производственных процессов и ремонтно-профилактические мероприятия, возрастает количество изношенного оборудования.*

*В данной работе на основе обобщения опыта оценивания и прогнозирования рисков возникновения чрезвычайных ситуаций в разных регионах Украины, в первую очередь на территориях повышенной природной и техногенной опасности, разрабатываются методологические основы оценки рисков жизнедеятельности в этих условиях.*

*Ключевые слова:* чрезвычайные ситуации, риски жизнедеятельности, техногенные и природные угрозы.

**EVALUATION RISKS OF LIVE ACTIVITY OF PEOPLE IN NATURAL AND TECHNOGENIC ENVIRONMENT IN CONDITIONS OF SPECIAL PERIOD**

*Mikola Bychenok (Doctor of Technical Science, Senior Research Fellow)*

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

*The increase in anthropogenic impact on the environment, together with the intensive use of natural resources, cause a steady tendency to increase the negative consequences for the life of the population from emergencies of natural and man-made origin in Ukraine. In addition, in adverse economic conditions, as well as a hybrid war in eastern Ukraine from the Russian Federation, the level of technological discipline is reduced, the costs of introducing the latest technologies, modernizing production processes and repair and maintenance measures are decreasing, and the number of worn-out equipment is increasing.*

*In this work, based on a generalization of the experience of assessing and predicting the risks of emergencies in different regions of Ukraine, primarily in areas of high natural and man-made danger, methodological foundations for assessing the risks of life in these conditions are developed.*

**Key words:** *emergency situations, life risks, man-made and natural threats.*

**References**

- 1. Danilishin B.M.** Natural-technogenic catastrophes: problems of economical analyses and control – K.: NICH LAVA, 2001. – 260 p. **2. Bychenok M.M., Ivanjta S.P., Yakovlev Y.A.** About influence of exogenic geological process on level tehnogenic risk of live activity// Collection of scientific works of UkrDIGRI 2006 №1.- C.85-91 **3. Buravlov E.P., Getman V.V.** Control of technogenic safety – K.: IPNB, 2006. – 248 p. **4. National Report** about state of technogenic and natural safety in Ukraine in 2006 y. – K.: DP «Chernobylinterinform», 2007. – 236 p. **5. Ivanjta S.P.** GIS realization of estimation risk of life activity from accidents on chemical dangerous objects : // Ecologic and resourses – K.: IPNB, 2005. № 11. – P.95–101. **6. Kachynsky A.B** Safety, threats and risk : scientific models and mathematical methods K.: IPNB, NASBU, 2004.-.472c. **7. Order** of Ministry from questions of extraordinary situations and defence of population from consequences of Chernobyl catastrophe, Ministry of agrarian politics, Ministry of economic, Ministry of ecologic and natural resources № 73/82/64/122 from 27 March 2001 year «About confirmation of metodic prognouzing consequences influence (throw out) dangerously chemical substance in the time accidenns on industrial objects and transport. **8. Muschik E., Muller P.** Methods of technic decides – M.: Universe, 1990.-206 p.

*Дмитро Анатолійович Чопа* (кандидат технічних наук, с.н.с.)<sup>1</sup>  
*Анатолій Йосипович Дерев'янчук* (кандидат технічних наук, професор)<sup>2</sup>  
*Дмитро Андрійович Чехута*<sup>2</sup>

<sup>1</sup>Національний університет оборони України імені Івана Черняхівського, Київ, Україна

<sup>2</sup>Сумський державний університет, Суми, Україна

## ДЕЯКІ АСПЕКТИ СТВОРЕННЯ ТА ЗАСТОСУВАННЯ МОБІЛЬНИХ ДОДАТКІВ ДЛЯ ВИВЧЕННЯ ВІЙСЬКОВО-ТЕХНІЧНИХ ДИСЦИПЛІН

Сучасні умови функціонування Збройних Сил України, насамперед, підготовка військових фахівців в режимі скороченого часу та обмежених можливостей навчальної матеріально-технічної бази обумовлює нові підходи до організації навчання та підготовки. Тому у статті розглядаються деякі аспекти щодо створення мобільних додатків військово-технічного призначення, які можна встановлювати на різноманітні мобільні пристрої та використовувати їх під час підготовки військових спеціалістів. Авторами розглядаються етапи створення мобільних додатків, принципи побудови, функції та завдання, які мають вирішуватися мобільними додатками військово-технічного призначення.

Наведені результати аналізу педагогічного експерименту зі студентами, які навчаються на кафедрі військової підготовки Сумського державного університету, що дозволило зробити висновок про позитивний вплив використання мобільних додатків на підвищення якості та зростання рівня підготовки під час вивчення військово-технічних дисциплін.

Запропоновані напрями подальших досліджень щодо створення мобільних додатків військово-технічного призначення.

**Ключові слова:** мобільні додатки; мобільні пристрої; інтерфейс; користувач мобільного додатку; критерій Ст'юдента.

### Вступ

Дану статтю слід розглядати як подальший аналіз шляхів підвищення ефективності підготовки військових фахівців з військово-технічних питань за рахунок використання сучасних інформаційних технологій.

**Постановка проблеми.** Зараз існує нагальна потреба у вирішенні дуже складної проблеми: як здійснити якісну підготовку військових спеціалістів ракетних військ і артилерії (РВ і А) за короткий термін навчання (в умовах особливого періоду) та опанування зразками озброєння та військової техніки (ОВТ), що стоять на озброєнні Збройних Сил України, або швидко поновити отримані раніше та втрачені знання та практичні навички особовим складом, для ефективного виконання завдань у зоні проведення операції Об'єднаних сил (ООС).

Зазначені чинники вже висвітлювалися авторами в попередніх працях, де був здійснений аналіз основних стратегічних напрямів вирішення зазначеної проблеми. Досвід впровадження інформаційних технологій в навчання та підготовку військових фахівців надає широкі можливості для їх вдосконалення, а саме: підвищення мотивації до навчання; закріплення знань і практичних навичок; зменшення часу і коштів на підготовку; підвищення безпеки під час експлуатації ОВТ. Однак, при цьому, відслідковується недостатня орієнтація на підготовку фахівців у місцях виконання завдань, де відсутні мультимедійні та інші інтерактивні засоби навчання, а це позначається на якості підготовки фахівців, особливо у зоні бойових дій.

Слід зазначити, що розвиток мобільних

пристроїв відкриває нові можливості у використанні їх в інтересах підготовки у будь-якому місці, за будь-яких умов.

**Мета дослідження** полягає у подальшому пошуку та розвитку підходів щодо впровадження мобільних технологій у процес навчання спеціалістів у ВВНЗ, підготовки в військових частинах та навчальних центрах.

### Виклад основного матеріалу дослідження

Для кожного викладача або командира прагнення досягти максимально можливого рівня знань тими, хто навчається, завжди було і є професійною потребою та обумовлювало пошук шляхів до його здійснення.

З розвитком інформаційних технологій, мобільних пристроїв та Internet технологій, відкриваються нові шляхи і можливості втілити задумки викладача, командира передати знання особовому складу, навчити їх мислити і приймати правильні рішення у нештатних ситуаціях.

Тому у статті, будуть розглянуті деякі підходи щодо створення і застосування мобільних додатків, які можна використовувати на різних мобільних пристроях: смартфони; планшети; ноутбуки тощо.

Відмітимо, що мобільні додатки широко застосовуються у різноманітних галузях: бізнес, реклама і т. і., а у військовій галузі, зокрема для підготовки фахівців РВіА, майже не використовуються.

Тому в статті будуть розглянуті завдання, функції та операції, які повинні виконувати мобільні додатки; як будуть оброблятися дані; як

забезпечити зручність мобільного додатку для користувачів.

Аналіз досвіду створення мобільних додатків свідчить, що спроба відразу втілити в продукт повний набір функцій призводить до того, що мобільний додаток стає громіздким, складним і користуватися ним просто неможливо, так як він визначає не тільки стратегію і тактику у вивченні військово-технічних дисциплін (ВТД), інтеграцію інформаційних технологій у навчальний процес, але й дає ключові поняття цих технологій та раціональне їх використання.

Різні автори пропонують різні етапи створення мобільних додатків [2,3].

Огляд досліджень [1,4-6] показав, що кількість етапів буде залежати від відповіді на такі питання: для чого створюється цей додаток? Яку користь він принесе користувачам? Чи захочуть користувачі його використовувати? Яка аудиторія користувачів? Які переваги буде мати мобільний додаток перед іншими, якщо такі вже є?

Щоб знайти відповіді на ці питання потрібно провести аналіз запиту потреб користувачів. А для цього необхідно обґрунтувати їх зацікавленість (мотивацію) у використанні мобільного додатку.

Спочатку провести моніторинг цільової аудиторії та визначити її так звані "больові точки", тобто з'ясувати її потреби.

По-друге, визначити обсяг потреб наших користувачів.

По-третє, треба сформулювати функціонал мобільного додатку і визначити його ключові можливості. Із наведеного вище, впливає потреба у визначенні ключових моментів, як повинен функціонувати мобільний додаток, а саме: що він повинен робити; які завдання, функції та операції він повинен виконувати (інтеграція з іншими додатками або контентом і т. і.), як він буде (якщо це потрібно) обробляти дані і чи буде збирати такі дані від користувачів.

Викладене вище є **першим етапом**, на якому розробляються варіанти використання для того, щоб зрозуміти, як користувачі будуть взаємодіяти з додатком. Зауважимо, що чим більше буде додано функцій, тим складнішим буде продукт і, відповідно, часу на його створення буде витрачено більше.

Найголовніше, що потрібно мати на увазі при розробленні мобільного додатку - переконатися, що він є одночасно і корисним, та інтуїтивно зрозумілим. Добре продуманий дизайн інтерфейсу користувача вирішує обидві ці проблеми. Основні пріоритети щодо розроблення дизайну наведені нижче.

**Видалення зайвого.** Надлишковий інтерфейс перевантажує користувача занадто великим обсягом інформації: кожна нова кнопка, зображення або рядок тексту робить екран більш складним.

**Очевидна навігація.** Допомога в навігації має бути головним пріоритетом будь-якої програми.

**Встановлення правильних розмірів цілей натискання,** кнопки тощо. По маленьких кнопках користувачу складніше влучити, ніж по великих. При створенні мобільного інтерфейсу кнопки та

об'єкти натискання краще робити досить великими, щоб по них було простіше натиснути.

**Текст повинен бути розбірливим.** У порівнянні зі стаціонарними комп'ютерами, які комплектуються достатньо великими моніторами, мобільні гаджети мають відносно невеликі екрани, а це означає, що одна з проблем мобільного дизайну – вмістити великий обсяг інформації на маленькому UI (*User Interface*).

**Елементи інтерфейсу має бути добре видно.** Розробники повинні використовувати такий колір і контраст, щоб допомогти користувачам бачити та інтерпретувати зміст нашого додатку, тобто необхідно забезпечити зручність користування (*usability*).

Викладене вище, представляє собою **другий етап** створення мобільного додатку.

Розглянемо ще один важливий аспект технічних можливостей нашого додатку, які суттєво впливають на якість і інформативність додатку в цілому, а саме, **анімацію**.

Анімації використовуються коли користувач не має можливості спостерігати ті чи інші явища в реальному часі-просторі, наприклад, дію снаряда по броні, дію механізмів підричника при пострілі, у польоті, при зустрічі з перешкодою тощо.

Під час вивчення зразка ОБТ, наприклад, самохідних гармат, анімація дає можливість побачити всі вузли і механізми, які знаходяться всередині гармати, та їх дію. В даному випадку найбільш доцільно використовувати 3D, 3D-max моделювання з одночасним стислим описом того чи іншого явища, дії механізму, боеприпасу тощо.

Таким чином розглянуто **третій етап** створення мобільного додатку.

Після завершення процесу розроблення мобільного додатку потрібно перевірити, виявити неточності, помилки та інші негативні сторони програмного продукту.

Після того, як базовий функціонал протестований, необхідно переконатися, що мобільний додаток є досить простим у використанні та забезпечує потрібний результат для користувача.

**Тестування сумісності.** Мобільні пристрої розрізняються залежно від платформи, моделі та версії їх операційної системи. Важливо обрати таку підмножину пристроїв та програмного забезпечення, яка буде відповідати нашому додатку.

Необхідно врахувати вплив зовнішніх чинників, а саме, наявність інших мобільних додатків на пристрої, які можуть негативним чином впливати на роботу знов розробленого додатку.

Викладене вище представляє собою **четвертий та п'ятий етапи**. Таке поєднання відбувається тому, що низка процедур із забезпечення потреб користувача відбувається на етапі тестування. Процедура, яка не відбувається на етапі тестування – це розміщення додатку в мережі Internet.

Загальна схема розроблення мобільного додатку представлена на рис. 1.



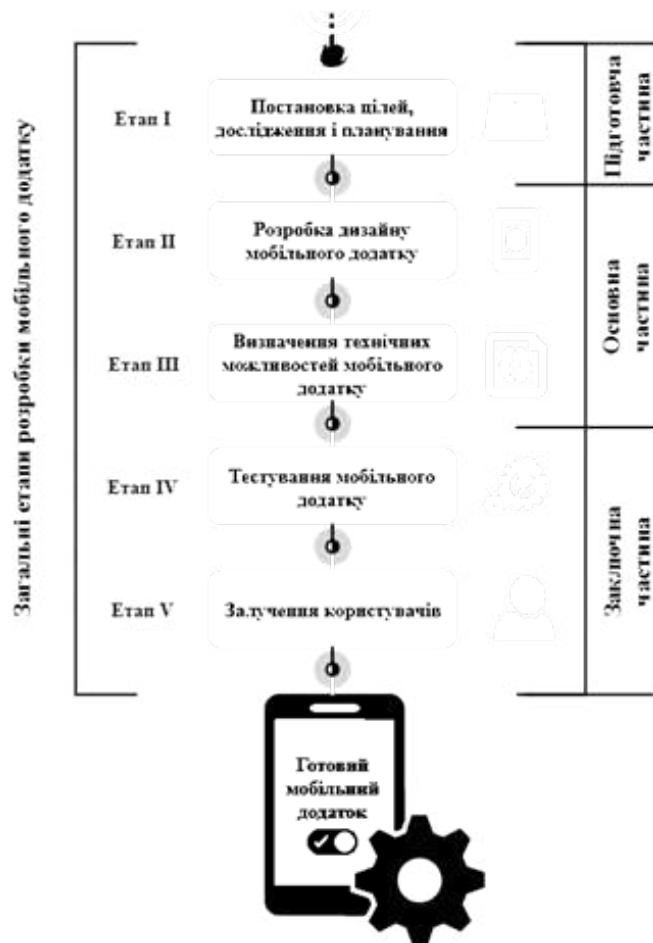


Рис. 1. Етапи створення мобільного додатку

**Вибір операційної системи (ОС).** Пропонується використання ОС Android, тому що саме ця ОС найбільше розповсюджена серед користувачі мобільних пристроїв, забезпечує більш дешеве та доступне розроблення. Крім того, мобільний додаток під ОС Android дає доступ до широкій аудиторії фахівців. Як приклад, розглянемо

розроблений мобільний додаток “152-мм самохідна гаубиця 2С3М. Це дуже просто (Вивчаємо за 10 днів)”.

Скріншоти інтерфейсу та приклади користування мобільним додатком наведені на рис. 2, 3.

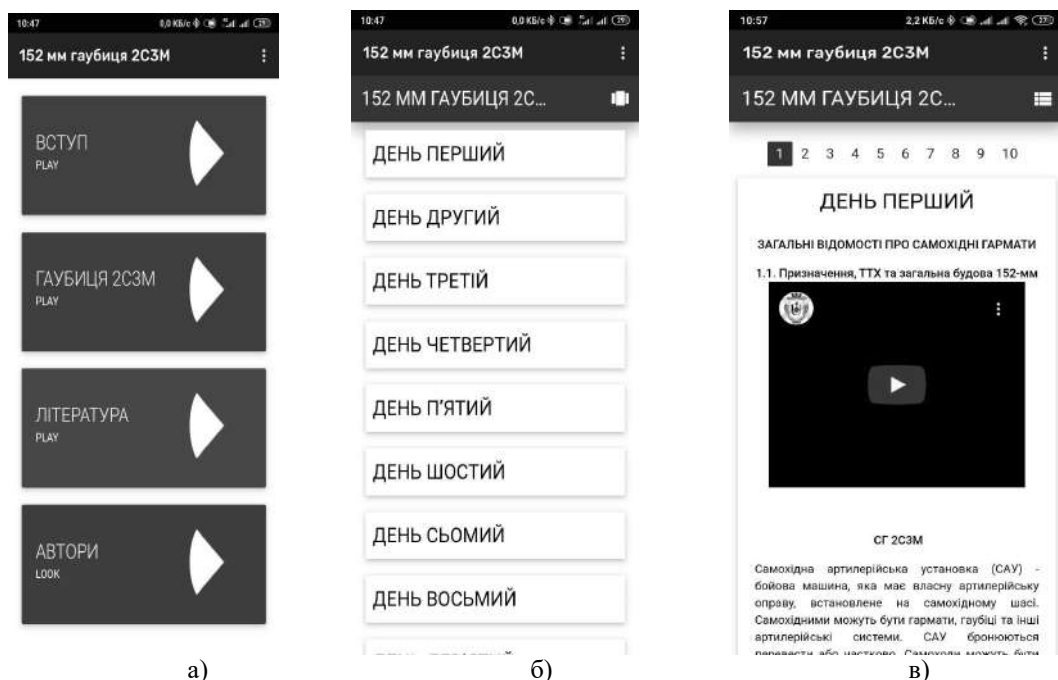


Рис. 2 Скріншоти інтерфейсу мобільного додатку (а – навігація додатку; б – зміст додатку; в – перехід із змісту на пункт навігації (день 1-й))

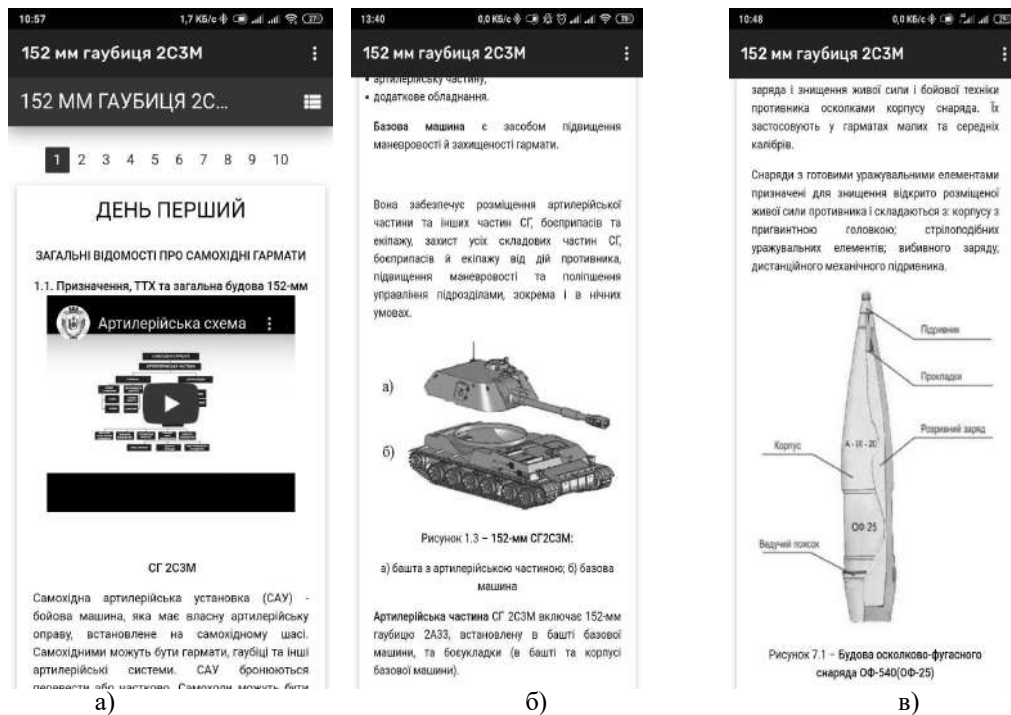


Рис. 3 Скріншоти з мобільного додатку (а – використання відео у додатку; б – використання анімації при вивченні будови 2С3М (день 1-й); в – використання анімації при вивченні будови осколково-фугасного снаряда (день 7-й))

Після створення мобільного додатку можна розглянути його переваги, які наведені на рис. 4.

З метою перевірки доцільності застосування мобільного додатку був організований демонстраційний експеримент.

На початку використання мобільного додатку у процесі навчання результати не відповідали очікуванням, з достатньою кількістю помилок і значною витратою часу.

На проміжному етапі процес навчання із застосуванням мобільного додатку показав

зростаючу динаміку. Паралельно була запропонована методика оцінки застосування мобільного додатку в процесі навчання студентів.

Таким чином, використовуючи методику оцінки застосування мобільного додатку було досліджено вплив мобільного додатку на процес навчання студентів. Взвод був поділений на дві групи по 13 чоловік у кожній. Перша група використовувала традиційний метод, як на планових заняттях, так і під час самостійної підготовки.

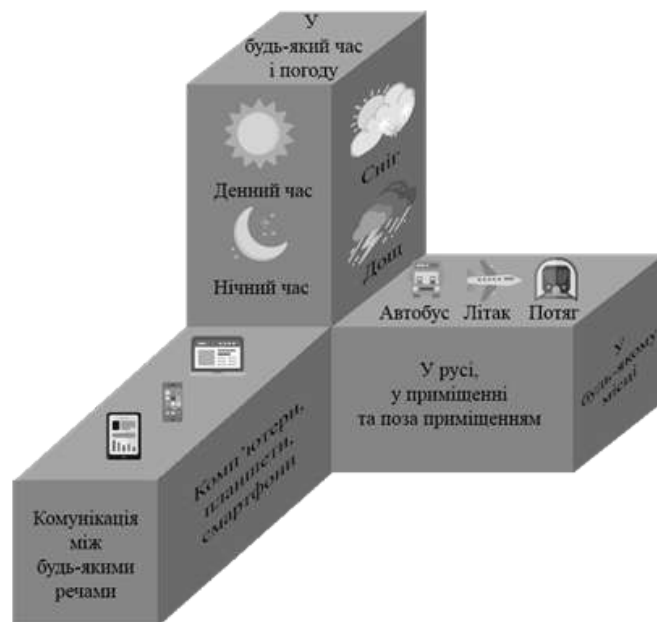


Рис. 4 Переваги використання мобільного додатку перед традиційними методами навчання

У другій групі проводилось заняття з використанням мобільного додатку.

Результати досліджень у згаданих вище групах наведені у таблиці 1. Було перевірено гіпотезу

впливу інноваційного метода навчання (застосування мобільного додатку) на підготовку студентів з рівнем значимості 0,05. У даному випадку представлені парні вибірки.

Таблиця 1

Порівняльні результати визначення рівнів розвитку студентів на традиційних заняттях та заняттях із використанням мобільного додатку

Студенти	До проведення занять	Після проведення	Різниця величин	Квадрат різниці
1	45	53	8	64
2	37	42	5	25
3	64	80	16	256
4	65	73	8	64
5	56	67	11	121
6	65	81	14	196
7	52	68	16	256
8	80	92	8	64
9	78	85	7	49
10	77	87	10	100
11	72	84	12	144
12	80	90	9	81
13	70	79	9	81

Подальші розрахунки (результати) отримані після проведення статистичного аналізу даних за допомогою розрахунку критерію Ст'юдента і наведені у таблиці 2.

Аналіз та обробка отриманих експериментальних даних шляхом проведення контрольних заходів, відбувалась із застосування статистичного критерію Ст'юдента. Відповідно до результатів аналізу, можна зробити висновок, що гіпотеза, яка перевірялася, має право на існування, про що свідчить порівняння отриманого значення критерію Ст'юдента із табличним.

Отримане значення критерію Ст'юдента  $t_c$

менше табличного, що в свою чергу, підтверджує висунуту гіпотезу. Маючи результати перевірки гіпотези, можна зробити висновок, що особовий склад групи 2, підготовка якого відбувалась з використанням мобільного додатку, ефективніший, успішніший, має більш якісний показник отриманих знань за групу 1, підготовка якої здійснювалась традиційним способом.

Обчислений показник ефективності групи 2 дає можливість побачити наскільки ефективніше відбувається підготовка військових спеціалістів з використанням мобільного додатку.

Таблиця 2

Результати аналізу порівняння підготовки двох груп традиційним та інноваційним способами

Група № 1 – Традиційний спосіб підготовки		Група № 2 – підготовка взводу з використанням мобільного додатку	
$M = 11,4$	Обчислення математичного очікування	$M = 13,6667$	
$S = 1,24845$	Обчислення середньоквадратичного відхилення	$S = 0,49013$	
Обчислюємо значення критерію Ст'юдента та порівнюємо його з табличним значенням, для прийняття або відхилення гіпотези, що перевіряється.			
$t_c = 0,23013$		<	$t_{c(табл)} = 12,7062$

Показник ефективності Е визначається за формулою (1):

$$E = \left( \frac{M_2 \cdot 100}{M_1} \right) - 100 \quad (1)$$

де:  $M_1, M_2$  – обчислене математичне очікування для груп 1, 2.

Обчислення формули (1) показали, що ефективність групи 2 у порів'янні із групою 1

більша на 19,88 %, що в свою чергу, підтверджує доцільність впровадження та ефективність використання мобільного додатку у процесі підготовки військових спеціалістів. З метою удосконалення створення мобільних додатків та методики їх застосування серед студентів проведено опитування щодо його оцінки. Результати опитування відображені на рис.5.

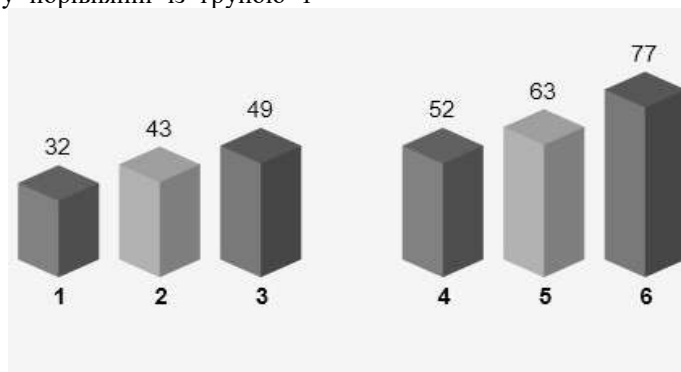


Рис. 5 Рівень оцінювання мобільного додатку студентами (1, 2, 3, 4, 5, 6 – умовні позначення навчальної групи)

Приблизно 11% студентів не оцінили традиційних методів навчання (на рисунку не показано) застосування мобільного додатку через складність інтегрування застосування мобільного додатку до

## Висновки і перспективи подальших досліджень

Таким чином, в статті розглянуті основні етапи створення та використання мобільного додатку. Це дозволяє зробити висновок про доцільність їх впровадження як в теорію, так і в практику організації

освітнього процесу та підготовки військових фахівців.

Подальші дослідження щодо розроблення та використання мобільних додатків доцільно присвятити розробці web-ресурсу, що дозволить вирішити проблеми сумісності з операційними системами та іншими мобільними та стаціонарними пристроями.

## Література

1. Разработка мобильных приложений <https://ru.flamix.software/about/news-article/razrabotka-mobilnykh-prilozheniy/>. 2. Этапы разработки мобильных приложений <https://appsstudio.ru/etapy-razrabotki-mobilnogo-prilozheniya>. 3. Этапы разработки мобильного приложения <http://www.orthedu.ru/news/13655-etapy-razrabotki-mobilnogo-prilozheniya.html>. 4. Создание мобильного приложения за 1

месяц. Реальность или миф? [https://inostudio.com/ru/article/mobile\\_app\\_sroki.html](https://inostudio.com/ru/article/mobile_app_sroki.html). 5. Полат Е.С. Новые педагогические и информационные технологии в системе образования. Москва. Академия, 2002. 272 с. 6. Принципы дизайна мобильных приложений от google <https://lpgenerator.ru/blog/2016/04/05/principy-dizajna-mobilnyh-prilozhenij-ot-google/>.

## НЕКОТОРЫЕ АСПЕКТЫ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ДЛЯ ИЗУЧЕНИЯ ВОЕННО-ТЕХНИЧЕСКИХ ДИСЦИПЛИН

*Дмитрий Анатольевич Чопа (кандидат технических наук, с.н.с.)<sup>1</sup>  
Анатолий Йосипович Деревьянчук (кандидат технических наук, профессор)<sup>2</sup>  
Дмитрий Андреевич Чехута<sup>2</sup>*

<sup>1</sup>Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

<sup>2</sup>Сумской государственной университет, Сумы, Украина

Современные условия функционирования Вооруженных Сил Украины, прежде всего, подготовка военных специалистов в режиме сокращенного времени и ограниченных возможностей учебной материально-технической базы обуславливает новые подходы к организации обучения и подготовки. Поэтому в статье рассматриваются некоторые аспекты по созданию мобильных приложений военно-технического назначения, которые можно устанавливать на различные мобильные устройства и использовать их при подготовке военных специалистов. Авторами рассматриваются этапы создания мобильных приложений, принципы построения, функции и задачи, которые должны решаться мобильными приложениями военно-технического назначения.

Приведенные результаты анализа педагогического эксперимента со студентами, которые учатся на кафедре военной подготовки Сумского государственного университета, позволило сделать вывод о положительном влиянии использования мобильных приложений на повышение качества и рост уровня подготовки при изучении военно-технических дисциплин.

Предложены направления дальнейших исследований по созданию мобильных приложений военно-технического назначения.

**Ключевые слова:** мобильные приложения; мобильные устройства; интерфейс; пользователь мобильного приложения; критерий Стьюдента.

## SOME ASPECTS OF CREATING AND USING MOBILE APPLICATIONS FOR THE LEARNING OF MILITARY TECHNICAL DISCIPLINES

*Dmitro Chopa (Candidate of technical sciences, Senior Research Fellow)<sup>1</sup>  
Anatolii Dereviachuk (Candidate of technical sciences, professor)<sup>2</sup>  
Dmitro Chehuta*

<sup>1</sup>National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

<sup>2</sup>Sumy State University, Sumy, Ukraine

Modern conditions for the functioning of the Armed Forces of Ukraine, first of all, the training of military specialists in the conditions of reduced time and limited capabilities of the educational and training base determines new approaches to the organization of education and training. Therefore, the article discusses some aspects of development military-technical mobile applications that can be installed on various mobile devices and used in training military specialists. The authors consider the stages of creating mobile applications, the principles of construction, functions and tasks that should be solved by mobile military-technical applications.

The results of the analysis of the pedagogical experiment with students who are studying at the Department of Military Training of Sumy State University allowed us to conclude that the use of mobile applications has a positive effect on improving the quality and increase of the level of training in the learning of military-technical disciplines.

The directions of further research on the development of mobile military-technical applications are proposed.

**Keywords:** mobile applications; mobile devices; interface; mobile application user; Student criterion.

## References

1. Razrabotka mobilnykh prilozheniy [Mobile Application Development]. <https://ru.flamix.software/about/news-article/razrabotka-mobilnykh-prilozheniy/>. 2. Etapyi razrabotki mobilnykh prilozheniy [Mobile applications development stages]. <https://appsstudio.ru/etapy-razrabotki-mobilnogo-prilozheniya>. 3. Etapyi razrabotki mobilnogo prilozheniya [Mobile application development stages]. <http://www.orthedu.ru/news/13655-etapy-razrabotki-mobilnogo-prilozheniya.html>. 4. Sozdanie mobilnogo prilozheniya za 1 mesyats. Realnost ili mif? [Creation of a mobile

application in 1 month. Reality or myth]. [https://inostudio.com/ru/article/mobile\\_app\\_sroki.html](https://inostudio.com/ru/article/mobile_app_sroki.html). 5. Polat E. (2002). Novyie pedagogicheskie i informatsionnyie tehnologii v sisteme obrazovaniya [New pedagogical and information technologies in the education system]. Moskva. Akademiya. 6. Printsipyi dizayna mobilnykh prilozheniy ot google [Google mobile app design principles]. <https://lpgenerator.ru/blog/2016/04/05/principy-dizajna-mobilnyh-prilozhenij-ot-google/>.

*Юрій Васильович Кравченко (доктор технічних наук, професор)*

*Андрій Петрович Мусієнко (доктор технічних наук)*

*Максим Георгійович Тищенко (кандидат технічних наук)*

*Спартак Юрійович Гогоняц (кандидат військових наук, с.п.с.)*

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

## МЕТОДИКА ОПРАЦЮВАННЯ ЕКСПЕРТНИХ ДАНИХ ДЛЯ УДОСКОНАЛЕННЯ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

*В роботі було проведено класифікацію засобів автоматизації освітнього процесу у системі військової освіти. На основі проведеного аналізу було визначено, що одним із важливих факторів ефективного функціонування системи дистанційного навчання є наявність експертів, які контролюють якість дистанційних курсів та пропонують методи їх удосконалення. З метою розроблення механізму роботи експертів щодо оцінювання ефективності та якості курсів дистанційного навчання була запропонована методика здійснення колективної експертизи ефективності та якості курсів дистанційного навчання та опрацювання отриманих експертних даних у групі експертів. Алгоритм розрахунків з використанням запропонованої методики передбачає визначення фахового рівня експертів; оброблення значень показників, визначених експертами; визначення узагальненого значення певного показника; визначення значення узагальненого показника.*

***Ключові слова:** дистанційне навчання; експертна оцінка; інформаційні технології; військова освіта.*

### Вступ

Швидкий розвиток комп'ютерних технологій став поштовхом до розвитку інформаційного суспільства. Об'єктивним процесом постіндустріального інформаційного суспільства є інформатизація та інтелектуалізація освіти. Вона полягає в глобальній інформатизації інтелектуальної діяльності за рахунок використання інформаційних технологій та можливості підбору відповідних курсів навчання в залежності від рівня підготовленості слухача. Інформаційні технології за своїми дидактичними властивостями впливають на всі компоненти навчання. Завдяки процесу інформатизації стала можливою нова синтетична, інтегральна гуманістична форма навчання – дистанційне навчання, яке вбирає в себе кращі риси традиційних форм навчання і добре з ними інтегрується [1]. Згідно із Законом України „Про вищу освіту” дистанційна освіта набула офіційного статусу самостійної форми навчання і розвивається швидкими темпами.

Обґрунтуємо доцільність створення системи дистанційного навчання у Збройних Силах України. В Україні та за кордоном вже накопичений значний досвід впровадження

дистанційного навчання. Увага до цієї форми навчання спостерігається як у цивільній, так і у військовій освіті [2]. В умовах їх інтеграції стає очевидним, що науково-дослідна та практична робота у військових навчальних закладах над проблемами дистанційного навчання повинна бути постійною і безперервною. Водночас слід зауважити, що специфіка підготовки військових фахівців визначає деякі особливості впровадження дистанційної форми навчання. Освітній процес за дистанційною формою навчання на першому етапі втілення можна поділити на чотири напрями [3, 4]:

навчання в межах системи військової освіти слухачів, курсантів, студентів ВВНЗ (ВНП ЗВО) (підготовка офіцерів запасу), фахівців для інших силових структур та іноземних військовослужбовців;

підвищення кваліфікації та курсова підготовка, індивідуальна підготовка офіцерів Збройних Сил України;

надання можливості військовослужбовцям строкової служби (служби за контрактом) отримати освіту за дистанційною формою навчання за рахунок МО України (умови контракту);

надання можливості військовослужбовцям Збройних Сил України отримати вищу освіту за дистанційною формою навчання за рахунок фізичних або юридичних осіб.

Отже, дистанційна форма навчання у системі військової освіти призвана вирішувати специфічні завдання, які важко вирішити з використанням традиційних форм, що потребують впровадження нових педагогічних технологій навчання; застосування засобів телекомунікаційного зв'язку; розвитку творчої складової освіти; створення віртуального інформаційно-освітнього середовища.

**Постановка проблеми.** Для реалізації освітнього процесу у системі військової освіти за дистанційною формою навчання необхідне створення системи дистанційного навчання військової освіти та розроблення механізму роботи експертів щодо оцінювання ефективності та якості курсів дистанційного навчання. Це завдання передбачає: створення нової нормативно-правової бази; визначення джерел фінансування; створення організаційних структур, які забезпечать реалізацію цієї форми навчання; використання висококваліфікованих експертів для аналізу та удосконалення розроблених курсів дистанційного навчання.

Таким чином актуальною є проблема розроблення теоретичних підходів до здійснення колективної експертизи ефективності та якості курсів дистанційного навчання та опрацювання отриманих експертних даних в групі експертів.

**Метою статті** є формулювання методики роботи експертів щодо оцінювання ефективності та якості курсів дистанційного навчання.

### Виклад основного матеріалу дослідження

Використання інформаційних технологій у системі військової освіти в першу чергу спрямовано на розвиток інформаційного забезпечення навчального процесу шляхом застосування інформаційних систем для денного (заочного) та дистанційного навчання, електронних підручників, автоматизованих систем контролю знань, автоматизованих систем проектування та наукових досліджень, автоматизованих систем моделювання, баз даних та баз знань. Також широкого застосування набули автоматизовані бібліотечні системи, довідникові системи тощо. Всі ці системи дозволяють сформулювати та підтримувати роботу єдиного інформаційного простору [5]. Окрім цього, існує другий тип автоматизованих систем управління у системі військової освіти, які призначені для підтримки функціонування системи дистанційної освіти з точки зору адміністративно-управлінського функціоналу. Це автоматична

система управління для планування, аналітичної обробки, супроводу та управління адміністративно-господарської та фінансово-економічної діяльності. Таким чином, можна класифікувати автоматизовані системи за двома напрямками: автоматизовані системи управління навчальним процесом військовослужбовців та автоматизовані системи управління для забезпечення даного навчання.

Отже, автоматизовані системи управління класифікуються за характером задач, які вони здатні вирішувати. Це автоматизовані системи адміністративного управління, управління персоналом, управління документами, управління науково-дослідними роботами, організаційного та матеріально-технічного управління, управління якістю освіти, управління документообігом.

Як зазначено в [6], інформаційні технології відкривають нові умови та можливості для сфери освітньої діяльності: покращення навчального процесу, оновлення навчальних програм, оперативного пошуку інформації тощо. В [7] розглядається створення корпоративної інформаційної системи вищого навчального закладу, яка враховує галузеву специфіку діяльності. Розширення та поява нових видів діяльності вимагає розвитку організаційної структури, яка визначає функції та склад управління структурними підрозділами. При цьому змін зазнають також і структурні одиниці.

Особливостями створення інформаційних систем дистанційного навчання військовослужбовців є [8]:

діяльність в різних областях, багатопрофільність; різноманіття форм організації навчальної роботи, методів; просторово розгалужена інфраструктура.

При створенні інтегрованої інформаційної системи дистанційного навчання військовослужбовців необхідно:

дотримуватись модульності структури; забезпечувати єдині вимоги до інтерфейсів; використовувати надійні, здатні до розширення, програмні та апаратні рішення; залучати спеціалістів з предметних областей тих задач, які автоматизуються – управлінська сфера, навчання, наука тощо.

Створена таким чином інформаційна система буде здатна вирішувати поставлені задачі та сприятиме покращенню діяльності системи дистанційного навчання Збройних Сил України. Проте, жодна система дистанційного навчання не може існувати без експертів, які контролюють якість дистанційних курсів та пропонують методи їх удосконалення. В першу, основними експертами з оцінювання якості дистанційних курсів є

безпосередньо ті, хто навчається. Саме вони можуть надати найбільш об'єктивну інформацію щодо зручності інтерфейсу курсу, логічності структурування та подання навчальної інформації, та рекомендацій щодо покращення, як змістовної частини, так і формату курсу. Але, на етапі розроблення та удосконалення дистанційних курсів необхідно мати групу висококваліфікованих експертів предметної галузі та тих, хто має досвід розроблення навчальних матеріалів із використанням технологій дистанційного навчання.

Методи оброблення експертної інформації можна розподілити на три основні групи: статистичні, алгебраїчні та шкалування. Статистичні методи ґрунтуються на ідеї, що відхилення оцінок експертів від істинних здійснюється у силу випадкових причин; завдання полягає у тому, щоб відновити це істинне значення з найменшою похибкою. Зміст алгебраїчних методів полягає в тому, що на множині допустимих оцінок задається відстань. Результат визначається як оцінка, сума відстаней від якої до оцінок експертів буде мінімальна. Метод шкалування полягає у тому, що завдяки експертній інформації про ступінь розбіжностей об'єктів встановлюється мінімальний або близький до мінімального набір критеріїв. Далі на основі даних критеріїв проводиться оцінювання об'єктів та виявляються розбіжності. В роботі [9] запропоновано використання спектрального підходу до оцінювання експертних знань, але на практиці цей підхід поки що не використовується. Авторами [10-14] досліджені питання розвитку систем дистанційного навчання, які є теоретичною основою запропонованою в статті методики.

В роботі пропонується методика опрацювання експертних даних в групі експертів. Вимоги до методики: урахування професійного рівня експертів; нейтралізація максимально можливою мірою фактору суб'єктивізму.

Загальний зміст методики: здійснюється визначення фахового рівня експертів;

визначається експерт-лідер на основі оцінки фахового рівня експертів;

усі значення показників, визначені експертами, перераховуються з урахуванням їх професійного рівня відносно експерта-лідера;

загальна оцінка за кожним показником визначається як середньоарифметична величина оцінок усіх експертів.

Алгоритм розрахунків.

1. Визначення фахового рівня експертів.

З метою об'єктивізації та узагальнення оцінок експертів застосований підхід, який полягає у максимальному урахуванні рівня професійності

під час узагальнення даних, отриманих від експертів. Для цього були визначені показники оцінки фахового рівня експертів  $f_e$ .

Для спрощення процедури урахування досвіду експертів показники оцінюються за двозначною шкалою:

1 – наявність визначених умов;

0 – відсутність визначених умов.

Введемо значення інтегрального показника як сума значень всіх показників.

З метою виділення одного лідера серед фахівців, які мають найвищий фаховий рівень, як правило, надають перевагу тому, хто має теоретичний та практичний досвід роботи у сфері розроблення курсів дистанційного навчання.

2. Перерахування значень показників, визначених експертами. Різниця між фаховим рівнем експерта-лідера і експерта визначається за формулою

$$\Delta f_e = f_{el} - f_e,$$

де:  $f_e(f_{el})$  – фаховий рівень експерта (експерта-лідера), який показує ступінь відповідності визначених ним показників реальному стану справ (значення належать інтервалу  $[0...1]$ ).

Величина розбіжності між значеннями певного показника, визначеними експертом-лідером і експертом, визначається за формулою

$$\Delta q_e = q_{el} - q_e,$$

де:  $q_e(q_{el})$  – значення певного показника, визначене експертом (експертом-лідером).

Перераховане значення показника, визначене експертом, з урахуванням поправки на його фаховий рівень, визначається за формулою

$$q'_e = q_e + \Delta f_e \cdot \Delta q_e = q_e + (f_{el} - f_e) \cdot (q_{el} - q_e).$$

Фізичний зміст другої складової у цій формулі полягає у тому, що вона визначає ту частку похибки, яка вноситься експертом за рахунок різниці у фаховому рівні між ним та експертом-лідером  $(f_{el} - f_e)$ . Знак цієї складової

визначається різницею  $(q_{el} - q_e)$ , адже різниця  $(f_{el} - f_e)$  завжди має знак «+», оскільки значення фахового рівня експерта-лідера не може бути нижчим за фаховий рівень інших експертів. Отже, перераховане значення певного показника  $q'_e$ , визначене експертом, буде завжди ближчим до значення цього ж показника, визначеного експертом-лідером  $q_{el}$ .

3. Визначення узагальненого значення певного показника.

Отримані на першому кроці перераховані значення певного показника, як і початково визначені експертами з різним фаховим рівнем, відображають їх оцінки значення цього показника так, якби кожний з експертів мав такий же фаховий рівень, який у експерта-лідера. Це припущення дає підстави для того, щоб узагальнене значення певного показника визначати як середньоарифметичне від значень показника, визначених кожним експертом

$$q_{yj} = \frac{\sum_{i=1}^N q_{ei}^j}{N},$$

де  $q_{ei}^j$  – перераховане значення  $j$ -го показника, початково визначене  $i$ -м ( $i \in [1, \dots, N]$ );

$N$  – кількість експертів.

4. Визначення значення узагальненого показника.

Для визначення узагальненого показника стану ситуації за даною методикою необхідно визначити перераховані значення важливості  $j$ -го показника. Величина розбіжності між значеннями важливості певного показника, визначеними експертом-лідером і експертом, визначається за формулою

$$\Delta w_e = w_{el} - w_e,$$

де  $w_e(w_{el})$  – значення важливості певного показника, визначене експертом (експертом-лідером).

Перераховане значення важливості показника, визначене експертом, з урахуванням поправки на його фаховий рівень, визначається за формулою  $w'_e = w_e + \Delta f_e \cdot \Delta w_e = w_e + (f_{el} - f_e) \cdot (w_{el} - w_e)$ . Фізичний зміст другої складової у цій формулі аналогічний розглянутому раніше. Узагальнене значення важливості певного показника визначається також як середньоарифметичне від перерахованих значень важливості показника:

$$w_{yj} = \frac{\sum_{i=1}^N w_{ei}^j}{N}.$$

Наступним кроком визначається нормоване значення важливості  $y$ -го показника за формулою

$$w_{Hj} = \frac{w_{yj}}{\sum_{i=1}^N w_{ei}^j},$$

де  $w_{yj}$  – значення важливості  $j$ -го показника ( $j \in [1, \dots, K]$ );

$K$  – кількість показників.

Значення узагальненого показника ефективності визначається за формулою

$$q_y = \sum_{j=1}^K q_{yj} w_{Hj}.$$

Результати аналізу надаються кожною комісією у вигляді розгорнутого висновку, в якому визначається обґрунтована пропозиція комісії щодо ефективності та якості певного курсу дистанційного навчання.

Завданням експертизи у цілому є отримання об'єктивних характеристик (як позитивних, так і негативних) та складання пропозицій щодо ефективності розроблених курсів в системі дистанційного навчання Збройних Сил України. Після обговорення кожного з вузлових питань в експертній комісії готується висновок, що є першою ітерацією пропозицій щодо вирішення питання ефективності розробленого курсу (їх кількість дорівнює кількості комісій) та передається для обговорення в підрозділ дистанційного навчання ВВНЗ (ВНП ЗВО). Комісія обговорює зауваження, вносить корективи. Таким чином відбувається удосконалення системи дистанційного навчання Збройних Сил України.

### Висновки і перспективи подальших досліджень

В роботі визначено, що методи експертного аналізу є основними в категорії методів інтелектуального аналізу даних. Когнітивні функції експерта часто неможливо описати аналітичними чи іншими способами. Тому пропонується використовувати саме їх для аналізу проблем, отримання експертної інформації в механізмі прийняття рішень щодо ефективності курсів дистанційного навчання та розроблення рекомендацій з покращення існуючих курсів. В роботі запропонована методика здійснення колективної експертизи та опрацювання експертних даних в групі експертів. Дана методика використовується з урахування професійного рівня експертів, нейтралізації максимально можливою мірою фактору суб'єктивізму, максимальної простоти та орієнтації на використання фахівців, які мають справу з роботою та навчанням в галузі військових наук та інформаційних технологій.

### Література

1. Jacob W. Interdisciplinary trends in higher education / Palgrave Communications. 2015. Vol. 1. URL: <https://www.nature.com/articles/palcomms20151>.

Наказ Міністерства Оборони України від 21.12.2015 №744 Про затвердження Концепції дистанційного навчання у Збройних Силах України. – [Електр. ресурс].



– Режим доступу: [www.mil.gov.ua/science\\_and\\_defense](http://www.mil.gov.ua/science_and_defense).  
**3. Walcutt, J.J. & Schatz, S.** (Eds.) (2019). *Modernizing Learning: Building the Future Learning Ecosystem*. Washington, DC: Government Publishing Office. License: Creative Commons Attribution CC BY 4.0 IGO  
**4. Voloshinov S.** *Modern trends for higher education in Ukraine/Engineering and Educational Technologies*, 2018, 6 (4), pp. 38-46. DOI <https://doi.org/10.30929/2307-9770.2018.06.04.04>  
**5.** Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу : Офіційне Інтернет-представництво Президента України <http://www.president.gov.ua>  
**6. M. Moore,** (Ed.). *Handbook of distance education*. Edition 3, Routledge, 2013.  
**7. Гніденко М.П.** Новий підхід до педагогічного процесу в умовах інформатизації / М.П. Гніденко, О.О. Ільїн, О.В. Кліменко // Вісник Державного університету інформаційно-комунікаційних технологій. – К.:ДУІКТ, 2012. – Т.10, №3. – С. 61–68.  
**8. Опар Н.В.** Особливості нормативно-правового забезпечення якості вищої освіти в Україні в умовах євроінтеграції. Теорія та практика державного управління і місцевого самоврядування. Електронне наукове фахове видання. – 2015. – №1. [Електронний ресурс]. – Режим доступу: [http://el-zbirndu.at.ua/index/zmist\\_2015\\_1/0-18](http://el-zbirndu.at.ua/index/zmist_2015_1/0-18)  
**9.** Організація та використання технологій

дистанційного навчання у Збройних Силах України : навч.-метод. посіб. / колектив авторів ; за заг. ред. С. М. Салкуцана. – К. : НУОУ, 2017. – 124 с. **10.** Салкуцан С.М. Стан системи дистанційного навчання Збройних Сил України та погляди на її подальший розвиток / С.М. Салкуцан, М.Г. Тищенко, С.Ю. Гогоняц // Матеріали II Міжнародної науково-практичної конференції “Проблеми впровадження дистанційного навчання в освітньому процесі вищих військових навчальних закладів та можливі шляхи їх вирішення”. – К.: НУОУ. – 2019. – С. 170-173. **11.** Обґрунтування рекомендацій щодо удосконалення системи дистанційного навчання Збройних Сил України: звіт про НДР (остат.) / НУОУ; кер. С.М.Салкуцан; викон.: С. Ю. Гогоняц [та ін.]. шифр “Адель”. №0018u005049..К. : НУОУ. – 2019. – 185 с. **12.** Дистанційний навчальний процес : навчальний посібник [за ред. В. Ю. Бикова та В. М. Кухаренка]. – К. : Міленіум, 2005. – 292 с. **13. Ленков С.В.,** Гахович С.В., Гунченко Ю.О., Лукін В.С., Шворов С.А. Побудова та використання систем дистанційного навчання з елементами штучного інтелекту: Монографія. – Одеса, Вид-во ВМВ, 2014. – 324 с. **14.** Об’єктно-орієнтоване програмування: лабораторний практикум. Уклад.: О.В. Коба, С.В. Пустова. – К.: НАУ, 2011. – 76 с.

## **МЕТОДИКА ОБРАБОТКИ ЭКСПЕРТНЫХ ДАННЫХ ДЛЯ УСОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В ВООРУЖЕННЫХ СИЛАХ УКРАИНЫ**

*Юрий Васильевич Кравченко (доктор технических наук, профессор)*

*Андрей Петрович Мусиенко (доктор технических наук)*

*Максим Георгиевич Тищенко (кандидат технических наук)*

*Спартак Юрьевич Гогоняц (кандидат военных наук, с.н.с.)*

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

*В работе было проведено классификацию средств автоматизации образовательного процесса в системе военного образования. На основе проведенного анализа было определено, что одним из важных факторов эффективного функционирования системы дистанционного обучения является наличие экспертов, которые контролируют качество дистанционных курсов и предлагают методы их совершенствования. С целью разработки механизма работы экспертов по оцениванию эффективности и качества курсов дистанционного обучения была предложена методика осуществления коллективной экспертизы эффективности и качества курсов дистанционного обучения и обработки полученных экспертных данных в группе экспертов. Алгоритм расчетов с использованием предложенной методики предполагает определение профессионального уровня экспертов; обработки значений показателей, определенных экспертами; определение обобщенного значения определенного показателя; определение значения обобщенного показателя.*

*Ключевые слова:* дистанционное обучение; экспертная оценка; информационные технологии; военное образование.

## **THE EXPERT DATA PROCESSING METHOD FOR THE DISTANCE LEARNING SYSTEM IMPROVEMENT IN THE ARMED FORCES OF UKRAINE**

*Yurii Kravchenko (Doctor of Technical Sciences, Professor)*

*Andrii Musienko (Doctor of Technical Sciences)*

*Maksym Tyshchenko (Candidate of Technical Sciences)*

*Spatak Hohoniants (Candidate of Military Sciences, Senior Research Fellow)*

*The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine*

*The classification of educational process automation tools in the military education system was carried out in the paper. Based on the analysis, it was determined that one of the important factors in the effective functioning of the distance learning system is the availability of experts who monitor the quality of distance learning courses and offer methods for improving them. The method for conducting the collective examination of the effectiveness and quality of distance learning courses and processing the received expert data in an expert group was proposed in order to develop the mechanism for experts to assess the effectiveness and quality of distance learning courses. The calculation algorithm of the proposed method involves determining the professional level of experts; processing the values of indicators determined by experts; determination of the generalized value of a particular indicator; determination of the value of a generalized indicator.*

**Key words:** distance learning; expert review; information technology; military education.

### References

1. **Jacob W.** (2015), Interdisciplinary trends in higher education, Palgrave Communications, Vol. 1, URL: <https://www.nature.com/articles/palcomms20151>.
2. Concept of creating a distance learning system in the Armed Forces of Ukraine, Access mode: [www.mil.gov.ua/science\\_and\\_defense](http://www.mil.gov.ua/science_and_defense)
3. **Walcutt, J.J. & Schatz, S.** (Eds.) (2019). Modernizing Learning: Building the Future Learning Ecosystem. Washington, DC: Government Publishing Office. License: Creative Commons Attribution CC BY 4.0 IGO
4. **Voloshinov S.** (2018), Modern trends for higher education in Ukraine/Engineering and Educational Technologies, 6 (4), pp. 38-46. DOI <https://doi.org/10.30929/2307-9770.2018.06.04.04>
5. Doctrine of Information Security of Ukraine, approved by the Decree of the President of Ukraine № 514/2009 08.07.2009 Access mode: <http://www.president.gov.ua>
6. **M. Moore**, (Ed.). Handbook of distance education. Edition 3, Routledge, 2013.
7. **Hnidenko M.P.**, (2009), A new approach to the pedagogical process in the context of informatization, Bulletin of the State University of Information and Communication Technologies, Kyiv, pp 61-68.
8. **Opar N.** (2015), Features of legal and regulatory quality assurance of higher education in Ukraine in the context of European integration. The theory and practice of public administration and local self-government. Electronic scientific professional publication №1.
9. **Salkutsan S.M.** (2017), Organization and use of distance learning technologies in the Armed Forces of Ukraine, Training manual 124 p.
10. **Salkutsan S.M.** (2019), Status of the distance learning system of the Armed Forces of Ukraine and views on its further development, Proceedings of the Second International Scientific and Practical Conference "Problems of implementation of distance learning in the educational process of higher military educational Institutions and possible ways to solve it", Kyiv, pp. 170-173.
11. **Salkutsan S.M.** (2019), Substantiation of Recommendations for Improving the Distance Learning System of the Armed Forces of Ukraine: R&D Report, code "Adele", 185 p.
12. **Bykov V.**, Kukhareno V. (2005) Distance Learning Process: Tutorial, 292 p.
13. **Lienkov S.V.**, Hakhovych S.V., Hunchenko Yu.O., Lukin V.Y., Shvorov S.A. (2014), Construction and use of distance learning systems with elements of artificial intelligence: Monograph, 324 p.
14. **Koba O.**, Pustova C. (2011), Object-Oriented Programming: Laboratory Workshop, 76 p.

*Олександр Йосипович Мацько (кандидат військових наук, професор)*  
*Владислав Григорович Солонніков (доктор технічних наук, професор)*  
*Сергій Миколайович Костюченко*

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

## **ЗАСТОСУВАННЯ МОДЕЛІ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ТЕХНІКИ З ПОЧАСОВОЮ НАДМІРНІСТЮ ДЛЯ ПІДВИЩЕННЯ ЇЇ НАДІЙНОСТІ В ХОДІ ВИКОНАННЯ ЗАВДАНЬ ПІДРОЗДІЛАМИ ІНЖЕНЕРНИХ ВІЙСЬК ЗС УКРАЇНИ ПРИ ПРОВЕДЕННІ ОПЕРАЦІЇ ОБ'ЄДНАНИХ СИЛ**

*В статті засобами теорії почасового резервування обґрунтована доцільність використання планових простоїв інженерної техніки для профілактичного технічного обслуговування і поточного ремонту з метою підтримки її надійності на необхідному рівні. Для кількісної оцінки впливу процесу організації функціонування системи ТО у відповідності до запропонованої моделі на зміну рівня надійності інженерної техніки розроблена методика розрахунку коефіцієнту технічного використання МІО, яка враховує не ідеалізовані, а реальні можливості щодо використання щодобових простоїв техніки в якості резервного часу для підвищення коефіцієнту її технічного використання.*

**Ключові слова:** Система технічного обслуговування, коефіцієнт технічного використання, почасове резервування, напівмарківські процеси, простої техніки.

### **Вступ**

Багатовікова історія війн та збройних конфліктів свідчить про те, що успіху у боротьбі, як правило, досягали війська, які були добре озброєні та технічно і матеріально забезпечені. Тому, якщо говорити про озброєння і військову техніку, треба зазначити, що в усі часи до якості, а точніше до їх тактико-технічних характеристик (ТТХ), завжди висувалися надзвичайно високі і жорсткі вимоги. Вони стосувалися як ефективності бойового застосування озброєння і військової техніки, так і всіх аспектів їх надійності, тобто здатності зберігати свої бойові характеристики в часі в визначених умовах експлуатації.

Переходячи до предмету нашого обговорення, тобто питання забезпечення виконання завдань підрозділами інженерних військ Збройних Сил України при проведенні операції об'єднаних сил (ООС), треба констатувати, що до складу цих підрозділів входить техніка, яка знаходиться на експлуатації понад 20–25 років і за своїм станом потребує значних робіт з відновлення технічної придатності та проведення регламентованого технічного обслуговування. Під час приведення озброєння і військової техніки (ОВТ) до застосування фактичний рівень справності інженерної техніки виявився майже критичним [1]. Такі показники надійності цієї техніки як безвідмовність, довговічність, збереженість та ремонтпридатність, враховуючи загальні (вікові) терміни їх знаходження на експлуатації, вже не відповідали паспортним значенням цих характеристик на момент прийняття їх на озброєння.

**Постановка проблеми.** В зв'язку з очевидною неможливістю забезпечити потрібну надійність

зразків інженерної техніки за рахунок підвищення безвідмовності її елементів (елементну базу і технологію виготовлення елементів ми змінити не в змозі) гарантований позитивний результат застосування машин інженерного озброєння (МІО) в умовах, що склалися, може бути реалізованим лише при раціональних режимах використання інженерної техніки за призначенням з обов'язковим врахуванням всіх особливостей поставлених завдань та впровадженні оптимальної системи технічного обслуговування та ремонту МІО. Тільки завдяки впровадженню таких заходів можливе підтримання інженерної техніки в стані готовності до використання за призначенням та забезпечення її надійності на працездатному рівні.

**Аналіз остатніх досліджень і публікацій.** Вирішення цієї проблеми стикається із суттєвими труднощами як теоретичного, так і практичного характеру. В роботах [2,3,5,6] зазначалося, що одним з перспективних шляхів підвищення надійності МІО є виявлення в алгоритмах їх функціонування резервів часу (почасової надмірності) та врахування і використання останніх при проведенні технічного обслуговування та ремонту МІО під час технологічних простоїв чи простоїв, обумовлених порядком використання техніки за призначенням (розпорядком дня).

Аналіз експлуатації інженерної техніки при проведенні АТО та ООС свідчить про те, що процес використання МІО за призначенням носить систематичний, періодичний (щодобовий) характер, при цьому етап безпосереднього застосування інженерної техніки, який, як правило, припадає на світлу частину доби,

змінюється теж щодобово етапом її простою в нічний час. Наявність в алгоритмі експлуатації МІО етапів простою техніки, обумовлених суворо детермінованим щодобовим використанням МІО за призначенням, дозволяє умовно розглядати їх як системи неперервного використання з фіксованою щодобовою (тобто систематично відновлюваною) почасовою надмірністю (резервом часу), яку можна використовувати для діагностування зразків інженерної техніки, проведення робіт їх технічного обслуговування та відновлювання.

В зв'язку з цим, спираючись на рекомендації теорії почасового резервування, доцільно щодобовий час простою техніки розглядати як систематично поповнювану почасову надмірність організаційного змісту і використовувати її для проведення планових робіт ТО і відновлювання МІО. Але оскільки щодобовий час невикористання техніки за призначенням у відповідності з розпорядком денним, як правило, припадає на вечірні і нічні часи, які в першу чергу повинні використовуватися для повноцінного відпочинку особового складу, в тому числі і ремонтного підрозділу, то зрозуміло, що період невикористання МІО за призначенням в повному обсязі не може бути задіяний як резервний час для проведення ТО та виконання відновлювальних робіт. Тому для практичної реалізації виявленої почасової надмірності пропонується перенести лише частину робочого часу ремонтного підрозділу (2,0-2,5 години) на періоди простою МІО. Це дозволить суттєво підвищити як часткові, так і комплексні показники надійності функціонування зразків інженерної техніки. Але, як зазначається в [4], реальне підвищення надійності МІО при використанні часу простою техніки для її ТО і ремонту буде дещо меншим ніж його значення, отримане з допомогою розрахунків відповідно до теорії почасового резервування. Справа полягає в тому, що відповідно до класичного варіанту теорії почасової надмірності наявний резерв часу вступає в дію відразу з моменту фіксації відмови об'єкту чи з моменту початку часу ТО відповідно до встановленої періодичності його проведення. Що ж стосується реальної ситуації використання інженерної техніки в АТО та ООС, то треба зазначити, що у випадку, коли відмова припадає на період функціонування МІО вона враз зупиняє час використання техніки за призначенням і з цього моменту починається відлік часу, що характеризує непрацездатний стан МІО. Це означає, що миттєве використання щодобового резерву часу неможливе. Використання резервного часу для проведення технічного обслуговування МІО стає припустимим лише з моменту завершення визначеного розпорядком денним робочого часу. Тільки з цього моменту час простою техніки можна розглядати за умовами розглянутої теорії як резервний час. Аналізуючи ситуацію, яка складається в такому випадку, приходимо до висновку, що проміжок часу від відмови до закінчення робочого дня або від відмови до закінчення ремонту (якщо відновлення об'єкту почнеться і завершиться до кінця робочого часу) буде збільшувати загальний

час непрацездатного стану МІО і негативно впливати на значення комплексного коефіцієнту надійності даного зразка інженерного озброєння.

**Мета статті.** У зв'язку з цим як з теоретичної точки зору, так і з чисто практичних міркувань можна вважати за доцільне спробувати вдосконалити методику застосування теорії почасового резервування [5,6,7] в напрямку підвищення точності розрахунку часткових і комплексних показників надійності МІО шляхом врахування конкретного часу затримання моменту вступу в дію щодобового резерву часу на проведення поточного ремонту. В разі вирішення цього завдання стане можливим оцінити рівень підвищення надійності техніки не тільки за рахунок використання теорії почасової надмірності в цілому, але й безпосередньо враховувати як саме затримка надання часового резерву (час доставки зразка озброєння до ремонтного підрозділу або час простою у черзі на ремонт) впливає на зниження значення комплексного коефіцієнту надійності зразків інженерного озброєння в конкретних умовах обстановки, що характеризуються різними режимами планового використання за призначенням та технічного обслуговування, і забезпечити завдяки цьому більш повну оцінку реального стану його надійності.

### Виклад основного матеріалу дослідження

З метою розв'язання сформульованого завдання розглянемо дві математичні моделі періодичного технічного обслуговування зразка інженерного озброєння, що можна умовно віднести до систем неперервного використання. Обидві моделі являють собою систему обслуговування з щодобово поповнюваним резервом часу, в яких об'єкт обслуговування поданий одним структурним елементом, напрацювання якого на відмову – випадкова величина  $t_n$ , закон розподілення якої може бути поданий експоненціальною залежністю  $F(t) = 1 - \exp(-\lambda t)$ , де  $\lambda$  – інтенсивність відмов техніки. В системі передбачено проведення двох видів відновлювальних робіт: періодичного технічного обслуговування (ТО), яке проводиться з періодичністю  $T_{TO}$ , і аварійно-профілактичних (поточних) ремонтів. Тривалість проведення ТО –  $t_{TO}$  є випадковою величиною з функцією розподілення  $\Phi(t) = 1 - \exp(-\theta t)$  та значенням МОЧ  $\bar{t}_{TO}$ , де  $\theta$  – інтенсивність проведення ТО. У випадку відмови техніки в системі передбачено виконання поточного ремонту, тривалість якого  $t_B$  – випадкова величина з функцією розподілу  $F_B(t) = 1 - \exp(-\mu t)$  і кінцевим значенням МОЧ  $\bar{t}_B$  та  $\mu$  – інтенсивності відновлювання техніки. В системі передбачені резерви часу:  $\tau_{Д1}$  на проведення ТО і  $\tau_{Д}$  – на проведення поточного ремонту техніки. Величини  $\tau_{Д1}$  і  $\tau_{Д}$  є випадковими з функціями розподілу

$D_1(t) = 1 - \exp(-\gamma_1 t)$ ;  $D(t) = 1 - \exp(-\gamma t)$  і кінцевими значеннями МОЧ  $\bar{t}_{D1}$  і  $\bar{t}_D$  відповідно, де  $\gamma_1$  і  $\gamma$  – інтенсивності надання резервів часу  $\tau_{D1}$  і  $\tau_D$  відповідно.

Перша з моделей, що розглядаються, – ідеалізована і функціонує у суворій відповідності до класичного варіанту теорії почасового резервування. Це означає, що у випадку, коли до визначеного моменту  $t_{TO}$  техніка не відмовила, то відразу саме з цього моменту розпочинаються роботи, що входять до складу планового ТО. З цього ж моменту починається також відлік резервного часу, що передбачений на проведення ТО. При умові, що час проведення ТО не перевищує  $\tau_{D1}$ , тобто  $t_{TO} \leq \tau_{D1}$ , його відносять до корисного часу функціонування системи, в протилежному випадку – до непрацездатного стану. Крім того при виникненні відмови техніки миттєво починається проведення її ремонту і також починає спливати резервний час, що передбачений на його проведення. При виконанні умови  $t_B \leq \tau_D$  час відновлення техніки відносять до її працездатного стану, в іншому випадку – до непрацездатного.

При побудові другої моделі враховуються реальні можливості щодо використання системою резерву часу, який формується з врахуванням затвердженого плану застосування техніки за призначенням, діючого у військовій частині розпорядку дня та реальних можливостей ремонтного підрозділу щодо негайного початку відновлювальних робіт. Порядок використання часового резерву при проведенні планових ТО для другої моделі прийнятий такий, як і для першої. Тобто наявний резерв часу вступає в дію відразу з моменту планового початку робіт ТО відповідно до встановленої періодичності його проведення. Обґрунтування правомірності такої регламентації почасового резервування обумовлюється відповідністю реальних умов функціонування інженерної техніки вихідним теоретичним передумовам. Законність використання часу простою МІО при відсутності планових роботах як резервного часу для проведення ТО не викликає ніяких заперечень. Дійсно, якщо навіть час проведення чергових робіт ТО припадає на період використання МІО за призначенням, то зрозуміло, що можна без будь-яких ускладнень (без зупинення цих робіт) дочекатися наступного періоду простою техніки (завершення терміну використання техніки за призначенням на поточний день) і після цього приступати до виконання необхідних робіт ТО. Запропонована незначна затримка в початку виконання робіт ТО практично не вплине на ефективність його проведення і не позначиться на рівні надійності МІО (навіть при значному відхиленні (на 20%) в бік збільшення або зменшення від оптимального значення часу періодичності обслуговування коефіцієнт технічного використання  $K_{ТВ}$  зменшується порівняно із своїм максимальним значенням не більше як на декілька відсотків)[6].

Тобто зсув у часі використання резерву часу (початку виконання робіт ТО) не порушує загальних принципів застосування розглянутих теоретичних положень і дозволяє скористатися викладеними вище результатами щодо можливості підвищення надійності МІО шляхом використання часу простою МІО для їх технічного обслуговування.

Що ж стосується виконання робіт поточного ремонту техніки то теж передбачається можливість використання резерву часу  $\tau_D$ . Але для другого варіанту моделі системи ТО в цьому випадку відмова враз зупиняє час використання техніки за призначенням і починається відлік часу, що характеризує непрацездатний стан МІО. При цьому миттєве використання щодобового резерву часу неможливе. Час непрацездатного стану МІО буде тривати аж до моменту завершення визначеного розпорядком дня робочого часу і відсутності черги на виконання ремонтних робіт. Тільки з цього моменту час простою техніки можна розглядати за умовами функціонування другої моделі як резервний час. Якщо відновлення працездатності техніки відбудеться протягом резервного часу  $\tau_D$ , то цей часовий інтервал, на протязі якого відбувалося відновлювання зразка озброєння, будемо відносити до часу знаходження МІО у працездатному стані. При невиконанні умови  $t_B \leq \tau_D$ , тобто при перевищенні часу ремонту техніки наявного резерву часу, продовжується відлік непрацездатного стану техніки. Аналізуючи ситуацію, яка складається в такому випадку, приходимо до висновку, що проміжок часу від відмови до закінчення робочого дня або від відмови до закінчення ремонту (якщо відновлення об'єкту завершиться до кінця робочого часу) буде збільшувати загальний час непрацездатного стану МІО і негативно впливати на значення комплексного коефіцієнту надійності даного зразка інженерного озброєння.

Для математичного підтвердження вище викладеного представимо процес функціонування розглянутих моделей системи ТО шляхом застосування математичного апарату напівмарківських процесів (НМП) і з їх допомогою розрахуємо значення показників надійності МІО в процесі їх експлуатації у відповідності з умовами функціонування цих моделей. Порівняння результатів проведених розрахунків зможе дати кількісну оцінку доцільності використання запропонованої (другої) моделі функціонування системи ТО інженерної техніки як більш адекватної реальним умовам функціонування відносно першої моделі – ідеалізованого варіанту системи ТО з почасовою надмірністю. Математичний апарат НМП дозволяє здійснити визначення показників надійності через визначення часу перебування процесу функціонування системи у фіксованій підмножині станів. У відповідності до методики застосування НМП [7] процес функціонування системи ТО інженерної техніки може бути описаний НМП  $X(t)$ , графі станів і переходів якого щодо першої

та другої розглянутих моделей наведені на рис.1 та рис.2 відповідно.

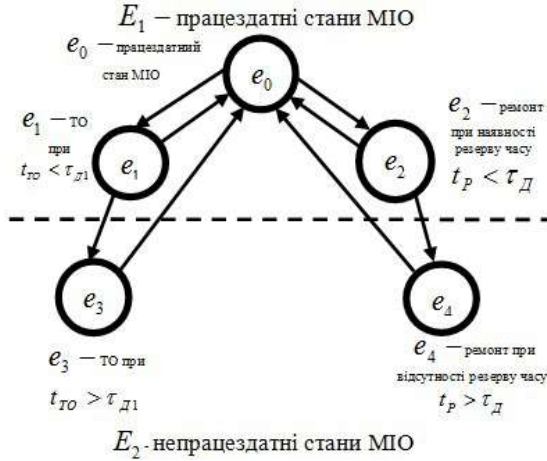


Рис. 1. Граф стану і переходів щодо першої моделі

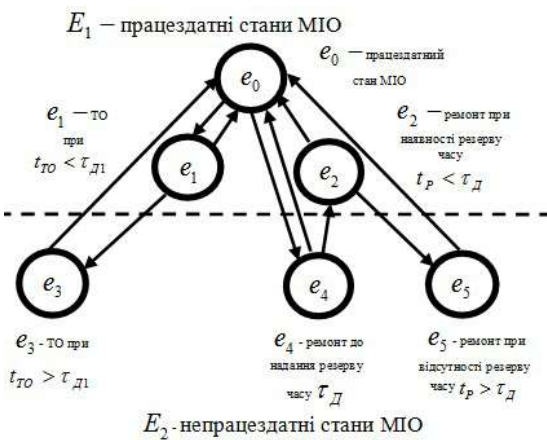


Рис. 2. Граф стану і переходів щодо другої моделі

Як слідує з рис.1, система ТО у відповідності з першою моделлю функціонування в довільний момент часу може знаходитися в одному з наступних станів:  $e_0$  – стан, в якому об’єкт обслуговування працездатний;  $e_1$  – стан, під час перебування в якому на об’єкті проводиться ТО за передбачений резервний час  $\tau_{D1}$ ;  $e_2$  – стан, в якому відбувається відновлення працездатності об’єкту обслуговування за передбачений час резерву  $\tau_D$ ;  $e_3$  та  $e_4$  – стани, в яких на об’єкті проводяться відповідно ТО і поточний ремонт після закінчення резервів часу  $\tau_{D1}$  і  $\tau_D$ ;  $E_+$ ,  $E_-$  – області працездатних і непрацездатних станів об’єкту системи ТО відповідно.

Рівень надійності функціонування МІО будемо оцінювати з використанням комплексного показника надійності, в якості якого доцільно [5] вибрати коефіцієнт технічного використання  $K_{ТВ}$ . Коефіцієнт технічного використання  $K_{ТВ}$  обчислюється як відношення математичного очікування сумарного часу  $T_{E+}$  перебування об’єкту обслуговування в працездатному стані за деякий період експлуатації до математичного очікування сумарного часу перебування об’єкту в непрацездатному стані і

простоїв, обумовлених ТО і ремонтом за той же період часу ( $T_{E+} + T_{E-}$ ).

$$K_{ТВ}(\tau_D) = M[T_{E+}] / M[T_{E+} + T_{E-}], \quad (1)$$

де:  $M[x]$  – математичне очікування випадкової величини  $x$ .

Формула (1) з урахуванням графу станів і переходів (рис.1) приймає вигляд:

$$K_{ТВ}(\tau_D) = \sum_{i=0}^2 \pi_i a_i / \sum_{i=0}^4 \pi_i a_i, \quad (2)$$

де:  $\pi_i$  – стаціонарні імовірності вкладеного ланцюгу Маркова, які визначаються з системи рівнянь

$$\pi_i = \sum_{j \in E} P_{ji} \pi_j, \quad (3)$$

з урахуванням умови нормування  $\sum_{i \in E} \pi_i = 1$ .

Стаціонарні імовірності вкладеного ланцюгу Маркова  $\pi_i$  ( $i = 0, 1, 2, 3, 4$ ), які входять до формули (2), визначимо із наведеної нижче системи рівнянь, отриманої у відповідності до виразу (3) і з урахуванням графу станів і переходів першої моделі системи ТО і ремонту МІО із двох, що розглядаються (рис. 1).

$$\begin{aligned} \pi_0 &= \pi_1 P_{10} + \pi_2 P_{20} + \pi_3 P_{30} + \pi_4 P_{40}; \\ \pi_1 &= \pi_0 P_{01}; \\ \pi_2 &= \pi_0 P_{02}; \\ \pi_3 &= \pi_1 P_{13}; \\ \pi_4 &= \pi_2 P_{24}. \end{aligned} \quad (4)$$

Враховуючи вихідні умови функціонування системи ТО і поточного ремонту відповідно до першої моделі, можна записати наступні розрахункові формули для стаціонарних ймовірностей  $P_{ji}$  і середніх інтервалів часу перебування  $a_i$  в станах  $i$ .

$$\begin{aligned} a_0 &= \frac{1}{\lambda} [1 - \exp(-\lambda T_{ТО})]; \quad a_1 = \frac{1}{\theta + \gamma_1}; \quad a_2 = \frac{1}{\mu + \gamma}; \\ a_3 &= \frac{1}{\theta}; \quad a_4 = \frac{1}{\mu}; \quad P_{01} = \exp(-\lambda T_{ТО}); \end{aligned} \quad (5)$$

$$P_{02} = 1 - \exp(-\lambda T_{ТО}); \quad P_{13} = \frac{\gamma_1}{\gamma_1 + \theta}; \quad P_{24} = \frac{\gamma}{\gamma + \mu}.$$

Розв’язуючи систему рівнянь (4) і підставляючи знайдені значення  $\pi_i$  в (2), після нескладних математичних перетворень отримаємо проміжний вираз для  $K_{ТВ}(\tau_D)$ :

$$K_{ТВ}(\tau_D) = \frac{a_0 + a_1 P_{01} + a_2 P_{02}}{a_0 + a_1 P_{01} + a_2 P_{02} + a_3 P_{01} P_{13} + a_4 P_{02} P_{24}}. \quad (6)$$

Підставляючи в (6) значення для  $a_i$  і  $P_{ji}$ , після низки перетворень і спрощень отримаємо остаточне розрахункове співвідношення для коефіцієнту технічного використання

$$K_{ТВ}(\tau_D) = \frac{\frac{1}{\lambda} + \frac{1}{\mu + \gamma} + e^{-\lambda T_{ТО}} \left[ \frac{1}{\lambda} + \frac{1}{\theta + \gamma_1} - \frac{1}{\mu + \gamma} \right]}{\frac{1}{\lambda} + \frac{1}{\mu + \gamma} + A + e^{-\lambda T_{ТО}} \left[ -\frac{1}{\lambda} + \frac{1}{\theta + \gamma_1} - \frac{1}{\mu + \gamma} + B - A \right]} \quad ..(7)$$

$$\text{де: } A = \frac{\gamma}{\mu(\gamma + \mu)}; B = \frac{\gamma_1}{\theta(\gamma_1 + \theta)}. \quad (8)$$

Для другої моделі функціонування системи ТО і відновлювання МІО (рис. 2), зазначимо, що в цьому випадку об'єкт обслуговування (МІО) може знаходитися у наступних станах:  $e_0$  – стан, в якому об'єкт працездатний;  $e_1$  і  $e_2$  – стани, в яких на об'єкті проводиться планове ТО або виконуються відновлювальні роботи на протязі наперед заданих резервів часу  $\tau_{Д1}$  і  $\tau_{Д}$  відповідно;  $e_3$  і  $e_5$  – стани, на яких відповідно проводяться ТО і роботи по відновленню працездатності після закінчення резервів часу  $\tau_{Д1}$  і  $\tau_{Д}$ ;  $e_4$  – стан, під час якого об'єкт непрацездатний, на ньому можуть проводитися або не проводитися ремонтні роботи, але використання часового резерву  $\tau_{Д}$  ще не можливо, тому що ще не сплив щодобовий час використання техніки за призначенням. Тобто відповідно до графу станів і переходів другої моделі системи (рис. 2) коефіцієнт технічного використання може бути поданий наступним чином

$$K_{ТВ}(\tau_{Д}) = \frac{\sum_{i=0}^2 \pi_i a_i}{\sum_{i=0}^5 \pi_i a_i} \quad (9)$$

Розмірковуючи аналогічно як і при розгляді першої моделі функціонування системи ТО і ремонту МІО, можна отримати систему рівнянь

$$\left. \begin{aligned} \pi_0 &= \pi_1 P_{10} + \pi_2 P_{20} + \pi_3 P_{30} + \pi_4 P_{40} + \pi_5 P_{50} \\ \pi_1 &= \pi_0 P_{01} \\ \pi_2 &= \pi_4 P_{42} \\ \pi_3 &= \pi_1 P_{13} \\ \pi_4 &= \pi_0 P_{04} \\ \pi_5 &= \pi_2 P_{25} \end{aligned} \right\} \quad (10)$$

Розв'язання цієї системи рівнянь відносно  $\pi_i$  дає можливість записати формулу (9) у вигляді

$$K_{ТВ}(\tau_{Д}) = \frac{a_0 + a_1 P_{01} + a_2 P_{04} P_{42}}{a_0 + a_1 P_{01} + a_2 P_{04} P_{42} + a_3 P_{01} P_{13} + a_4 P_{04} + a_5 P_{04} P_{25}} \quad (11)$$

Очевидно, що для другої моделі розрахункові формули стаціонарних ймовірностей  $P_{ji}$  і середніх інтервалів часу  $a_i$  перебування процесу в різних станах з врахуванням вихідних умов функціонування моделі можуть бути подані наступними виразами

$$\begin{aligned} a_0 &= \frac{1}{\lambda} [1 - \exp(-\lambda T_{ТО})]; a_1 = \frac{1}{\theta + \gamma_1}; a_2 = \frac{1}{\mu + \gamma}; \\ a_3 &= \frac{1}{\theta}; a_4 = \frac{1}{\mu}; a_5 = \frac{1}{\mu}; \quad (12) \\ P_{01} &= \exp(-\lambda T_{ТО}); P_{04} = 1 - \exp(-\lambda T_{ТО}); \\ P_{13} &= \frac{\gamma_1}{\gamma_1 + \theta}; P_{25} = \frac{\gamma}{\gamma + \mu}; P_{42} = \frac{\mu}{\gamma + \mu}. \end{aligned}$$

Тому не складно довести, що після очевидних математичних перетворень розрахункові формули для коефіцієнту технічного використання МІО другої моделі функціонування системи будуть

мати наступний вигляд:

$$K_{ТВ}(\tau_{Д}) = \frac{\frac{1}{\lambda} + \frac{1}{\gamma + \mu} * C + e^{-\lambda T_{ТО}} \left[ -\frac{1}{\lambda} + \frac{1}{\gamma_1 + \theta} - \frac{1}{\gamma + \mu} * C \right]}{\frac{1}{\lambda} + \frac{1}{\gamma + \mu} * C + A_1 + e^{-\lambda T_{ТО}} \left[ -\frac{1}{\lambda} + \frac{1}{\gamma_1 + \theta} - \frac{1}{\gamma + \mu} * C + B - A_1 \right]} \quad (13)$$

$$\text{де: } A_1 = \frac{1}{\mu} + A * C; A = \frac{\gamma}{\mu(\gamma + \mu)}; B = \frac{\gamma_1}{\theta(\gamma_1 + \theta)};$$

$$C = \frac{\mu}{\gamma + \mu}. \quad (14)$$

Для дослідження впливу процесу організації роботи системи ТО і ремонту на зміну рівня надійності зразка інженерного озброєння при його обслуговуванні системою ТО і ремонту, що функціонує у відповідності до розглянутих двох різних моделей надання резерву часу, побудуємо графіки коефіцієнтів технічного використання МІО у відповідності до формул (11, 12) і (13, 14), що характеризують особливості використання резервів часу у цих моделях. Для побудови графіків коефіцієнту технічного використання  $K_{ТВ}(\tau_{Д})$  скористаємося системою MATLAB – сучасним засобом автоматизації математичних розрахунків, що побудована на розширеному уявленні і застосуванні матричних операцій [8]. Результати отриманих розрахунків наведені на рис. 3-6.

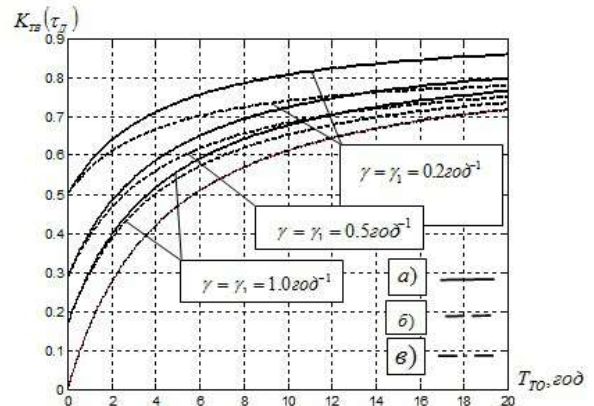


Рис. 3. Залежність  $K_{ТВ}(\tau_{Д})$  МІО при обслуговуванні системою ТО з почасовою надмірністю від  $T_{ТО}$

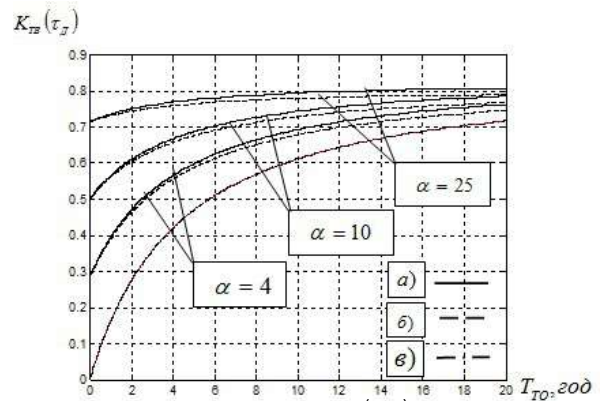


Рис. 4. Залежність  $K_{ТВ}(\tau_{Д})$  МІО при обслуговуванні системою ТО з часовою надмірністю

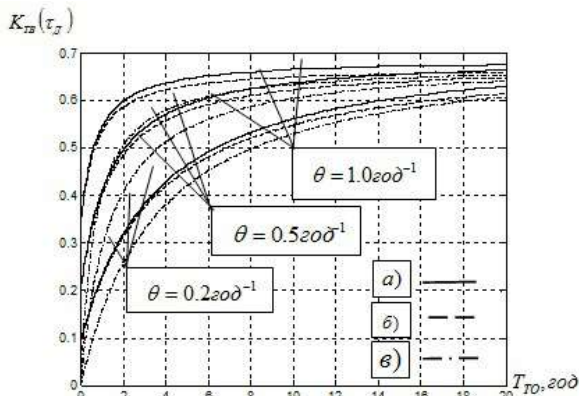


Рис. 5. Залежність  $K_{TB}(\tau_D)$  МІО з врахуванням почасової надмірності від періодичності проведення технічного обслуговування  $T_{TO}$

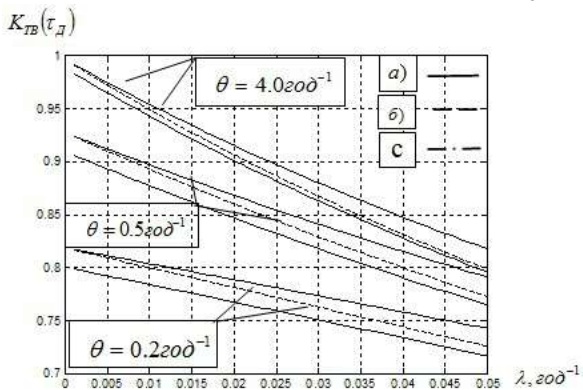


Рис. 6. Залежність екстремальних значень коефіцієнту технічного використання МІО з врахуванням часової надмірності від інтенсивності відмов апаратури

Графіки, зображені на рис. 3, ілюструють залежність коефіцієнту технічного використання  $K_{TB}(\tau_D)$  МІО при обслуговуванні системою ТО з почасовою надмірністю від періодичності проведення планових попереджувальних профілактик  $T_{TO}$  для випадку, коли напрацювання елемента між відмовами розподілене за експоненціальним законом  $F(t) = 1 - \exp(-\lambda t)$ , а функції розподілення випадкових величин, що характеризують можливості системи щодо обслуговування техніки, мають наступний вигляд:

$$F_B(t) = 1 - \exp(-\mu t); \quad D(t) = 1 - \exp(-\gamma t);$$

$$D_1(t) = 1 - \exp(-\gamma_1 t); \quad \Phi(t) = 1 - \exp(-\theta t),$$

при значеннях:  $\lambda = 0.05 \text{ год}^{-1}$ ;  $\mu = 0.2 \text{ год}^{-1}$ ;  $\theta = 0.2 \text{ год}^{-1}$ ;  $\gamma = \gamma_1 = 0.2, 0.5, 1.0 \text{ год}^{-1}$ .

Розрахунки проводилися для випадків:

а) коли резерв часу надається безпосередньо в момент відмови об'єкту і відразу розпочинаються ремонтні роботи;

б) коли ремонтні роботи розпочинаються теж після відмови техніки, але резервний час починає використовуватися лише після закінчення щодобового часу використання техніки за призначенням.

в) при відсутності резерву часу на проведення технічного обслуговування.

На рис. 4 відображена залежність коефіцієнту технічного використання  $K_{TB}(\tau_D)$  МІО при обслуговуванні системою ТО з часовою надмірністю від періодичності проведення технічного обслуговування  $T_{TO}$  при різних значеннях  $\alpha = \gamma/\gamma_1$  – параметрів експоненціального розподілення випадкових величин  $\tau_D$  і  $\tau_{D1}$  і значеннях  $\lambda = 0.05 \text{ год}^{-1}$ ;  $\mu = \theta = 0.2 \text{ год}^{-1}$ ;  $\gamma = 2 \text{ год}^{-1}$ .

На рис. 5 показані залежності коефіцієнту технічного використання  $K_{TB}(\tau_D)$  МІО з врахуванням почасової надмірності від періодичності проведення технічного обслуговування  $T_{TO}$ , інтенсивності його проведення  $\theta = 1/\bar{t}_{TO}$  при напрацюванні елемента між відмовами, розподіленому за експоненціальним законом  $F(t) = 1 - \exp(-\lambda t)$ , і функціями розподілення випадкових величин, що характеризують можливості системи щодо обслуговування техніки, поданими у вигляді:

$$F_B(t) = 1 - \exp(-\mu t); \quad D(t) = 1 - \exp(-\gamma t);$$

$$D_1(t) = 1 - \exp(-\gamma_1 t); \quad \Phi(t) = 1 - \exp(-\theta t)$$

при  $\lambda = 0.05 \text{ год}^{-1}$ ;  $\mu = 0.2 \text{ год}^{-1}$ ;  $\gamma = \gamma_1 = 2 \text{ год}^{-1}$ ;  $\theta = 0.2, 1; 2, 4 \text{ год}^{-1}$ .

На рис. 6 наведені графіки залежності екстремальних значень коефіцієнту технічного використання  $K_{TB}^*(\tau_D)$  МІО з врахуванням часової надмірності від інтенсивності відмов апаратури  $\lambda$  та інтенсивності проведення технічного обслуговування  $\theta$ , які отримані для таких самих вихідних значеннях параметрів, як і при побудові попередніх графіків.

Розрахунки, результати яких наведені на рис. 4-6, проводилися для випадків:

а) коли резерв часу надається безпосередньо в момент відмови об'єкту;

б) коли резерв часу надається тільки після завершення щодобового часу використання інженерної техніки за призначенням.

Аналіз отриманих графіків коефіцієнту технічного використання  $K_{TB}(\tau_D)$  МІО дозволяє зробити наступні висновки:

1. Результати порівняння значень коефіцієнту технічного використання  $K_{TB}(\tau_D)$  інженерної техніки для різних моделей її технічного обслуговування свідчать про те, що системи ТО з почасовою надмірністю (перша і друга моделі) забезпечують суттєве збільшення комплексного показника надійності  $K_{TB}(\tau_D)$  порівняно з із звичайною планово-періодичною системою ТО (рис. 3).

2. Значення коефіцієнту  $K_{TB}(\tau_D)$  МІО при її технічному обслуговуванні за алгоритмом функціонування другої моделі ТО при однакових початкових даних випадкових величин, що входять до розрахункових формул, дещо менше значень цього коефіцієнту, отриманих для першої моделі ТО (рис. 3). Це пояснюється тим, що запропонована модель системи ТО з часовою



надмірністю (друга модель) враховує не ідеалізовані, а реальні можливості щодо використання щодобових простоїв техніки в якості резервного часу для профілактичного технічного обслуговування та поточного ремонту, тобто дозволяє дати більш об'єктивну оцінку реальної надійності МІО.

3. При збільшенні значень резерву часу (зменшенні значень  $\gamma$  і  $\gamma_1$ ) (рис. 4) і збільшенні інтенсивності проведення ТО і поточного ремонту МІО  $\theta$  і  $\mu$  відповідно (рис. 5) величина коефіцієнту технічного використання  $K_{ТВ}(\tau_D)$  зростає як для першої, так і для другої моделей організації робіт системи технічного обслуговування, при цьому, як це вже вище пояснювалося, для першої моделі у всіх випадках його значення залишаються завищеними у порівнянні з реальними.

4. Збільшення інтенсивності проведення технічного обслуговування  $\theta$  призводить до зростання коефіцієнту технічного використання МІО  $K_{ТВ}(\tau_D)$  як функції інтенсивності відмов техніки  $\lambda$ . При цьому залежність  $K_{ТВ}(\tau_D)$  від  $\lambda$  описується лінійною функцією. При  $\lambda \rightarrow 0$  значення коефіцієнту  $K_{ТВ}(\tau_D) \rightarrow 1$ . Відповідно при  $\lambda \rightarrow \infty$  величина коефіцієнту  $K_{ТВ}(\tau_D) \rightarrow 0$ . Тобто підтверджується відомий з практики факт, що ефективність проведення ТО з точки зору його позитивного впливу на коефіцієнт технічного використання тим більший, чим менше його тривалість і простої техніки, пов'язані з його проведенням. Крім того, абсолютний приріст значення коефіцієнту  $K_{ТВ}(\tau_D)$  при збільшенні інтенсивності проведення ТО (рис. 6) зменшується при збільшенні інтенсивності відмов техніки  $\lambda$ . Це пояснюється тим, що несуттєве зростання коефіцієнту  $K_{ТВ}(\tau_D)$  від підвищення інтенсивності  $\theta$  проведення ТО при збільшенні інтенсивності відмов техніки  $\lambda$  в абсолютному вимірі – зменшується.

5. Необхідно звернути увагу на той факт, що при збільшенні значень  $\lambda$  різниця між значеннями коефіцієнту  $K_{ТВ}(\tau_D)$ , розрахованими для першої і другої моделей функціонування системи ТО МІО, суттєво збільшується. Цей факт пояснюється тим, що, як вже зазначалося вище, різниця в значеннях коефіцієнту  $K_{ТВ}(\tau_D)$ , розрахованих для першої і другої моделей функціонування системи ТО, пояснюється необґрунтовано завищеними значеннями резервів часу  $\tau_D$  і  $\tau_{D1}$  при функціонуванні системи ТО у відповідності до першої моделі. Зрозуміло, що при збільшенні інтенсивності відмов об'єкту обслуговування  $\lambda$

(зменшенні часу напрацювання об'єкту на відмову  $\bar{t}_n$ ) відносна вага цієї необґрунтованої частини часового резерву зростає при обчисленні коефіцієнту  $K_{ТВ}(\tau_D)$  у відповідності до першої моделі функціонування системи ТО. Тобто можна стверджувати, що якщо при розрахунку коефіцієнту технічного використання МІО, обслуговування яких відбувається з використанням їх простоїв для проведення ТО, використовується перша модель функціонування системи ТО, то помилка в точності розрахунку  $K_{ТВ}(\tau_D)$  буде тим більша, чим вища інтенсивність відмов об'єкту обслуговування  $\lambda$ .

Таким чином підводячи підсумки викладеному, можна стверджувати, що результати проведеного аналізу впливу різних моделей організації робіт і окремих параметрів системи ТО з почасовою надмірністю на експлуатаційну надійність інженерної техніки підтверджує доцільність проведення організації роботи системи ТО техніки частин і підрозділів інженерних військ, що приймають участь у проведенні ООС на сході нашої країни, відповідно до запропонованої (другої) моделі організації робіт ТО з використанням щодобових простоїв техніки, обумовлених затвердженими планами використання МІО за призначенням та розпорядком денним військової частини.

### Висновки й перспективи подальших досліджень

Підводячи підсумки викладеному, можна стверджувати, що результати проведеного аналізу впливу різних моделей організації робіт і окремих параметрів системи ТО з почасовою надмірністю на експлуатаційну надійність інженерної техніки підтверджує доцільність проведення організації роботи системи ТО техніки частин і підрозділів інженерних військ, що приймають участь у проведенні ООС на сході нашої країни, відповідно до запропонованої (другої) моделі організації робіт ТО з використанням щодобових простоїв техніки, обумовлених затвердженими планами використання МІО за призначенням та розпорядком денним військової частини.

В подальшому планується на основі проведеного дослідження додатково оцінити можливості структурного резервування, а також різних стратегій і параметрів організації і проведення ТО щодо позитивного впливу на комплексний показник надійності МІО – коефіцієнт їх технічного використання. Це, на думку авторів, може забезпечити підтримання необхідного рівня надійності МІО підрозділів інженерних військ Збройних Сил України при проведенні операції об'єднаних сил.

інженерних військ Збройних Сил України у ході виконання завдань у складі міжнародних миротворчих сил. / Колос О.Л. - К. : НАОУ, Труды академії, №4(84), 2008, С. 152-161.  
3. Використання методу почасового резервування для вдосконалення системи технічного обслуговування техніки як один із способів підвищення її надійності в ході виконання завдань підрозділами інженерних військ ЗС України у складі міжнародних миротворчих контингентів /

### Література

1. Солонніков В.Г., Колос О.Л. Підвищення коефіцієнта технічного використання машин інженерного озброєння в особливих умовах експлуатації шляхом розробки математичних моделей технічного обслуговування і відновлення об'єктів з врахуванням почасової та структурної надмірності. Монографія,- Львів: Видавництво "Растр-7", 2017.-168с. 2. Солонніков В.Г. Особливості та проблеми технічного забезпечення частин і підрозділів

[Мальченко С.В., Колос О.Л., Солонніков В.Г., Полякова О.В.] - К. : НАОУ, Труды университета, № 1(91), 2009, С. 121-132. 4. Аналіз відповідності існуючої системи технічного обслуговування озброєння і військової техніки умовам експлуатації техніки інженерних підрозділів Збройних Сил України в ході виконання завдань у складі міжнародних миротворчих сил / Солонніков В.Г., Колос О.Л., Полякова О.В. - К. : НАОУ, Труды академії, №3(90), 2009, С. 157 - 165. 5. Черкесов Г. Н. Надежность технических систем с

временной избыточностью [под ред. А. М. Половко. М. ] / Сов. радио, 1974. – 296 с. 6. Креденсер Б. П. Прогнозирование надежности систем с временной избыточностью. - К. : Наукова думка, 1978. - 240 с. 7. Креденсер Б.П. та ін. Модели технического обслуживания систем с избыточностью – К. : Фенікс, 2002. – 192 с. 8. Дьяконов В.П. MATLAB 6/6.1/6.5 +Simulink в математике и моделировании. Полное руководство пользователя. М.: СОЛОН-Прес. 2003. 576с.

## ПРИМЕНЕНИЕ МОДЕЛИ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ТЕХНИКИ С ВРЕМЕННОЙ ИЗБЫТОЧНОСТЬЮ ДЛЯ ПОВЫШЕНИЯ ЕЕ НАДЕЖНОСТИ В ХОДЕ ВЫПОЛНЕНИЯ ЗАДАЧ ПОДРАЗДЕЛЕНИЯМИ ИНЖЕНЕРНЫХ ВОЙСК ВС УКРАИНЫ ПРИ ПРОВЕДЕНИИ ОПЕРАЦИИ ОБЪЕДИНЕННЫХ СИЛ

*Александр Иосифович Мацько ( кандидат военных наук, профессор )  
Владислав Григорьевич Солонников (доктор технических наук, профессор)  
Сергей Николаевич Костиюченко*

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

*В статье средствами теории временного резервирования обоснована целесообразность использования плановых простоев инженерной техники для профилактического технического обслуживания и текущего ремонта с целью поддержания ее надежности на необходимом уровне. Для количественной оценки влияния процесса организации функционирования системы ТО в соответствии с предложенной моделью на изменение уровня надежности инженерной техники разработана методика расчета коэффициента технического использования МИВ, которая учитывает не идеализированные, а реальные возможности по применению ежесуточных простоев техники в качестве резервного времени для повышения коэффициента ее технического использования.*

*Ключевые слова:* система технического обслуживания, коэффициент технического использования, временное резервирование, полумарковские процессы, простои техники.

## APPLICATION OF THE TECHNICAL SUPPORT MODEL WITH VARIABLE REDUNDANCY TO INCREASE ITS RELIABILITY DURING TASKS BY THE UNITS OF ENGINEERING AIRCRAFT OF UKRAINE WHEN THE JOINT FORCE OPERATIONS ARE PERFORMED

*Oleksandr Matsko (Candidate of military sciences, Professor)  
Vladyslav Solonnikov (Doctor of technical sciences, Professor)  
Serhii Kostiuchenko*

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

*In the article by means of the theory of time reservation the reasonableness of use of planned downtime of engineering equipment for preventive maintenance and current repair in order to maintain its reliability at the required level is substantiated. To quantify the impact of the process of organizing the functioning of the maintenance system in accordance with the proposed model to change the level of reliability of engineering technology developed a method of calculating the coefficient of technical use of engineering machines, which takes into account not idealized, but the real possibilities for the use of daily downtime of the equipment as a reserve time its technical use.*

*Keywords:* maintenance system, coefficient of technical use, temporary reservation, semi-markov processes, downtime of technology

### References

1. Solonnikov V.Gh., Kolos O.L. Pidvyshhennja koeficijenta tekhnichnogo vykorystannja mashyn inzheneremogho ozbrojennja v osoblyvykh umovakh ekspluataciji shljakhom rozrobky matematychnykh modelej tekhnichnogo obslughovuvannja i vidnovljuvannja ob'ektiv z vrakhuvannjam pochasovoji ta strukturnoji nadmimosti. Monografija,- Ljviv: Vydavnytvo "Rastr-7", 2017.-168s. 2. Solonnikov V.Gh. Osoblyvosti ta problemy tekhnichnogo zabezpechennja chastyn i pidrozdiliv inzhenernykh vijsjk Zbrojnykh Syl Ukrainy u khodi vykonannja zavdanj u skladi mizhnarodnykh myrotvorchykh syl. / Kolos O.L. - K. : NAOU, Trudy akademiji, №4(84), 2008, S. 152-161. 3. Vykorystannja metodu pochasovogho rezervuvannja dlja vdoskonalennja systemy tekhnichnogo obslughovuvannja tekhniky jak odyz iz sposobiv pidvyshhennja jiji nadijnosti v khodi vykonannja zavdanj pidrozdilamy inzhenernykh vijsjk ZS Ukrainy u skladi mizhnarodnykh myrotvorchykh kontyngentiv /

[Maljchenko S.V., Kolos O.L., Solonnikov V.Gh., Poljakova O.V.] - K. : NAOU, Trudy universytetu, № 1(91), 2009, S. 121-132. 4. Analiz vidpovidnosti isnujuchoji systemy tekhnichnogo obslughovuvannja ozbrojennja i vijsjkovoji tekhniky umovam ekspluataciji tekhniky inzhenernykh pidrozdiliv Zbrojnykh Syl Ukrainy v khodi vykonannja zavdanj u skladi mizhnarodnykh myrotvorchykh syl / Solonnikov V.Gh., Kolos O.L., Poljakova O.V. - K. : NAOU, Trudy akademiji, №3(90), 2009, S. 157 - 165. 5. Черкесов Г. Н. Надежность технических систем с временной избыточностью [под ред. А. М. Половко. М. ] / Сов. радио, 1974. – 296 с. 6. Креденсер Б. П. Прогнозирование надежности систем с временной избыточностью. - К. : Наукова думка, 1978. - 240 с. 7. Креденсер Б.П. та ін. Модели технического обслуживания систем с избыточностью – К. : Фенікс, 2002. – 192 с. 8. Дьяконов В.П. MATLAB 6/6.1/6.5 Simulink в математике и моделировании. Полное руководство пользователя. М.: СОЛОН-Прес. 2003. 576с.

*Володимир Юрійович Богданович* (доктор технічних наук, професор)<sup>1</sup>

*Олександр Володимирович Дублян* (кандидат військових наук)<sup>1</sup>

*Анатолій Миколайович Сиротенко* (доктор військових наук)<sup>2</sup>

*Олександр Вікторович Передрій* (кандидат військових наук)<sup>1</sup>

*Андрій Миколайович Прима*<sup>1</sup>

<sup>1</sup>Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

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

## МЕТОДИКА ПРОГНОЗНОГО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ АСИМЕТРИЧНОГО РЕАГУВАННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ НА ЗАГРОЗИ У ВОЄННІЙ СФЕРІ

Представлена методика прогнозного оцінювання ефективності асиметричної протидії сучасним загрозам в інтересах забезпечення достатнього рівня воєнної безпеки держави. В умовах комплексного використання військових і невійськових інструментів (економічних, політичних, інформаційно-психологічних тощо) виникла потреба в оцінюванні та прогнозуванні ефективності асиметричного застосування військових та невійськових сил і засобів у протидії силовому тиску та застосуванню військової сили проти держави, що протистоїть більш сильному у військовому відношенні противнику.

Основним обмеженням держави, що проводить наступальні дії, є втрати особового складу. Для держави-жертви агресії втрати населення, інфраструктури тощо у такому конфлікті набагато більші. Світовий досвід показує, що значно слабша у військовому відношенні країна, здійснюючи асиметричні заходи протидії загрозам військовими і невійськовими суб'єктами сил оборони, здатна завдати противнику неприйнятної збитку, в т.ч. і в невійськових сферах безпеки, і тим самим примусити навіть більш сильного у воєнному відношенні противника відмовитися від застосування військової сили проти неї.

Пропонується ефективність протидії агресії держави, що значно переважає державу-мішень за військовою «потужністю», оцінювати сумарним рівнем деескалації загрози на певний момент часу за рахунок симетричної (прямої військової) та асиметричної (комплексної) протидії агресії у формі проведення локальної спеціальної операції. Кількість локальних спеціальних операцій визначається можливостями держави-жертви агресії. Сформована система обмежень та визначені критерії прийняття рішення державою-агресором про відмову від подальших агресивних дій.

**Ключові слова:** воєнна безпека; загроза; асиметрична протидія; силовий тиск; військова сила; ефективність протидії; збройний конфлікт; деескалація загрози.

### Вступ

**Постановка проблеми.** Стаття присвячена загальній проблемі забезпечення достатнього рівня воєнної безпеки держави в умовах здійснення проти неї силового тиску або застосування військової сили більш потужною у військовому відношенні державою. Частковим завданням загальної проблеми визначено розроблення методики прогнозного оцінювання ефективності асиметричної протидії сучасним загрозам воєнній безпеці держави.

**Аналіз останніх досліджень і публікацій.** Чинна нормативно-правова база воєнної безпеки України не визначає асиметричну протидію недружнім державам, які вдаються до силового тиску або до застосування воєнної сили проти неї. Так у Законі України «Про національну безпеку України» [1] у загальному плані визначаються шляхи досягнення цілей державної політики у

воєнній сфері, сферах оборони і військового будівництва, але ні симетрична, ні асиметрична протидія не згадуються.

Визначені у законодавчих документах [2-4] шляхи формування національних безпекових та оборонних спроможностей обумовлюють сумісне використання сил і засобів сектору безпеки і оборони (СБОУ). При цьому пріоритет надається невійськовим засобам усунення або нейтралізації загроз національним інтересам. Асиметричні форми використання сил і засобів СБОУ у законодавчих документах не визначені.

У монографії [5] запропонована методика визначення стратегічних завдань суб'єктам системи забезпечення воєнної безпеки щодо нейтралізації загроз воєнного характеру в умовах позаблокового статусу, але варіанти інтеграції

зусиль окремих елементів системи, у тому числі їх асиметричне застосування, не розглянуті.

Принципи інтеграції сил і засобів СБОУ, можливі форми і способи їх сумісного (комплексного) використання детально розглянуті у монографії [6], але питанням їх асиметричного застосування в роботі приділено недостатньо уваги.

**Метою статті** є розроблення методики прогнозного оцінювання ефективності асиметричної протидії загрозам воєнній безпеці держави (далі – Методика)

### Виклад основного матеріалу дослідження

У Воєнній доктрині України [3] однією із головних тенденцій формування та розвитку безпекового середовища у світі визначається перенесення ваги у воєнних конфліктах на асиметричне застосування військової сили не передбаченими законом збройними формуваннями, зміщення акцентів у веденні воєнних конфліктів на комплексне використання військових і невійськових інструментів (економічних, політичних, інформаційно-психологічних тощо), що принципово змінює характер збройної боротьби.

Успішна протидія силовому тиску та застосуванню військової сили проти держави, що протистоїть більш сильному у військовому відношенні противнику, потребує кількісного оцінювання та прогнозування ефективності асиметричного застосування військових та невійськових сил і засобів. Особливу актуальність даної проблеми визначають події на Близькому і Середньому Сході на початку 2020 року.

Для вирішення цих завдань запропонована методика прогнозного оцінювання ефективності асиметричної протидії сучасним загрозам воєнній безпеці держави. Слабша у воєнному відношенні країна, проводячи асиметричні заходи протидії загрозам військовими і невійськовими суб'єктами сил оборони, здатна завдати противнику неприємного збитку, в т.ч. і в невійськових сферах безпеки, і тим самим примусити навіть більш сильного у воєнному відношенні противника відмовитися від застосування військової сили проти неї.

Методика, блок-схема якої наведена на рис.1, є послідовним виконанням визначених процедур щодо аналізу безпекового середовища, моніторингу, оцінювання рівня та характеру загроз воєнного або гібридного характеру, визначення необхідних ресурсів, потрібного часу і рівня деескалації (зниження) загрози та вибору необхідної для цього групи суб'єктів збройних сил і їх потрібних спроможностей для формування потенціалу асиметричної протидії (ПАП).

Суть методики полягає у наступному.

**На етапі № 1** проводиться аналіз безпекового середовища на предмет зародження або існування небезпечних явищ, потенційних та реальних загроз

національним інтересам, в умовах яких держава реалізує свою політику національної безпеки [7]. Здійснюється оцінювання ВПО станом на  $t_1$ . Проводиться моніторинг загроз, під час якого виявляються загрози (небезпеки та інші деструктивні чинники) воєнного або гібридного характеру з боку тих держав, що розглядаються потенційно небезпечними з воєнної точки зору, рис. 2. Результатом моніторингу є множина загроз  $\{z\}$ ,  $z = \overline{1, Z}$  воєнного або гібридного характеру, які можуть істотно вплинути на воєнну безпеку держави (*основними методами виявлення загроз є метод зіставлення та метод експертного оцінювання*).

**На етапі № 2** експертами здійснюється побудова найбільш ймовірного сценарію агресивних дій з боку більш сильної у військовому відношенні держави. Агресивні дії слід очікувати одночасно у військовій, інформаційній, дипломатичній, політичній, гуманітарній та інших сферах. Опис сценарію має бути настільки детальним, щоб можна було сформувати системну модель загрози державі у воєнній сфері та у подальшому провести оцінювання її рівня за допомогою моделі М7 [8].

**На етапі № 3** методом експертного оцінювання здійснюється формування пріоритетного ряду виявлених загроз воєнній безпеці держави, для нейтралізації (усунення) яких необхідно залучення збройних сил  $\{z_{zc}\} = \overline{1, Z_{zc}}$ . Спочатку розглядається найбільш важлива загроза. З використанням методу Ісікави [9] експерти проводять декомпозицію загрози воєнній безпеці держави та визначення пріоритетного ряду факторів  $P_z$  (рис. 3), які формують цю загрозу на момент оцінювання. Цей етап є ключовим для подальшої організації протидії загрозі  $Z$ , оскільки від точності прогнозу рівня воєнної небезпеки та повноти факторів, що її формують, залежатиме результативність усіх подальших дій з нейтралізації цієї загрози [10] (*виявлення факторів, що формують загрозу, здійснюється методом Ісікави та експертним методом, а оцінювання рівнів – з використанням удосконаленого методу аналізу ієрархій (МАІ) та моделі М7 [8]*).

**На етапі № 4** за допомогою удосконаленого МАІ та з використанням комп'ютерної моделі М7 здійснюється експертно-аналітичне оцінювання поточного рівня  $K_{\text{пот } z}(t_1)$  виявленої загрози  $z$ , рис. 4.

Властивістю моделі М7 є те, що вона може оперувати якісними та кількісними показниками одночасно. Також модель дозволяє оперувати 9 факторами формування загроз, по кожному з яких аналізувати до 9-13 показників. Рівень загрози  $K_z(t)$  оцінюється за формулою:

$$K(t)_z = \sum_{i=1}^I \sum_{j=1}^J (L_i \times P_{ij}) / \sum_{i=1}^I \sum_{j=1}^J \max (L_i \times P_{ij}),$$

де  $L_i$  – значення пріоритету  $i$ -го ( $i=1, I$ ) фактора, що впливає на рівень загрози;

$P_{ij}$  – значення пріоритету  $j$ -го ( $j=1, J$ ) показника  $i$ -го фактора, що впливає на рівень загрози.

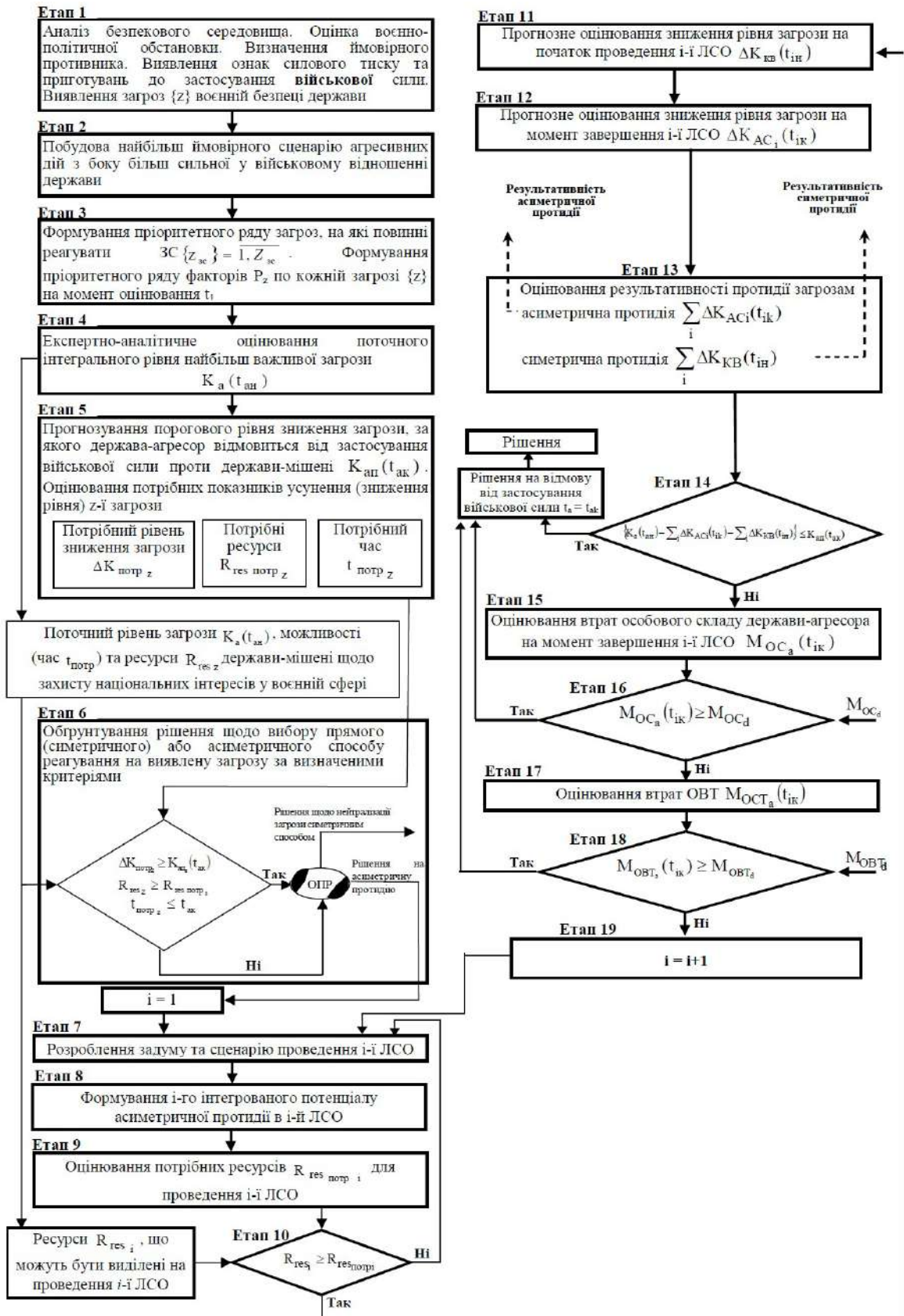


Рис. 1. Блок-схема методики прогнозного оцінювання результативності асиметричної протидії загрозам воєнній безпеці держави



Рис. 2. Узагальнена схема моніторингу загроз воєнній безпеці держави

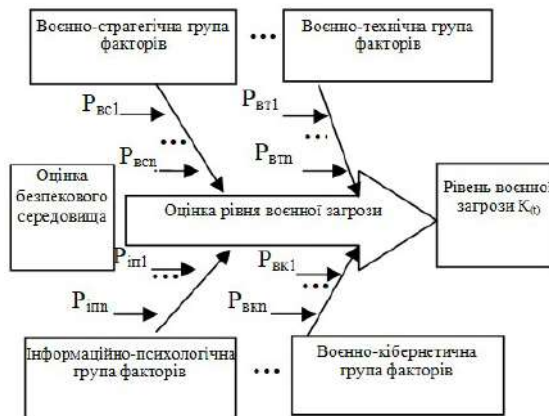


Рис. 3. Приклад декомпозиції загроз воєнній безпеці держави з використанням методу Іскави

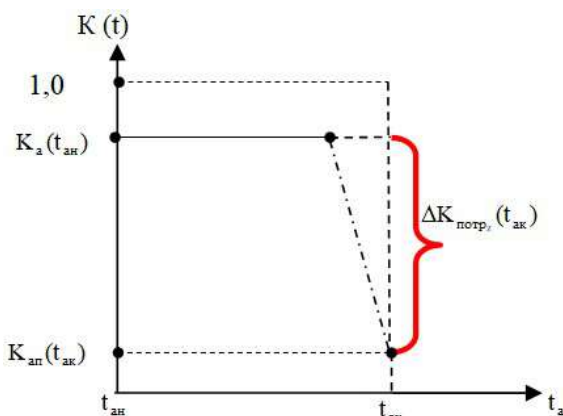


Рис. 4. Гіпотетичний приклад формування потрібного рівня зниження загрози з  $\Delta K_{потр_z}(t_{ак})$  на момент прогнозування  $t_{ак}$ :  $K_{ан}(t_{ак})$  – пороговий рівень воєнної загрози z – визначається в системі забезпечення воєнної безпеки для кожної загрози за окремою методикою;  $K_a(t_{ак})$  – поточний рівень воєнної загрози z на момент оцінювання  $t_{ак}$

На етапі № 5 з використанням удосконаленого методу аналізу ієрархій та моделі М7 здійснюється експертно-аналітичне прогнозування порогового рівня зниження загрози, за якого держава-агресор відмовиться від застосування військової сили проти держави-мішені.

Методом експертних оцінок проводиться оцінювання потрібних показників щодо усунення (зниження рівня) Z-ї загрози, а саме:

потрібного рівня зниження загрози  $\Delta K_{потр_z}$ , як різниця між поточним  $K_a(t_{ак})$  та пороговим  $K_{ан}(t_{ак})$  рівнями загрози

$$\Delta K_{потр_z}(t_{ак}) = K_a(t_{ак}) - K_{ан}(t_{ак}),$$

$K_{пор_z}(t_1) = K_{пор_z}(T_{пр})$ . Приклад формування потрібного рівня зниження  $\Delta K_{потр_z}(t_{ак})$  загрози на момент прогнозування  $t_{ак}$  показано на рис. 4;

оцінювання потрібних ресурсів  $R_{рес\ потр_z}$  для досягнення потрібного рівня зниження загрози; потрібного часу  $t_{потр_z}$  для досягнення потрібного рівня зниження загрози.

На етапі № 6 обґрунтовується рішення щодо вибору прямого (симетричного) або асиметричного способу реагування на виявлену загрозу за критеріями:

досягнення потрібного рівня зниження загрози

$$\Delta K_{потр_z} \geq K_{ан_z}(t_{ак});$$

виділені (наявні) ресурси  $R_{рес_z} \geq R_{рес\ потр_z}$ ;

обмеження у часі  $t_{потр_z} \leq t_{ак}$ .

Якщо зазначені умови виконуються, то може бути прийнято рішення на нейтралізацію загрози прямим (симетричним) методом; якщо хоча б одна із умов не виконується, то доцільно прийняти рішення на асиметричну протидію.

На етапі № 7 після прийняття рішення щодо нейтралізації загрози асиметричним методом експертами здійснюється розроблення проекту задуму (пропозиції) та сценарію проведення і-ї ЛСО із залученням суб'єктів ЗС України для нейтралізації виявленої загрози з визначенням дольової участі кожного суб'єкта у формуванні і-го інтегрованого потенціалу асиметричної протидії.

У задумі (пропозиціях) повинні бути відображені такі основні положення:

1. Мета локальної спеціальної операції.
2. Висновки із оцінки обстановки (противник та його основні параметри, зокрема чисельність особового складу, що залучений до агресії, чисельність резерву, співвідношення воєнних потенціалів, допустимі втрати особового складу супротивника, за яких він відмовиться від подальших бойових дій  $M_{осд}$ , допустимі втрати озброєння і військової техніки супротивника, за яких він відмовиться від агресії  $M_{овтд}$ , оцінений інтегрований рівень воєнної загрози, прогнози

ризика деструктивного впливу на визначальні сфери національної безпеки, найбільш уразливі місця (точки) завдання збитку противнику асиметричними діями).

3. Бойові завдання суб'єктам, що залучаються до ЛСО. Особливістю даного пункту замислу є не тільки зміст бойового завдання, а й ступінь його впливу на досягнення мети ЛСО, який оцінюється за 8-бальною шкалою експертним шляхом з використанням моделі М7. Крім того, для кожного суб'єкта формується мережева граф-модель виконання поставлених завдань, у якій вершини представляють собою завдання або їх етапи, а дуги визначають часові нормативи їх виконання.

4. Завдання щодо підготовки району проведення ЛСО.

5. Порядок та способи виведення суб'єктів, із яких сформовано потенціал асиметричної протидії, в район проведення ЛСО.

6. Управління в ході проведення ЛСО та взаємодія з іншими складовими сил оборони.

7. Легендування ЛСО.

8. Спеціальне інформаційне, психологічне та іміджове забезпечення проведення ЛСО.

9. Порядок виходу із ЛСО.

На етапі № 8 експертами здійснюється формування інтегрованого потенціалу асиметричної протидії зі складу збройних сил в і-ї ЛСО. Сформований інтегрований потенціал асиметричної протидії складається з вибраного  $\{V_{kz}\}$ , ( $k=1, K$ ) варіанта груп суб'єктів  $J$ , рис. 5, де  $K$  – кількість варіантів груп суб'єктів. Експертами для кожного пропонованого  $V_k$ -та обґрунтовуються потреби в ресурсах  $R_{res vkz}$  та потрібний час  $t_{vkz}$  для досягнення потрібного рівня деескалації загрози  $\Delta K_{потр z}$ .



Рис. 5. Суб'єкти ЗС, які можуть бути залучені при формуванні інтегрованого потенціалу асиметричної протидії

Наявність множини варіантів групи суб'єктів збройних сил для нейтралізації загрози пояснюється різними спроможностями складових збройних сил, складністю завдань, наявністю необхідних різного роду ресурсів, можливих (потрібних) проміжків часу для виконання завдань тощо.

На етапі № 9 здійснюється експертне оцінювання можливості виконання сформованим потенціалом асиметричного реагування завдань щодо нейтралізації загрози з урахуванням потрібних ресурсів ( $R_{res потр i}$ ) та наявних для нейтралізації загрози ресурсів ( $R_{res i}$ ):

$$R_{resi} \geq R_{res потр i}$$

На етапі № 10 якщо умова не виконується, то здійснюється нова ітерація на 7-му етапі.

На етапі № 11 з використанням удосконаленого методу аналізу ієрархій та моделі М7 здійснюється прогнозне оцінювання зниження рівня загрози на початок проведення і-ї ЛСО  $\Delta K_{KB}(t_{in})$ .

$\Delta K_{KB}(t_{in})$  – зниження рівня загрози на початок проведення і-ї ЛСО за рахунок військових та невійськових сил та засобів держави-жертви агресії (симетричної протидії).

На етапі № 12 з використанням удосконаленого методу аналізу ієрархій та моделі М7 здійснюється прогнозне оцінювання зниження рівня загрози на момент завершення і-ї ЛСО  $\Delta K_{AC i}(t_{ik})$ .

$\Delta K_{AC i}(t_{ik})$  – зниження рівня загрози за рахунок проведеної і-ї ЛСО з асиметричної протидії суб'єктами ЗС держави-жертви агресії.

Ураховуючи зазначене, очікувана результативність (ефективність) протидії агресії держави, що значно переважає державу-мішень за військовою «потужністю»  $E_{Ba}(t)$ , може бути оцінена сумарним рівнем деескалації загрози на момент часу  $t$  за рахунок симетричної (прямой військової) та асиметричної (комплексної) протидії агресії, рис. 6.

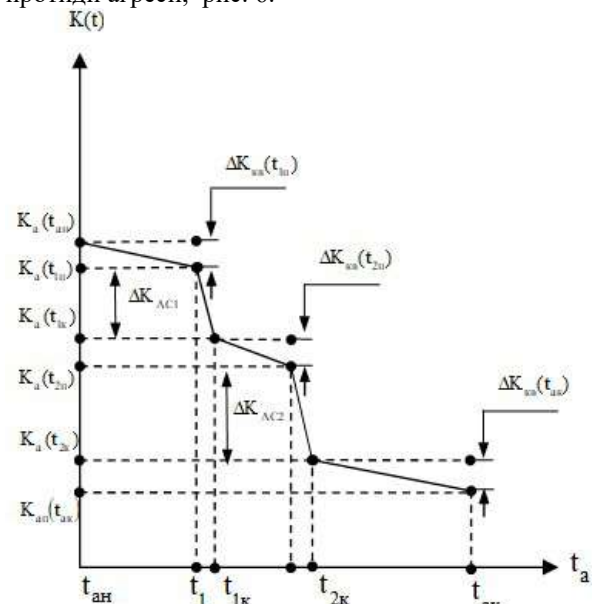


Рис. 6. Гіпотетичний приклад оцінювання ефективності відбиття агресії держави, що значно перевищує державу-мішень у військовій «потужності», з використанням симетричної і асиметричної протидії у двох ЛСО (I=2)

$$E_{Ba}(t) = K_a(t_{ah}) - \sum_{i=1}^I \Delta K_{AC i}(t_{ik}, R_{res i}, M_{oc i}, M_{ovt i}) -$$

$$\sum_{i=1}^I \Delta K_{KB}(t_{in}, R_{res i}, M_{oc i}, M_{ovt i}) - \Delta K_{KB}(t_a > t_{JK}, R_{res i}, M_{oc i}, M_{ovt i})$$

при  $R_{res i} \leq R_{res bi}$  ;

$$M_{oc i} \leq M_{осдоп i} ;$$

$$M_{\text{овт } i} \leq M_{\text{овтдоп } i};$$

де  $t$  – поточний час протидії (відбиття) агресії;

$t_{\text{ан}}(t_{\text{ак}})$  – час початку (закінчення) агресії;

$t_{\text{ін}}(t_{\text{ік}})$  – час початку (закінчення)  $i$ -ї, ( $i=1, I$ ), ЛСО асиметричної протидії;

$I$  – кількість проведених ЛСО;

$K_a(t_{\text{ан}})$  – рівень загрози, що несе державі-жертві розв'язувана агресія;

$\Delta K_{\text{AC } i}$  – зниження рівня загрози за рахунок проведення  $i$ -ї ЛСО;

$\Delta K_{\text{KB}}(t_{\text{ін}})$  – зниження рівня загрози на початок проведення  $i$ -ї ЛСО за рахунок комплексного використання військових і невійськових сил та засобів держави-жертви агресії (симетричної протидії);

$R_{\text{рес } i}(R_{\text{рес в } i})$  – ресурси (максимально можливі ресурси), що використовуються при проведенні  $i$ -ї ЛСО;

$M_{\text{ос } i}(M_{\text{осдоп } i})$  – втрати (допустимі втрати) особового складу при проведенні  $i$ -ї ЛСО;

$M_{\text{овт } i}(M_{\text{овтдоп } i})$  – втрати (допустимі втрати) озброєння і військової техніки в  $i$ -ї ЛСО;

$R_{\text{рес}}$  – ресурси, що використовуються при відбитті агресії симетричними методами або комплексним застосуванням військових і невійськових інструментів [5];

$M_{\text{ос}}$  – втрати особового складу, у тому числі невійськових суб'єктів сил оборони, що залучаються до відбиття агресії;

$M_{\text{овт}}$  – втрати озброєння і військової техніки в ході відбиття агресії.

Звідси ефективність асиметричної протидії агресії у загальному вигляді може бути оцінена як результат сумарного зниження рівня загрози в проведених ЛСО:

$$E_{\text{AC}}(t_a) = \sum_{i=1}^J \Delta K_{\text{AC } i}(t_{\text{ік}}, R_{\text{рес } i}, M_{\text{ос } i}, M_{\text{овт } i}).$$

Критерієм прийняття рішення державою-агресором про відмову від подальших агресивних дій є виконання хоча б однієї з умов:

$$E_{\text{ва}}(t_{\text{ак}}) \leq K_{\text{ап}}(t_{\text{ак}});$$

$$M_{\text{оса}}(t_{\text{ак}}) \geq M_{\text{осад}},$$

де  $K_{\text{ап}}(t_{\text{ак}})$  – пороговий рівень загрози, яку спричинила державі-жертві агресії розпочата проти неї агресія;

$M_{\text{оса}}(t_{\text{ак}})$  – втрати особового складу держави-агресора, що був залучений до здійснення агресії, у тому числі залучених бойовиків, найманців тощо;

$M_{\text{осад}}$  – допустимі для держави-агресора втрати особового складу.

**На етапі № 13** з використанням удосконаленого методу аналізу ієрархій та моделі

M7 здійснюється оцінювання результативності протидії загрозам:

$$\text{асиметрична протидія } \sum_i \Delta K_{\text{AC } i}(t_{\text{ік}});$$

$$\text{симетрична протидія } \sum_i \Delta K_{\text{KB}}(t_{\text{ін}}).$$

**На етапі № 14** проводиться оцінювання можливості відмови держави-А від подальших агресивних дій за критерієм

$$\left\{ K_a(t_{\text{ан}}) - \sum_i \Delta K_{\text{AC } i}(t_{\text{іі}}) - \sum_i \Delta K_{\text{KB}}(t_{\text{ін}}) \right\} \leq K_{\text{ап}}(t_{\text{ак}}).$$

**На етапі № 15** експертами проводиться оцінювання втрат особового складу держави-агресора на момент завершення  $i$ -ї ЛСО  $M_{\text{оса}}(t_{\text{ік}})$  (наприклад, з використанням даних Головного управління розвідки МО України).

**На етапі № 16** проводиться оцінювання можливості відмови держави-А від подальших агресивних дій за критерієм

$$M_{\text{оса}}(t_{\text{ік}}) \geq M_{\text{осд}}.$$

**На етапі № 17** експертами здійснюється оцінка втрат озброєння та військової техніки держави-агресора на момент завершення  $i$ -ї ЛСО  $M_{\text{овта}}(t_{\text{ік}})$  (наприклад, з використанням даних Головного управління розвідки ЗС України).

**На етапі № 18** проводиться оцінювання можливості відмови держави-А від подальших агресивних дій за критерієм

$$M_{\text{овта}}(t_{\text{ік}}) \geq M_{\text{овтд}}$$

**На етапі № 19** якщо одна із умов на етапі 13, 15 та 17 не виконується, готується та проводиться нова ЛСО.

Методика пропонується для використання вищим воєнно-політичним керівництвом держави із залученням прогнозистів, аналітиків і експертів.

Припинення агресії проти держави-жертви може бути здійснено і за інших умов, наприклад, за рішенням Ради Безпеки ООН, у відповідь на ультиматум створеної коаліції держав тощо.

### Висновки й перспективи подальших досліджень

Таким чином, розроблена методика прогнозного оцінювання ефективності асиметричного реагування Збройних Сил України на загрози у воєнній сфері дає змогу формувати інтегрований потенціал суб'єктів ЗС, практична реалізація якого у формі локальної спеціальної операції у визначених «больових точках» держави-агресора забезпечує завдання її неприйняттю збитку, в т.ч. і в невійськових сферах безпеки.

Методика забезпечує прогнозне оцінювання ефективності протидії агресії держави, що значно переважає державу-мішень за військовою «потужністю», за інтегральним показником «сумарний рівень деескалації загрози», на певний момент часу за рахунок симетричної (прямої військової) та асиметричної (комплексної) протидії агресії. Кількість локальних спеціальних



операцій визначається можливостями держави-жертви агресії. Сформована система обмежень та визначені критерії прийняття рішення державою-агресором про відмову від подальших

агресивних дій. Основними обмеженнями держави, що проводить наступальні дії, є втрати особового складу, озброєння та військової техніки її збройних формувань.

### Література

1. Україна. Закони. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII // Законодавство України з питань військової сфери. – К.: Голос України від 07.07.2018 року № 122 (6877). 2. Стратегія національної безпеки України: Указ Президента України: від 26 травня 2015 року № 287. – К.: АПУ, 2015. – 12 с. 3. Военна доктрина України: Указ Президента України від 24 вересня 2015 року № 555. – К.: АПУ, 2015. – 27 с. 4. Концепція розвитку сектору безпеки і оборони України: схвалена Указом Президента України від 14.03.2016 року № 92/2016. – К.: АПУ, 2016. – 17с. 5. **Богданович В. Ю.** Теоретико-методологічні основи забезпечення національної безпеки України: монографія: у 7 т. – Т.1. Теоретичні основи, методи й технології забезпечення національної безпеки України / В.Ю. Богданович, І.Ю. Свида, Є.Д. Скулиш; за заг. ред. Є.Д. Скулиша. – К.: Наук.-вид. відділ НА СБ України, 2012. – 548 с. 6. **Богданович В. Ю.** Методологія комплексного використання військових і невійськових сил і засобів сектора безпеки і оборони для протидії сучасним загрозам воєнній безпеці України: монографія /

В.Ю. Богданович, І.С. Романченко, І.Ю. Свида, А.М. Сиротенко. – К.: НАСВ, 2019. – 268 с. 7. **Богданович В. Ю.** Нові «лабіринти» безпекового середовища та їх вплив на забезпечення воєнної безпеки держави / В.Ю. Богданович, А.М. Сиротенко, А.М. Прима // Харків: ХУПС: Наука і техніка Повітряних сил Збройних Сил України, 2019, № 2 (35). С. 9–15. 8. **Богданович В. Ю.** Теоретико-методологічні основи забезпечення національної безпеки України: монографія : у 7 т. – Т.4. Военна безпека держави і шляхи її забезпечення / В.Ю. Богданович, І.Ю. Свида, Є.Д. Скулиш; за заг. ред. Є.Д. Скулиша. – К.:Наук.-вид. відділ НА СБ України, 2012. – 464 с. 9. Метод «Діаграма Іскави». [Електронний ресурс]. – Режим доступу до ресурсу:<http://www.inventech.ru/pub/methods/metod-0019/>. 10. **Богданович В. Ю.** Методичний підхід до визначення необхідних спроможностей складових інтегрованого потенціалу протидії загрозам на виконавчому рівні / В. Ю. Богданович, А. М. Прима // Харків: ХУПС: Наука і техніка Повітряних сил Збройних Сил України, 2017, № 2 (27). С. 162–166.

## МЕТОДИКА ПРОГНОЗНОГО ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ АСИММЕТРИЧНОГО РЕАГИРОВАНИЯ ВООРУЖЕННЫХ СИЛ УКРАИНЫ НА УГРОЗЫ В ВОЕННОЙ СФЕРЕ

*Владимир Юрьевич Богданович (доктор технических наук, профессор)<sup>1</sup>  
Александр Владимирович Дублян (кандидат военных наук)<sup>1</sup>  
Анатолий Николаевич Сиротенко (доктор военных наук)<sup>2</sup>  
Александр Викторович Передрий (кандидат военных наук)<sup>1</sup>  
Андрей Николаевич Прима<sup>1</sup>*

<sup>1</sup>Центральный научно-исследовательский институт Вооруженных Сил Украины, Киев, Украина

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

*Представлена методика прогнозного оценивания эффективности асимметричного реагирования на современные угрозы в интересах обеспечения достаточного уровня военной безопасности государства. В условиях комплексного использования военных и невоенных инструментов (экономических, политических, информационно-психологических и др.) появилась необходимость в оценивании и прогнозировании эффективности асимметричного использования военных и невоенных сил и средств в противодействии силовому давлению и использованию военной силы против государства, которое противостоит более сильному в военном отношении противнику.*

*Основным ограничением государства, которое проводит наступательные действия, являются потери личного состава. Для государства-жертвы агрессии потери личного состава, населения, инфраструктуры и т.п. в таком конфликте намного больше. Мировой опыт показывает, что значительно более слабое в военном отношении государство, осуществляя асимметричные меры противодействия угрозам военными и невоенными субъектами сил обороны, способно нанести противнику неприемлемый ущерб, в т.ч. и в невоенных сферах безопасности, и тем самым заставить даже более сильного в военном отношении противника отказаться от применения военной силы против него.*

*Предлагается эффективность противодействия агрессии государства, которое значительно превосходит государство-мишень по военной «мощности», оценивать суммарным уровнем деэскалации угрозы на определённый момент времени за счёт симметричной (прямой военной) и асимметричного (комплексного) противодействия агрессии в форме проведения локальной специальной операции. Количество локальных специальных операций определяется возможностями государства-жертвы агрессии. Сформирована система ограничения и определены критерии принятия решения государством-агрессором про отказ от дальнейших агрессивных действий.*

**Ключевые слова:** военная безопасность; угроза; асимметричное противодействие; силовое давление; военная сила; эффективность противодействия; вооруженный конфликт; деэскалация угрозы.

## METHODOLOGY FOR FORECASTING ASSESSING THE EFFECTIVENESS OF THE ASYMMETRIC RESPONSE OF THE ARMED FORCES OF UKRAINE TO THREATS IN THE MILITARY SPHERE

*Volodymyr Bohdanovych (Doctor of Technical Sciences, Professor)<sup>1</sup>*  
*Oleksandr Dublian (Candidate of Military Sciences)<sup>1</sup>*  
*Anatolii Syrotenko (Doctor of Military Sciences)<sup>2</sup>*  
*Oleksandr Peredrii (Candidate of Military Science)<sup>1</sup>*  
*Andrii Pryma<sup>1</sup>*

<sup>1</sup>*Central research institute of the Armed Forces of Ukraine, Kyiv, Ukraine*

<sup>2</sup>*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*A methodology for predictive evaluation of the effectiveness of an asymmetric response to modern threats is presented in the interests of ensuring an adequate level of military security of the state. In the context of the integrated use of military and non-military instruments (economic, political, information-psychological, etc.), there was a need to evaluate and predict the effectiveness of the asymmetric use of military and non-military forces and means in countering force pressure and the use of military force against a state that opposes a stronger military opponent.*

*The main limitation of the state, which conduct offensive actions, is the loss of personnel. For the state-victim of aggression, the loss of personnel, population, infrastructure, etc. in such a conflict much more. World experience shows that the state, which is significantly weak in military relations, by carrying out asymmetric measures to counter threats by military and non-military subjects of the defense forces, is capable of inflicting unacceptable damage on the enemy, including and in non-military areas of security, and thereby force an even stronger military opponent to abandon the use of military force against it.*

*We propose the effectiveness of counteracting state aggression, which significantly dominates the target state in military "power", to assess the total level of threat de-escalation at a certain time due to the symmetric (direct military) and asymmetric (complex) counteraction of aggression in the form of conducting a local special operation. The number of local special operations is determined by the capabilities of the state-victim of aggression. Formed system of restriction and decision-making criteria defined the aggressor state to refuse further aggressive actions.*

**Key words:** *military security; threat; asymmetric counteraction; force pressure; military force; effectiveness of counteraction; armed conflict; de-escalation of the threat.*

### References

1. *Ukrajina. Zakony. Pro nacionaljnu bezpeku Ukrajinu: Zakon Ukrajinu vid 21 chervnja 2018 roku № 2469–VIII // Zakonodavstvo Ukrajinu z pytanj vijsjkovoji sfery. – K.: Gholos Ukrajinu vid 07.07.2018 roku № 122 (6877).*
2. *Strateghija nacionaljnoji bezpeky Ukrajinu: Ukaz Prezydenta Ukrajinu: vid 26 travnja 2015 roku № 287. – K.: APU, 2015. – 12 s.*
3. *Vojenna doktryna Ukrajinu: Ukaz Prezydenta Ukrajinu vid 24 veresnja 2015 roku № 555. – K.: APU, 2015. – 27 s.*
4. *Koncepcija rozvytku sektoru bezpeky i oborony Ukrajinu: skhvalena Ukazom Prezydenta Ukrajinu vid 14.03.2016 roku №92/2016. – K.: APU, 2016. – 17s.*
5. **Boghdanovych V. Ju.** *Teoretyko-metodologhichni osnovy zabezpechennja nacionaljnoji bezpeky Ukrajinu: monoghrafija: u 7 t. – T.1. Teoretychni osnovy, metody j tekhnologhiji zabezpechennja nacionaljnoji bezpeky Ukrajinu / V. Ju. Boghdanovych, I. Ju. Svyda, Je. D. Skulysh; za zagh. red. Je. D. Skulysha. – K.: Nauk.-vyd. viddil NA SB Ukrajinu, 2012. – 548 s.*
6. **Boghdanovych V. Ju.** *Metodologhija kompleksnogho vykorystannja vijsjkovykh i nevijsjkovykh syl i zasobiv sektora bezpeky i oborony dlja protydiji suchasnym zaghrozam vojennij bezpeci Ukrajinu: monoghrafija / V. Ju. Boghdanovych, I. S. Romanchenko, I. Ju. Svyda, A. M. Syrotenko. – K.: NASV, 2019. – 268 s.*
7. **Boghdanovych V. Ju.** *Novi «labirynty» bezpekovogho seredovyshha ta jikh vplyv na zabezpechennja vojennoji bezpeky derzhavy / V. Ju. Boghdanovych, A. M. Syrotenko, A. M. Pryma // Kharkiv: KhUPS: Nauka i tekhnika Povitrjanykh syl Zbrojnykh Syl Ukrajinu, 2019, № 2 (35). S. 9–15.*
8. **Boghdanovych V. Ju.** *Teoretyko-metodologhichni osnovy zabezpechennja nacionaljnoji bezpeky Ukrajinu: monoghrafija : u 7 t. – T.4. Vojenna bezpeka derzhavy i shljakhy jiji zabezpechennja / V. Ju. Boghdanovych, I. Ju. Svyda, Je. D. Skulysh; za zagh. red. Je. D. Skulysha. – K.: Nauk.-vyd. viddil NA SB Ukrajinu, 2012. – 464 s.*
9. *Metod «Diaghrama Isikavy». [Elektronnyj resurs]. – Rezhym dostupu do resursu: <http://www.inventech.ru/pub/methods/metod-0019/>.*
10. **Boghdanovych V. Ju.** *Metodychnyj pidkhd do vyznachennja neobkhdnykh spromozhnostej skladovykh integhrovanogho potencialu protydiji zaghrozam na vykonavchomu rivni / V. Ju. Boghdanovych, A. M. Pryma // Kharkiv: KhUPS: Nauka i tekhnika Povitrjanykh syl Zbrojnykh Syl Ukrajinu, 2017, № 2 (27). S. 162–166.*

*Василь Кузьмович Шевченко*

*Олександр Іванович Волощенко (кандидат військових наук)*

*Олександр Вікторович Бобрун (кандидат військових наук)*

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

## СПОСІБ ВИЗНАЧЕННЯ ВЕЛИЧИНИ ВПЛИВУ ФОРТИФІКАЦІЙНОГО ОБЛАДНАННЯ НА ЖИВУЧІСТЬ СИСТЕМИ УПРАВЛІННЯ ВІЙСЬКАМИ (СИЛАМИ) В ОПЕРАЦІЇ (БОЙОВИХ ДІЯХ)

*У статті йдеться про спосіб визначення величини впливу фортифікаційного обладнання на живучість системи управління військами (силами), який базується на теорії оцінювання живучості точкових військових об'єктів при прицільному вогневому впливі противника.*

*Зазначається, що особливістю способу визначення величини впливу фортифікаційного обладнання на живучість системи управління військами (силами) є врахування конфігурації зони ураження окремих елементів (об'єктів) системи управління військами (силами), можливої траєкторії польоту та кругового розсіювання боєприпасів під час прицільної дії на них засобів ураження противника.*

*Стверджується, що запропонований спосіб визначення величини впливу фортифікаційного обладнання на живучість системи управління військами (силами) дозволяє визначати черговість виконання заходів під час фортифікаційного обладнання цих об'єктів, що дозволить якнайшвидше укрити ці об'єкти у польових фортифікаційних спорудах і суттєво ускладнити їх виявлення, ідентифікацію та ураження під час бойових дій.*

*Зазначається, що запропонований спосіб може бути використаним для поточного прогнозування величини впливу фортифікаційного обладнання на живучість системи управління військами, а також під час проведення досліджень з питань живучості військ у сучасних збройних конфліктах.*

**Ключові слова:** система управління; живучість; фортифікаційне обладнання.

### Вступ

**Постановка проблеми.** Застосування у сучасних збройних конфліктах високоефективних систем розвідки та вогневого ураження призводить до великих втрат військ. Для мінімізації цих втрат війська змушені нарощувати спроможності з підвищення живучості своїх об'єктів, зокрема за рахунок їх укриття у польових фортифікаційних спорудах тобто виконанням заходів з їх фортифікаційного обладнання (далі – ФО) [1].

Результати досліджень живучості системи управління військами (силами) в операції (бойових діях) (далі – СУ) свідчать, що, виходячи з конфігурації і лінійних розмірів окремих елементів цієї системи, ці елементи, розглядаються, як точкові, групові, лінійні та площинні військові об'єкти. Аналіз свідчить, що в якості основного показника для оцінювання живучості СУ найчастіше приймається ймовірність збереження її функціонування.

Точковим об'єктом СУ (далі – об'єктом СУ),

який взято у якості основного для визначення величини впливу ФО на живучість СУ, прийнято вважати малорозмірний, порівняно із зоною свого ураження об'єкт, який являє собою єдине ціле під час виконання функцій управління військами (силами). Такими об'єктами у СУ є командно-штабні машини (КШМ), командно-спостережні пункти (КСП) тощо.

Відповідно теорії оцінки живучості військових об'єктів під час прицільного впливу, детальний опис якої наведено у [2], основними показниками для оцінювання живучості об'єкта СУ доцільно прийняти ймовірність збереження (ураження) певного об'єкта СУ, які пов'язані таким співвідношенням:

$$Q(A) + P(A) = 1. \quad (1)$$

де  $Q(A), P(A)$  – ймовірність збереження (ураження) об'єкта СУ.

Визначальним фактором живучості об'єкта СУ, є фактор часу. Суть цього фактора полягає у виконання заходів живучості об'єкта СУ у найкоротший термін. При цьому, вплив

яких на живучість об'єкта є найбільшими, повинні виконуватися в першу чергу. Це дозволить якнайшвидше виконати найважливіші заходи, що суттєво ускладнить його виявлення і ураження. Саме тому визначення величини впливу ФО на живучість СУ є важливим науковим завданням.

**Аналіз останніх досліджень і публікацій.** Аналіз останніх досліджень і публікацій з питань живучості СУ свідчить, що оперування тільки показниками, які фігурують в (1), не вирішує існуючої проблеми живучості СУ у сучасному збройному конфлікті.

**Метою статті** є опис способу визначення величини впливу ФО на живучість СУ в операції (бойових діях), який базується на теорії оцінювання живучості військових об'єктів під час прицільного впливу [2].

### Виклад основного матеріалу дослідження

Згідно [1] величина впливу ФО на живучість об'єкта СУ визначається так:

$$K_{\text{ФО}}^Q = \frac{Q^{(\text{ФО})} - Q^{(0\text{ФО})}}{Q^{(0)}}, \quad (2)$$

де  $Q^{(\text{ФО})}$  ( $Q^{(0\text{ФО})}$ ) – живучість об'єкта СУ, яка досягається за умови його ФО (без ФО);

$Q^{(0)}$  – початковий ступінь живучості об'єкта СУ.

Оскільки ступінь живучості об'єкта СУ звичайно залежить від ймовірності його виявлення та ураження, ступінь його живучості за умови його ФО визначається так [2]:

$$Q^{(\text{ФО})} = 1 - P_{\text{в}}^{(\text{ФО})} \times P_{\text{ур}}^{(\text{ФО})}, \quad (3)$$

де  $P_{\text{в}}^{(\text{ФО})}$  ( $P_{\text{ур}}^{(\text{ФО})}$ ) – ймовірність виявлення (ураження) об'єкта СУ за умови його ФО.

Згідно (3), живучість об'єкта СУ за відсутності ФО буде дорівнювати:

$$Q^{(0\text{ФО})} = 1 - P_{\text{в}}^{(0\text{ФО})} \times P_{\text{ур}}^{(0\text{ФО})}, \quad (4)$$

де  $P_{\text{в}}^{(0\text{ФО})}$ ;  $P_{\text{ур}}^{(0\text{ФО})}$  – ймовірність виявлення (ураження) об'єкта СУ без ФО.

Визначення невідомих величин у (3) і (4) можливе за допомогою теорії оцінки живучості військових об'єктів під час прицільного впливу, яка описана в [2]. У цій методиці величини ( $Q$ ) і ( $P_{\text{ур}}$ ) пов'язані співвідношенням  $Q + P_{\text{ур}} = 1$ .

Враховуючи, що основним завданням впливу засобів вогневого ураження по об'єкту СУ є його ураження, критерієм ефективності цього завдання є ймовірність ураження цього об'єкта ( $P_{\text{ур}}$ ), яка визначається за формулою повної ймовірності

$$P(A) = \sum_{i=1}^n P(B_i) \cdot P(A/B_i) \quad [1].$$

Зважаючи на те, що для ураження об'єкта СУ ймовірність його виявлення є ( $P_{\text{в}} = 1$ ), ймовірність ураження ( $P_{\text{ур}}$ ) визначається так [2]:

$$P_{\text{ур}} = \sum_{i=1}^n P_{n,m} \cdot Z(m), \quad (5)$$

де  $P_{n,m}$  – ймовірність попадання в зону ураження об'єкта СУ  $m$  боєприпасів противника із  $n$  можливих;

$Z(m)$  – закон ураження цілі. Умовна ймовірність ураження об'єкта, якщо в зону його ураження попало  $m$  із  $n$  наявних боєприпасів.

З огляду на те, що попадання у зону ураження об'єкта СУ кожного із  $m$  наявних у противника боєприпасів є подією незалежною, величина цієї події згідно [2] визначається так:

$$P_{n,m} = C_n^m (1 - P_1)^{n-m} P_1^m, \quad (6)$$

де  $P_1$  – ймовірність ураження об'єкта СУ за умови впливу на нього одного із  $m$  наявних боєприпасів противника.

Визначення величини  $Z(m)$  (5), яка у [2] визначається як закон ураження цілі, є доволі складним завданням. Це завдання у практичних задачах, найчастіше, вирішується експериментом, однак, у будь-якому випадку, цей закон мовою математики записується так:

$$Z(m) = \begin{cases} 0, & \text{при } m = 1 \\ 1, & \text{при } m \geq 1 \end{cases} \quad (7)$$

Отже, для ураження об'єкта СУ достатньо попадання у зону його ураження хоча б одного із  $m$  наявних у противника боєприпасів. За незалежного впливу боєприпасів противника по об'єкту СУ ймовірність його ураження, на відміну від (5), визначається за такою формулою:

$$P_{\text{ур}} = 1 - (1 - P_1)^n. \quad (8)$$

Враховуючи те, що об'єкти СУ мають різну конфігурацію, яка суттєво впливає на ймовірність їх виявлення і ураження, розглянемо розрахункові схеми визначення живучості для об'єктів СУ із круговою та прямокутною зонами ураження, а також ураження таких об'єктів за умови кругового розсіювання боєприпасів. Під час визначення ймовірності попадання боєприпасів у зону ураження об'єкта СУ її, частіше за все, приймають у вигляді круга з радіусом ( $R_{\text{ур}}$ ), як показано на рис. 1.

Згідно рис. 1 та відповідно [2], ймовірність ураження об'єкта СУ визначається за формулою:

$$P_{ур}^0 [(x,y)ID] = 1 - e^{-\rho^2 \frac{R_{ур}^2}{E^2}}, \quad (9)$$

де E – коефіцієнт Лапласа ( $E = \rho\sqrt{2}$ , де  $\rho = 0,477$ ).

Якщо ж точка прицілювання не збігається з центром об'єкта СУ (D) і він віддалений від неї на певну відстань (d), як показано на рис. 2, тоді ймовірність ураження такого об'єкта СУ визначається за формулою [2]:

$$P_{ур} = \begin{cases} (1 - e^{-\rho^2 \frac{R_{ур}^2}{E^2}}) e^{-\beta d^2} & \text{при } R_{ур} \leq 4E \\ e^{-\frac{4,2(d - R_{ур} + 4E)^2}{64E^2}} & \text{при } R_{ур} \geq 4E \end{cases}, \quad (10)$$

де  $\beta = \frac{4,2}{(4E + R_y)^2}$  – коефіцієнт, який враховує

зміну ймовірності ураження об'єкта СУ в залежності від величини d [2].

Якщо зона ураження об'єкта СУ має форму прямокутника із сторонами, паралельними осям осей, (рис. 3), тоді ймовірність попадання координат, а напрямок прицілювання засобів ураження противника співпадає з однією з цих точки  $E_x; E_y$ , у цю зону буде визначатись за такою формулою:

$$P_{ур} = (a \leq x \leq b, c \leq y \leq d, ) = \frac{\rho^2}{\pi E_x E_y} \int_a^b \int_c^d e^{-\rho^2 \left[ \left( \frac{x-x_{ур}}{E_x} \right)^2 + \left( \frac{y-y_{ур}}{E_y} \right)^2 \right]} dx dy \quad (11)$$

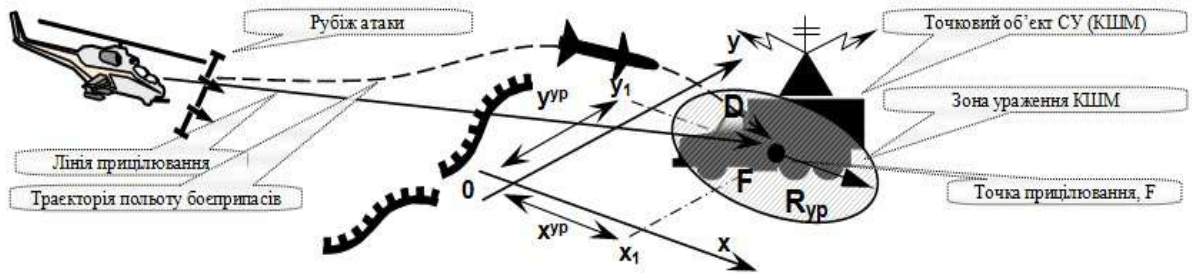


Рис.1 Розрахункова схема визначення живучості для об'єкта СУ з круговою зоною ураження

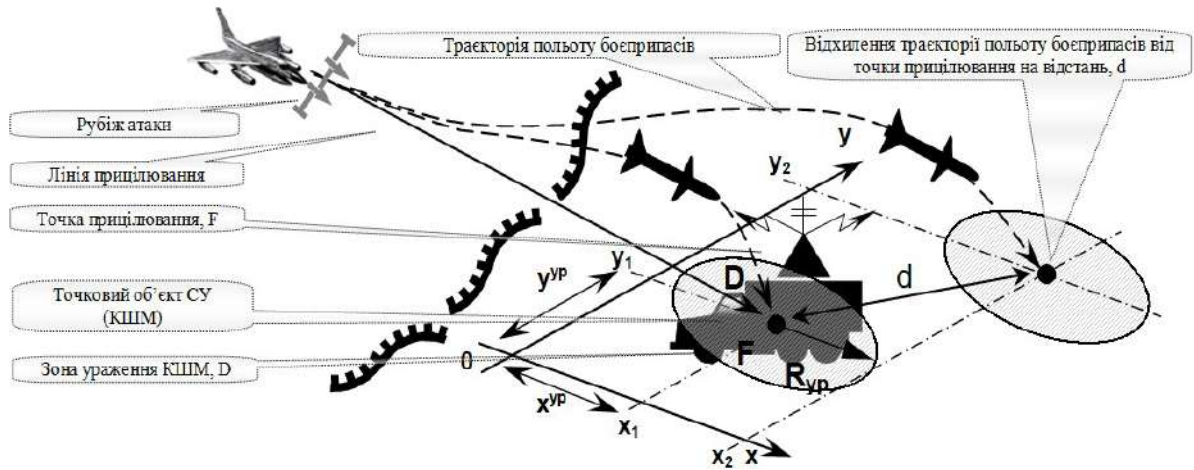


Рис. 2 Розрахункова схема визначення живучості для об'єкта СУ з круговою зоною ураження

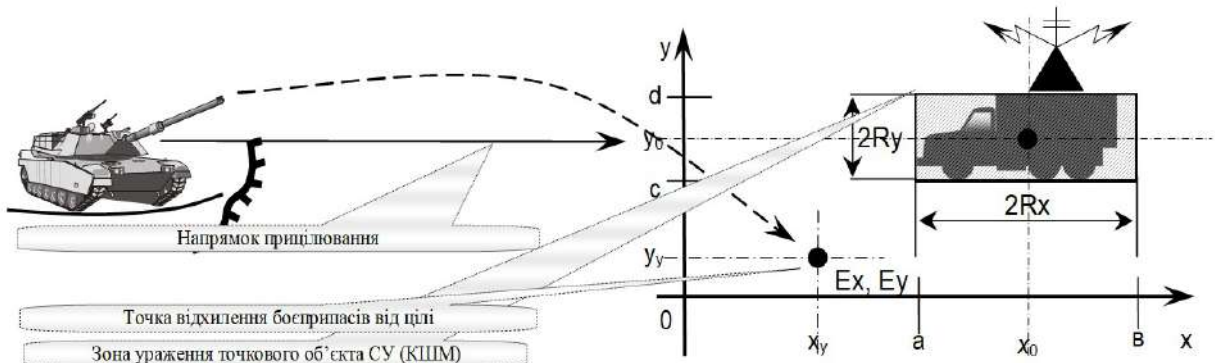


Рис. 3 Розрахункова схема визначення живучості для об'єкта СУ з прямокутною зоною ураження

Розрахунок (11) виконується за допомогою приведеної функції Лапласа [1]:

$$P_{ур} = \frac{1}{4} \left[ \Phi\left(\frac{b-x_{ур}}{E_x}\right) - \Phi\left(\frac{a-x_{ур}}{E_x}\right) \right] \times \left[ \Phi\left(\frac{d-y_{ур}}{E_y}\right) - \Phi\left(\frac{c-y_{ур}}{E_y}\right) \right]. \quad (12)$$

Якщо точка прицілювання співпадає з центром прямокутника з розмірами  $2R_x$  і  $2R_y$ , (рис.4), формула для розрахунку ймовірності ураження об'єкта СУ матиме такий вигляд:

$$P_{ур} = (a \leq x \leq b, c \leq y \leq d) = \Phi\left(\frac{R_x}{E_x}\right) \cdot \Phi\left(\frac{R_y}{E_y}\right). \quad (13)$$

Якщо точковий об'єкт СУ має значну протяжність в одному з напрямків (рис. 5) і його функціонування закінчується в разі ураження будь-якої його точки, тоді для визначення ймовірності ураження такого об'єкта можна використати формулу:

$$P_{ур} = (a \leq x \leq b) = \frac{1}{2} \left[ \Phi\left(\frac{b-x_{ур}}{E_x}\right) + \Phi\left(\frac{a-x_{ур}}{E_x}\right) \right]. \quad (14)$$

Визначення ймовірності ураження об'єкта СУ для випадку кругового розсіювання боеприпасів із певним наближенням можна звести до розрахунку ймовірності попадання точки прицілювання, яка розподілена за нормальним законом з ймовірним відхиленням цієї точки у рівновеликий круг з радіусом  $R$  або квадрат зі стороною  $a = R\sqrt{\pi}$ , тобто  $\frac{a}{2} = 0,0887 \cdot R$  і  $\delta = 1,5E$ .

$$P_{ур} [(x, y) \in D] = \left[ \Phi_0\left(\frac{d+0,0887R}{1,5E}\right) - \Phi_0\left(\frac{d-0,0887R}{1,5E}\right) \right] 2\Phi_0\left(\frac{0,0887R}{1,5E}\right), \quad (15)$$

де  $\Phi_0(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt$  – значення функції Лапласа.

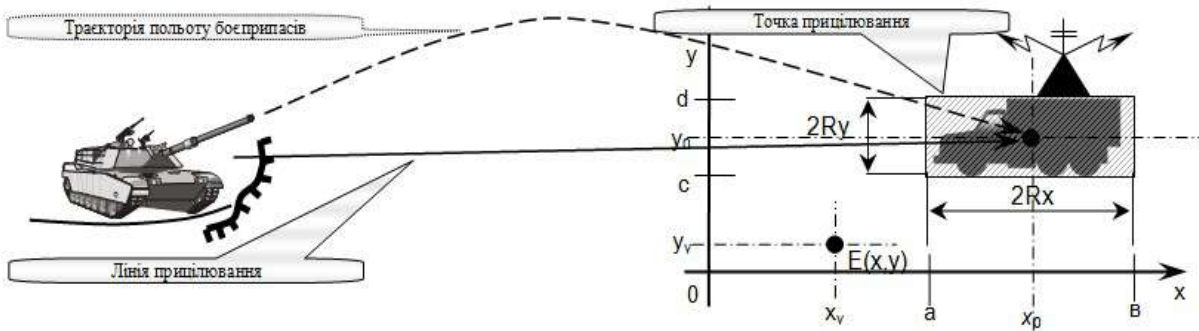


Рис. 4 Розрахункова схема визначення живучості для об'єкта СУ з прямокутною зоною ураження

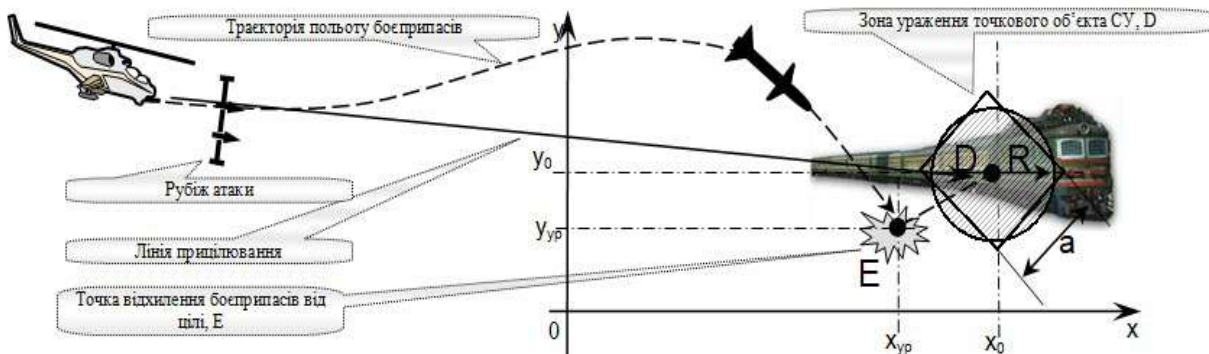


Рис. 5 Розрахункова схема визначення живучості для об'єкта СУ, який має значну протяжність в одному з напрямків, для випадку кругового розсіювання боеприпасів

Отримані таким чином величини ймовірності ураження об'єкта СУ використовуємо у формулах (2 – 4) та визначаємо величину впливу ФО на його живучість, а у загальному підсумку за всіма об'єктами СУ живучість СУ у цілому.

*Приклад.* Потрібно визначити величину впливу ФО на живучість КШМ під час бойових дій (рис. 6).

Припустимо, що ймовірність виявлення КШМ засобами розвідки противника дорівнює одиниці

( $P_B = 1$ ), а ймовірність її ураження за умови виконання та невиконання його ФО відповідно буде рівною  $P_{ур}^{FO} = 0,3$  та  $P_{ур}^{0FO} = 0,7$ .

Підставляємо визначені величини у формулу (2), та отримуємо величину впливу ФО на живучість КШМ, яка становить:

$$K_{FO}^Q = \frac{(1 - 1 \cdot 0,3) - (1 - 1 \cdot 0,7)}{1} = 0,4.$$

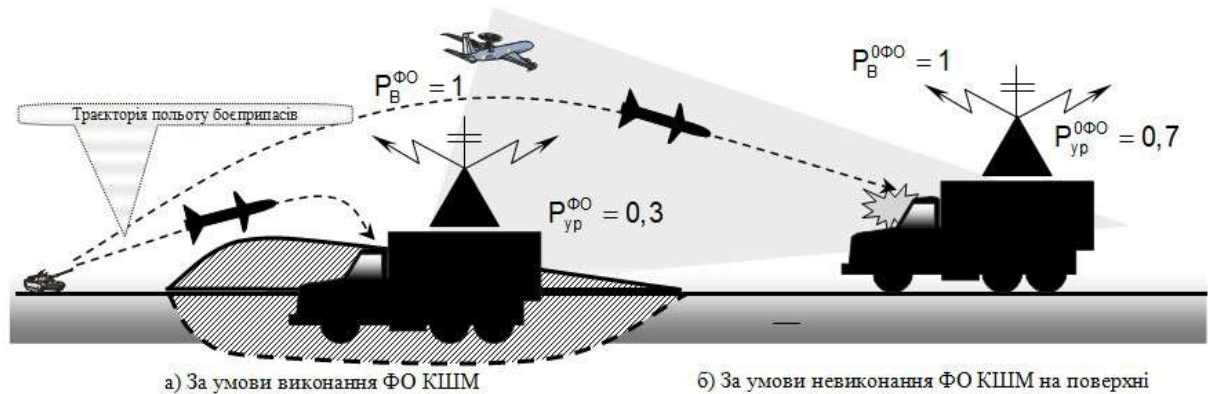


Рис. 6 Схема визначення величини впливу фортифікаційного обладнання на живучість КШМ

Порівнявши отриману величину впливу ФО на живучість КШМ з величинами інших заходів визначається послідовність їх виконання, що дозволяє якнайшвидше досягти потрібного ступеня живучості КШМ і тим самим максимально захистити її від засобів ураження противника.

Визначивши таким чином величину впливу ФО на живучість всіх об'єктів СУ можна визначити величину впливу ФО на живучість СУ в цілому.

Наведений приклад свідчить про можливість практичного застосування запропонованого способу визначення величини впливу ФО на живучість СУ, а також для вирішення практичних завдань підвищення живучості військ (об'єктів) у сучасних збройних конфліктах.

### Література

1. Шевчук А.Б. Фортификационное оборудование позиций и районов в локальных войнах и вооруженных конфликтах. А.Б. Шевчук. – М.: Воениздат, 1999. – 104 с.
2. Юрков Б.Н. Исследование операций. Б. Н. Юрков. – М.: ВИА, 1990. – 205 с.

## СПОСОБ ОПРЕДЕЛЕНИЯ ВЕЛИЧИНЫ ВОЗДЕЙСТВИЯ ФОРТИФИКАЦИОННОГО ОБОРУДОВАНИЯ НА ЖИВУЧЕСТЬ ТОЧЕЧНЫХ ОБЪЕКТОВ СИСТЕМЫ УПРАВЛЕНИЯ ВОЙСКАМИ (СИЛАМИ)

Шевченко Василий Кузьмич

Волощенко Александр Иванович (кандидат военных наук)

Бобрун Александр Викторович (кандидат военных наук)

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

В статье рассматривается способ определения величины воздействия фортификационного оборудования на живучесть точечных объектов системы управления войсками (силами), который основывается на методике оценки живучести войсковых объектов. Особенность способа заключается в учете конфигурации зоны поражения точечных объектов системы управления войсками (силами), предполагаемой траектории полета и кругового рассеивания боеприпасов при прицельном воздействии на них средств поражения противника.

Рассматриваемый способ позволяет определять величину воздействия фортификационного оборудования на живучесть точечных объектов системы управления войсками (силами), в соответствии с которой определяется очередность его выполнения. Повышается способность войсковых объектов выполнять боевые задачи согласно штатного предназначения во время ведения боевых действий в условиях воздействия современных средств поражения противника на фортификационное оборудование районов (позиций) войск (сил).

*Предложенный способ может использоваться для прогнозирования величины воздействия фортификационного оборудования на живучесть войск и объектов, а также во время проведения исследований, направленных на обоснование нужного состава инженерно-позиционных, инженерно-технических подразделений и подразделений оборудования пунктов управления.*

**Ключевые слова:** инженерное обеспечение; живучесть войск; фортификационное оборудование.

**METHOD OF DETERMINING THE MAGNITUDE OF THE EFFECT OF FORTIFICATION EQUIPMENT ON THE SURVIVABILITY OF THE TROOPS (FORCES) CONTROL SYSTEM IN THE OPERATIONS (COMBAT ACTIONS)**

*Vasyl Shevchenko*

*Oleksandr Voloshchenko (Candidate of the Military Science)*

*Oleksandr Bobrun (Candidate of the Military Science)*

*Central Research Institute of the Armed Forces of Ukraine*

*In the article it is about method of determining the magnitude of the effect of fortification equipment on the survivability of the troops (forces) control system based on the theory of survivability evaluation of point military objects when aiming enemy fire.*

*It is noted that characteristic of the method of determining the magnitude of the effect of fortification equipment on the survivability of the troops (forces) is the consideration of configuration of the affected area of individual elements (objects) of the troops (forces) control system, possible trajectory of flight and circular dispersion of ammunition during sighting action on them by the means of defeating the enemy.*

*It is confirmed that proposed method of determining the magnitude of the effect of fortification equipment on the survivability of the troops (forces) control system allows to determine the sequence of actions during fortification equipment of these objects, that allow to hide as soon as possible these objects in the field fortifications and significantly complicate their detection, identification and damage during combat actions.*

*It is noted that proposed method can be used for current forecasting of the magnitude of the effect of fortification equipment on the survivability of the troops (forces) control system and also during research on issues of survivability of the troops in modern armed conflicts.*

**Key words:** control system, survivability, fortification equipment.

**References**

1. **Shevchuk A.B.** Fortification of positions and areas in local wars and armed conflicts. A.B. Shevchuk. – M.: Voenizdat, 1999. – 104 p.
2. **Yurkov B.N.** Operations research. B.N. Yurkov. – M.: VIA, 1990. – 205 p.



Юрій Євгенович Репіло (доктор військових наук, професор)<sup>1</sup>  
 Андрій Іванович Мостовий<sup>2</sup>

<sup>1</sup>Національний університет оборони України імені Івана Черняхівського, Київ, Україна

<sup>2</sup>Національна академія Державної прикордонної служби України ім. Б. Хмельницького, Україна

## АНАЛІЗ ПРИКОРДОННОЇ БЕЗПЕКИ НА СХОДІ УКРАЇНИ ТА ОСОБЛИВОСТІ ЇЇ ЗАБЕЗПЕЧЕННЯ СИЛАМИ ТА ЗАСОБАМИ ПРИКОРДОННИХ ЗАГОНІВ В РАЙОНІ ОПЕРАЦІЇ ОБ'ЄДНАНИХ СИЛ

У науковій статті узагальнено основні загрози національній безпеці, надано характеристику операції Об'єднаних сил на сході України, прикордонній безпеці та розкрито особливості застосування сил та засобів прикордонних загонів Державної прикордонної служби України в районі проведення зазначеної операції. Узагальнено комплекс заходів, що проводяться прикордонними загонами Державної прикордонної служби України для протидії загрозам і викликам, що негативно впливають на стан прикордонної безпеки. Надано класифікацію кодів ускладнення обстановки та систематизовано за важливістю значень цифрові індекси кожного типу можливих небезпек на ділянці відповідальності прикордонних загонів.

Встановлено, що в умовах ускладнення обстановки функціонування прикордонних загонів в районі операції об'єднаних сил буде характеризуватись «зеленим» інформаційним кодом за рівнями ускладнення від «4» до «1», де: «4» – для реагування достатньо чергових сил та засобів прикордонного загону; «3» – потребує застосування резерву першої черги та чергових сил та засобів сусідніх прикордонних загонів; «2» – потребує застосування резерву другої черги та резерву першої черги сусідніх прикордонних загонів; «1» – потребує застосування усіх наявних ресурсів, а також резервів сусідніх прикордонних загонів.

**Ключові слова:** прикордонна безпека; операція Об'єднаних сил; прикордонний загін; обстановка.

### Вступ

Державна прикордонна служба (далі – ДПС) України у взаємодії з іншими суб'єктами забезпечення прикордонної безпеки, повноваження яких пов'язані з охороною та захистом державного кордону, продовжує здійснювати комплекс заходів щодо протидії усім загрозам державного суверенітету і територіальній цілісності України. Однак, трансформаційні процеси, що відбуваються в сучасному світі, зумовили появу нових загроз прикордонній безпеці України. Тому, вирішення проблемних питань щодо забезпечення прикордонної безпеки набуває дедалі більшої актуальності в загальному процесі пов'язаного з агресивною політикою Російської Федерації (далі – РФ) проти України, посиленням впливу проросійських центрів сил, наявністю сепаратистських настроїв у прикордонних регіонах України та Росії, що мають наміри переглянути належність частини державної території України та інше.

**Постановка проблеми.** Пріоритетність та масштабність завдань ДПС України щодо підвищення ефективності її діяльності і адекватної протидії загрозам прикордонній безпеці зумовлюють необхідність впровадження новітніх технологій охорони, покращення координації та взаємодії між суб'єктами забезпечення прикордонної безпеки та інші заходів, зокрема, удосконалення способів та методів застосування

сил та засобів прикордонних загонів для забезпечення прикордонної безпеки в районі операції об'єднаних сил (далі – ООС) на сході України [1]. У даному контексті, дослідження прикордонної безпеки на сході України та особливості її забезпечення силами та засобами прикордонних загонів в районі ООС є актуальним на національному, регіональному та міжнародному безпекових аспектах.

**Аналіз остатніх досліджень і публікацій.** Результати аналізу наукових праць свідчать, що питання щодо застосування сил та засобів прикордонних загонів в районі проведення ООС досліджувались у незначній кількості наукових праць. Розгляду науково-теоретичних та прикладних аспектів у сфері захисту та охорони державного кордону України присвячені дослідження [2–7]: В. О. Назаренка, О. А. Бінковського, Ю. Б. Івашкова, І. С. Катеринчука, В. А. Кириленка, Д. А. Купрієнка, М. М. Литвина, А. В. Махнюка, А. Б. Мисика, В. М. Серватюка, та ін. Водночас, попри значний інтерес до означеної проблематики, комплексних досліджень питань забезпечення прикордонної безпеки України силами та засобами прикордонних загонів в районі проведення ООС практично відсутні, що обумовлює необхідність у проведенні подальших наукових досліджень.

**Метою статті** є аналіз прикордонної безпеки на сході України та особливості її забезпечення силами та засобами прикордонних загонів в районі ООС.

## Виклад основного матеріалу дослідження

Основними загрозами національної безпеки на сході України є [1; 8–10]: військова агресія з боку РФ, участь регулярних військ, російських військових радників, інструкторів та найманців у бойових діях в окремих районах Донецької та Луганської областей; терористична загроза: переміщення на територію України членів терористичних угруповань, підрозділів сил спеціальних операцій збройних сил РФ, зброї, боєприпасів, засобів диверсій та терору, фінансування тероризму та екстремістських рухів в Україні з території окремих районів Донецької та Луганської областей, а також з території РФ; інформаційна загроза, пов'язана з переміщенням з РФ пропагандистських матеріалів антиукраїнського характеру та радикально налаштованих осіб, які намагаються дестабілізувати соціально-політичну обстановку та дискредитувати діяльність української влади; організована транскордонна злочинність у сферах незаконного переміщення осіб, наркотичних та психотропних речовин; незаконна міграція громадян країн Близького та Середнього сходу, Південно-східної Азії до країн Європейського союзу, як на організованих каналах незаконної міграції, так і на легальних каналах виїзду в Україну; торгівля людьми, як до Туреччини, Греції, Кіпру та країн арабського світу через пункти пропуску для авіаційного сполучення в Україні, так і до РФ залізничним та автомобільним сполученням; активна діяльність протиправних груп з незаконного переміщення товарів, стійкою пособницькою базою серед місцевих жителів.

З метою протидії загрозам національній безпеці, стабілізації ситуації, відновлення територіальної цілісності України та соціальне відродження східного регіону України 30 квітня 2018 року на окремих територіях Донецької та Луганської областей України розпочалась ООС [9].

Особливістю ООС на сході України є те, що Рішення про початок та завершення ООС приймає президент України, тоді як безпосереднє керівництво операцією та прийняття усіх рішень в рамках операції покладається на командувача Об'єднаного оперативного штабу Збройних сил (далі – ЗС). Таким чином, повноваження з керування військовими і правоохоронними підрозділами перейшло до Генерального штабу ЗС України. Командувач об'єднаних сил керує всіма військовими та правоохоронними підрозділами залученими до виконання із оборони та відсічі збройної російської агресії на сході України.

З початком ООС вводяться поняття «райони бойових дій» та «зони безпеки». Зокрема, під «районами бойових дій» маються на увазі території, охоплені бойовими діями уздовж лінії зіткнення, де відповідні військові та правоохоронні підрозділи виконують завдання із недопущення прориву ворога далі на територію України. Водночас «зони безпеки» тепер будуть розташовані на контрольованих Україною

територіях поруч з лінією розмежування на сході України, а їх межі визначатиме начальник Генштабу за поданням керівника об'єднаних сил. Крім того, в «зоні безпеки» можуть створюватися «райони обмеженого доступу» та «райони забороненого доступу», куди можна потрапити лише за спеціальними дозволами залежно від рівня допуску. Крім того, в «зонах безпеки» можуть вводитися різні режими перебування: зелений (без обмежень перебування та переміщення), жовтий (перебування та переміщення дозволене за наявності документів, допускається особистий огляд громадян, їхнього транспорту та речей) та червоний (перебування частково обмежене чи заборонене взагалі, пропуск громадян та посадових осіб дозволяється лише за наявності пропуску, транспорт та громадяни на окремі ділянки взагалі не допускаються).

З метою забезпечення безпекового простору та його режиму в районі проведення ООС України реалізується прикордонна політика у сфері захисту й охорони державного кордону, суверенних прав у виключній (морській) економічній зоні та континентального шельфу у [8].

Основними завданнями прикордонної політики України є: створення умов для забезпечення суверенітету і територіальної цілісності України, її прикордонної безпеки; удосконалення міжнародно-правового оформлення державного кордону; запобігання воєнній небезпеці, кризам і конфліктам у прикордонному просторі України; адекватне реагування на зміни рівня транскордонного співробітництва із суміжними державами» [10].

Основною складовою національної безпеки України є прикордонна безпека, яка характеризується ступенем захищеності територіальної цілісності та суверенітету держави, усіх сфер громадського життя і людської діяльності, прав та свобод громадян у прикордонному просторі, у зв'язку з чим досягається своєчасне виявлення, запобігання, нейтралізація реальних (потенційних) внутрішніх і зовнішніх загроз та забезпечується сталий розвиток прикордонних територій, транспарентність державного кордону для здійснення прикордонної діяльності та подорожування осіб [7; 9]. Така характеристика прикордонної безпеки дозволяє класифікувати її на три групи.

До першої групи слід віднести загрози, більшою мірою, впливають на становище держави в міжнародному співтоваристві. Вони не представляють серйозної небезпеки, але сильна країна не має права дозволяти навіть незначні правопорушення на своєму кордоні.

Друга група загроз являють собою правопорушення, здатні дестабілізувати обстановку у прикордонні і завдати їй певний матеріальний збиток.

Третя група загроз здатна не тільки загострити обстановку на кордоні і спричинити за собою значні матеріальні збитки, але і вплинути на безпеку країни в цілому.

Результати аналізу реальних та потенційних

загроз в районі проведення ООС свідчать про такі сталі тенденції, як:

довготривала агресія з боку РФ та контрольованих нею тимчасово окупованих окремих районів Луганської та Донецької областей;

продовжуються спроби ворожих спецслужб утворити в Україні низку незаконних організацій для посягання на її територіальну цілісність і державний суверенітет, дестабілізації суспільно-політичної та соціально-економічної обстановки.

незаконне переміщення через державний кордон України зброї, а також економічної контрабанди;

діяльність транснаціональних і транскордонних злочинних груп набуває все більшої організованості. При цьому найбільшу актуальність мають: неконтрольована міграція, торгівля людьми та їх органами, незаконний обіг зброї, боєприпасів і інших засобів терору, наркотичних засобів та їх прекурсорів, контрафактних товарів тощо.

З метою протидії загрозам і викликам, що негативно впливають на стан прикордонної безпеки України ДПС через підпорядковані прикордонні загоны здійснює комплекс заходів, а саме:

участь в обороні лінії зіткнення, відсічі збройної агресії на підконтрольну українській владі територію;

здійснення в установленому порядку пропуску осіб, транспортних засобів, вантажів через лінію зіткнення у встановлених контрольних пунктах в'їзду-виїзду (далі – КПВВ) та здійснення прикордонного контролю в ППР;

протидія протиправній діяльності в смузі безпеки та іншим правопорушенням законодавства України з прикордонних питань;

проведення заходів протидії диверсійно-розвідувальним силам противника, незаконним збройним формуванням, терористичним групам, які намагаються діяти через державний кордон;

посилення охорони визначених важливих об'єктів та комунікацій;

ведення оперативно-розшукової діяльності в інтересах забезпечення захисту суверенітету згідно із Законом України;

виконання доручень правоохоронних органів щодо осіб, які перетинають лінію зіткнення;

координація діяльності контрольних органів, що здійснюють різні види контролю при перетинанні лінії зіткнення або беруть участь у забезпеченні прикордонного режиму і режиму в КПВВ;

підтримання високого рівня боєготовності, організованості, статутного порядку та дисципліни.

Військовослужбовцям прикордонних загонів ДПС в районі проведення ООС законодавством України надано спеціальні повноваження:

перевіряти у громадян і посадових осіб документи, що посвідчують особу, а в разі відсутності документів – затримувати їх для встановлення особи;

застосовувати в разі крайньої необхідності зброю і спеціальні засоби до осіб, які вчинили або вчиняють

правопорушення чи інші дії, що перешкоджають виконанню законних вимог осіб, залучених до виконання заходів із забезпечення національної безпеки і оборони, відсічі та стримування збройної агресії РФ в Донецькій та Луганській областях, або дії, пов'язані з несанкціонованою спробою проникнення в район здійснення зазначених заходів;

затримувати і доставляти осіб до органів Національної поліції України;

здійснювати особистий огляд громадян, їхніх речей, транспортних засобів та речей, які вони перевозять;

тимчасово обмежувати або забороняти рух транспортних засобів і пішоходів на вулицях та дорогах, не допускати транспортних засобів, громадян на окремі ділянки місцевості та об'єкти, виводити громадян з окремих ділянок місцевості та об'єктів, відбуксировувати транспортні засоби;

заходити (проникати) в житлові та інші приміщення, на земельні ділянки, що належать громадянам, на територію та в приміщення підприємств, установ і організацій, перевіряти транспортні засоби;

використовувати із службовою метою засоби зв'язку і транспортні засоби, в тому числі спеціальні, що належать громадянам (за їхньою згодою), підприємствам, установам та організаціям, крім транспортних засобів дипломатичних, консульських та інших представництв іноземних держав та міжнародних організацій.

Роль прикордонних загонів в ООС по відношенню до завдань функціонування та процесу досягнення ними встановленої ефективності [11] полягає у створенні в контрольованих прикордонних районах належних умов, які б унеможливили реалізацію загроз та поширення їх наслідків углиб держави.

Особливості діяльності прикордонних загонів, їх місце, можливі форми і способи застосування визначаються положенням сторін, напрямками дій противника, завданнями ООС, динамікою обстановки тощо.

Діяльність прикордонних загонів в ООС характеризується специфічним спрямуванням, а саме: відбиття збройного вторгнення; прискання озброєних та інших провокацій; захист ділянки відповідальності прикордонного загону від злочинних посягань; недопущення перетину лінії розмежування поза КПВВ; пошук, виявлення та затримання правопорушників; підтримка режиму, прикордонного режиму, режиму в КПВВ, режиму особливого періоду тощо. Крім того, прикордонні загоны проводять комплекс заходів з викриття підготовки противника до агресії, виявлення диверсійно-розвідувальних груп, інших підрозділів спеціального призначення противника, ознак нарощування його агентурної та диверсійно-розвідувальної діяльності.

Особливості застосування прикордонних загонів в районі проведення ООС можна проаналізувати на основі інформаційних кодів, класифікація яких за окремими небезпеками представлена у таблиці 1 [12].

Класифікація колірнього коду ускладнення обстановки за окремими небезпеками на ділянці прикордонних загонів в районі ООС

Значення колірнього коду та типу небезпек	Основні реальні та потенційні загрози прикордонної безпеки в районі ООС	Основні завдання прикордонних загонів з протидії реальним та потенційним загрозам в районі ООС
<b>«червоний»</b>	- посягання на державний суверенітет України та її територіальну цілісність, територіальні претензії з боку інших держав; - РПД іноземних спецслужб; - можливість втягування України в регіональні збройні конфлікти чи у протистояння з іншими державами;	- здійснює ОДК на суші, морі, річках, озерах та інших водоймах, припиняє спроби незаконної зміни проходження державного кордону України; - у взаємодії з підрозділами військових формувань України, правоохоронних органів припиняє збройні конфлікти та провокації на кордоні, бере участь у відбитті вторгнення або нападу на територію України збройних сил іншої держави або груп держав тощо.
військово-політичні небезпеки		
<b>«білий»</b>	- можливість незаконного ввезення в країну зброї, боєприпасів, вибухових речовин і засобів масового ураження, радіоактивних і наркотичних засобів через пункти пропуску (КППВ); - нелегальна міграція на шляхах міжнародного сполучення;	- здійснює контроль за дотриманням режиму державного кордону та режиму в КППВ; - здійснює виявлення в КППВ осіб, які переховуються від органів досудового розслідування, слідчого судді та суду, ухиляються від відбуття кримінальних покарань, та виконання в установленому порядку інших доручень уповноважених державних органів тощо.
трансграничні небезпеки		
<b>«зелений»</b>	- можливість незаконного ввезення в країну зброї, боєприпасів, вибухових речовин і засобів масового ураження, радіоактивних і наркотичних засобів поза ППР; - нелегальна міграція; - незавершеність договірно-правового оформлення ДК;	- здійснює контроль за дотриманням режиму держ. кордону та прикордонного режиму в прикордонній смузі та контрольованому прикордонному районі; - бере участь у проведенні прикордонних (спільних) операцій, здійснює спеціальні дії щодо пошуку порушників законодавства України з прикордонних питань; - на основі аналізу ризиків у сфері прикордонної безпеки здійснює протидію нелегальній міграції, торгівлі людьми, незаконному переміщенню осіб, зброї, наркотичних засобів, психотропних речовин і прекурсорів, боєприпасів, вибухових, отруйних, радіоактивних речовин та інших предметів, заборонених до переміщення через держ. кордон та до тимчасово окупованої території і з неї, порушенням порядку в'їзду на тимчасово окуповану територію України та виїзду з неї тощо.
прикордонні небезпеки		

В цифровому індексі кожного типу небезпек узагальнюється ступінь важливості значення події чи загрози ускладнення обстановки на ділянці відповідальності прикордонних загонів (див. табл. 2).

Динаміка і масштаби ускладнення обстановки можуть поєднувати різні типи небезпек, тому цифровий індекс ступеня найскладнішого із них буде обумовлювати загальний інформаційний код.

Таблиця 2

Класифікація цифрових індексів ступеня небезпек на ділянці прикордонних загонів в районі ООС

Цифровий індекс	Вагове значення	Короткий опис небезпек
I	<i>катастрофічне</i>	- реальна загроза життю (загибель); - безпека суспільства і держави під загрозою; - неможливість забезпечити безпеки діяльності; - повне підпадання підрозділу під вплив небезпечних чинників; - суцільне знищення (втрата) засобів, пунктів, об'єктів та систем в зоні небезпеки; - неможливість подальших дій, функціонування чи застосування; - потреба в повному переорієнтуванні діяльності;
II	<i>критичне</i>	- потенційна загроза життю і здоров'ю (серйозні травми, захворювання); - суттєвий підрив інтересів суспільства і держави; - значне підпадання підрозділу під вплив небезпечних чинників; - значне порушення умов життєдіяльності; - значне ушкодження засобів, пунктів, об'єктів та систем в зоні небезпеки; - для здійснення подальших дій, функціонування чи застосування потрібні значні ресурси та зусилля тощо;

Цифровий індекс	Вагове значення	Короткий опис небезпек
III	<i>граничне</i>	- суттєва загроза здоров'ю (травми, захворювання); - загроза окремим інтересам суспільства і держави; - суттєве підпадання підрозділу під вплив небезпечних чинників; - певні порушення умов життєдіяльності; - суттєве ушкодження засобів, пунктів, об'єктів та систем в зоні небезпеки; - для здійснення подальших дій, функціонування чи застосування потрібні певні ресурси та зусилля тощо;
IV	<i>незначне</i>	- незначна загроза здоров'ю; - часткове підпадання підрозділу під вплив небезпечних чинників; - умови життєдіяльності дозволяють безпечно виконувати покладені завдання; - часткове ушкодження засобів, пунктів, об'єктів та систем в зоні небезпеки; - для здійснення подальших дій, функціонування чи застосування достатньо наявних ресурсів; - загалом немає потреби в переорієнтуванні діяльності, зосередження зусиль на інших напрямках (заходах) та інше.

### Висновки й перспективи подальших досліджень

Таким чином, на основі аналізу прикордонної безпеки на сході України узагальнено значущі чинники, що впливають на неї та надано загальну характеристику ООС.

Узагальнено завдання та розкрито основні аспекти і особливості застосування сил та засобів прикордонних загонів ДПС України для забезпечення прикордонної безпеки в районі проведення ООС.

Встановлено, що функціонування прикордонних загонів в районі ООС в умовах ускладнення обстановки буде характеризуватись «зеленим» інформаційним кодом і відповідними цифровими

індексами – від чотирьох до одного, який визначає необхідність застосування наступних: «4» – для реагування достатньо чергових сил та засобів прикордонного загону; «3» – рівень ускладнення обстановки потребує застосування резерву першої черги та чергових сил та засобів сусідніх прикордонних загонів; «2» – рівень ускладнення обстановки потребує застосування резерву другої черги та резерву першої черги сусідніх прикордонних загонів; «1» – суттєвий рівень ускладнення обстановки, який потребує застосування усіх наявних ресурсів підрозділу, а також резервів прикордонного загону та сусідніх з ним загонами.

### Література

1. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2018 році»: НІСД. Київ, 2018. 688 с. 2. Назаренко В. О. Безпека європейських кордонів: український вимір: Науковий вісник Державної прикордонної служби. № 1, 2008. С. 3–8. 3. Біньковський О. А. Сучасні підходи до розвитку системи пропуску через державний кордон осіб і транспортних засобів / Актуальні питання прикордонної безпеки. Сучасний стан та перспективи розвитку. 2011. № 2. С. 37–43. 4. Кириленко В. А. Загрози національній безпеці держави в прикордонній сфері та їх інформаційні ознаки: зб. наук. пр. № 43. Хмельницький: НА ДПСУ, 2008. С. 616. 5. Мисик А. Б., Купрієнко Д. А. Модель системи підтримки прийняття рішень на проведення спільних (міжнародних) прикордонних операцій: зб. наук. пр. Хмельницький: НА ДПСУ, 2016. № 24, ч. ІС. 12–26. 6. Литвин М. М. Прикордонна безпека України: етапи становлення, проблеми і перспективи // Національна безпека: український вимір: шокв. наук. зб. / Рада нац. безпеки і оборони України, Ін-т пробл. нац. безпеки; редкол.: Горбулін В.П. (голов. ред.) [та ін.], К., 2008. Вип. 1-2 (20-21), 41–46 с. 7. Серватюк В. М.

Основні підходи до оцінки регіональної стабільності у прикордонному просторі: зб. наук. пр. № 12, ч. 2. Хмельницький: НА ПВУ, 2000. С. 28–36. 8. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради України. Київ, 2018. № 31. Ст. 241. 9. Концептуальні засади розвитку системи забезпечення національної безпеки України: аналіт. доп. URL: [http://www.niss.gov.ua/content/articles/files/nac\\_bezp182c8.pdf](http://www.niss.gov.ua/content/articles/files/nac_bezp182c8.pdf) (дата звернення: 30.03.2020 р.). 10. Ставицький О. М., Мостовий А. І. Оцінка стану прикордонної безпеки за визначеними індикаторами: зб. наук. пр. Хмельницький: НА ДПСУ, 2018. № 1 (75) С. 231–242. 11. Майстренко О.В., Репіло Ю.Є., Демидко Д.Л. Пропозиції по уточненню понятійного апарату дослідження явищ та процесів: військовий аспект: Сучасні інформаційні технології у сфері безпеки та оборони, №3(24)/2015, С. 161–165. 12. Кириленко В. А., Городнов В. П., Каратаєв Р. Г. Загрози національній безпеці держави в прикордонній сфері та їх інформаційні ознаки: зб. наук. пр. № 43. Балашов В. О. Хмельницький: НА ДПСУ, 2008. С. 616.

### АНАЛИЗ ПОГРАНИЧНОЙ БЕЗОПАСНОСТИ НА ВОСТОКЕ УКРАИНЫ И ОСОБЕННОСТИ ЕЕ ОБЕСПЕЧЕНИЯ СИЛАМИ И СРЕДСТВАМИ ПОГРАНИЧНЫХ ОТРЯДОВ В РАЙОНЕ ПРОВЕДЕНИЯ ОПЕРАЦИИ ОБЪЕДИНЕННЫХ СИЛ

Юрий Евгеньевич Репило (доктор военных наук, профессор)<sup>1</sup>  
Андрей Иванович Мостовый<sup>2</sup>

<sup>1</sup>Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

<sup>2</sup>Национальная академия Государственной пограничной службы Украины им. Б. Хмельницкого, Украина

В научной статье обобщены основные угрозы национальной безопасности, подана характеристика операции Объединенных сил на востоке Украины, пограничной безопасности и раскрыты особенности применения сил и средств пограничных отрядов Государственной пограничной службы Украины в районе проведения указанной операции. Обобщен комплекс средств, которые проводятся пограничными отрядами Государственной пограничной службы Украины для противодействия угрозам и вызовам, что негативно влияют на состояние пограничной безопасности. Дана классификация кодов обострения обстановки и систематизированы по важности значений цифровые индексы каждого типа возможных угроз на участке ответственности пограничных отрядов.

Установлено, что в условиях обострения обстановки работа пограничных отрядов в районе проведения операции Объединенных сил будет выражаться «зеленым» информационным кодом по уровням осложнения от «4» до «1», где: «4» – для реагирования достаточно дежурных сил и средств пограничного отряда; «3» – требует применения резерва первой очереди и дежурных сил и средств соседних пограничных отрядов; «2» – требует применения резерва второй очереди и резерва первой очереди соседних пограничных отрядов; «1» – требует применения всех имеющихся ресурсов, а также резервов соседних пограничных отрядов.

**Ключевые слова:** пограничная безопасность; операция Объединенных сил; пограничный отряд; обстановка.

## BORDER SECURITY ANALYSIS IN EASTERN UKRAINE AND PECULIARITIES OF PROVIDING IT BY FORCES AND FACILITIES OF BORDER GUARD DETACHMENTS IN THE AREA OF JOINT FORCES OPERATION

*Iurii Repilo (Doctor of military sciences, Professor)<sup>1</sup>  
Andrii Mostovyi<sup>2</sup>*

<sup>1</sup>*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

<sup>2</sup>*National Academy of State Border Guard Service of Ukraine named after B. Khmelnytsky, Ukraine*

The scientific article summarizes the main threats to national security, describes the operation of the Joint Forces in eastern Ukraine, border security and reveals the peculiarities of using forces and facilities of border guard detachments of the State Border Guard Service of Ukraine in the area of the aforementioned operation. The complex of actions carried out by border guard detachments of the State Border Guard Service of Ukraine to counter threats and challenges that negatively affect the state of border security was summarized. The classification of codes for the situational aggravations is given and the indexes of each type of possible danger in the area of responsibility of the border guard detachments are organized according to the importance of values.

It is established that in conditions of aggravation of the situation for functioning of the border guard detachments in the area of the Joint Forces operation will be characterized by a "green" information code at the levels of aggravation from "4" to "1", where: "4" – to react it is enough regular forces and facilities of a border guard detachment; "3" – it is necessary to deploy the Ready Reserve and the standby forces of neighbouring border guard detachments; "2" – it is necessary to deploy the Standby Reserve and the Standby Reserve of neighbouring border guard detachments; "1" – it is necessary to deploy all available resources, as well as the reserves of neighbouring border guard detachments.

**Keywords:** border security; Joint Forces operation; border guard detachment; situation.

### References

1. Analitichna dopovid do Shchorichnoho Poslannia Prezydenta Ukrainy do Verkhovnoi Rady Ukrainy «Pro vnutrishnie ta zovnishnie stanovyshche Ukrainy v 2018 rotsi»: NISD. Kyiv, 2018. 688 s.
2. Nazarenko V. O. Bezpeka yevropeyskykh kordoniv: ukrainskyi vymir: Naukovyi visnyk Derzhavnoi prykordonnoi sluzhby. № 1, 2008. S. 3–8.
3. Binkovskiy O. A. Suchasni pidkhody do rozvytku systemy propusku cherez derzhavnyi kordon osib i transportnykh zasobiv / Aktualni pytannia prykordonnoi bezpeky. Suchasnyi stan ta perspektyvy rozvytku. 2011. № 2. S. 37–43.
4. Kyrylenko V. A. Zahrozy natsionalnoi bezpeky derzhavy v prykordonnii sferi ta yikh informatsiini oznaky: zb. nauk. pr. № 43. Khmelnytskyi: NA DPSU, 2008. S. 616.
5. Mysyk A. B., Kupriienko D. A. Model systemy pidtrymky pryiniattia rishen na provedennia spilnykh (mizhnarodnykh) prykordonnykh operatsii: zb. nauk. pr. Khmelnytskyi: NADPSU, 2016. № 24, ch. I. S. 12–26.
6. Lytvyn M. M. Prykordonna bezpeka Ukrainy: etapy stanovlennia, problemy i perspektyvy // Natsionalna bezpeka: ukrainskyi vymir: shchokv. nauk. zb. / Rada nats. bezpeky i oborony Ukrainy, In-t probl. nats. bezpeky; redkol.: Horbulin V.P. (holov. red.) [ta in.]. K., 2008. Vyp. 1-2 (20-21). 41–46 s.
7. Servatiuk V. M. Osnovni pidkhody do otsinky rehionalnoi stabilnosti u prykordonnomu prostori: zb. nauk. pr. № 12, ch. 2. Khmelnytskyi: NA PVU, 2000. S. 28–36.
8. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018 № 2469-VIII. Vidomosti Verkhovnoi Rady Ukrainy. Kyiv, 2018. № 31. St. 241.
9. Kontseptualni zasady rozvytku systemy zabezpechennia natsionalnoi bezpeky Ukrainy: analit. dop URL: [http://www.niss.gov.ua/content/articles/files/nac\\_bezip182c8.pdf](http://www.niss.gov.ua/content/articles/files/nac_bezip182c8.pdf)
10. Stavytskyi O. M., Mostovyi A. I. Otsinka stanu prykordonnoi bezpeky za vyznachenyimi indykatoramy: zb. nauk. pr. Khmelnytskyi: NA DPSU, 2018. № 1 (75) S. 231–242.
11. Maistrenko O.V., Repilo I.Y., Demydko D.L. Events and processes research conceptual structure refinement proposals: military aspect: Modern Information Technologies in the Sphere of Security and Defence, №3(24)/2015, P. 161–165.
12. Kyrylenko V. A., Horodnov V. P., Karataiev R. H. Zahrozy natsionalnoi bezpeky derzhavy v prykordonnii sferi ta yikh informatsiini oznaky: zb. nauk. pr. № 43. Balashov V. O. Khmelnytskyi: NA DPSU, 2008. S. 616.

Юрій Аркадійович Гусак (доктор військових наук, с.н.с.)

Василь Кузьмович Шевченко

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

## МЕТОДИЧНИЙ ПІДХІД ЩОДО АНАЛІЗУ ЖИВУЧОСТІ СИСТЕМИ ПУНКТІВ УПРАВЛІННЯ

У статті розглядається проблема аналізу живучості системи пунктів управління (ПУ) як одна із складових проблеми живучості військ (сил). При розгляді цієї проблеми здійснена декомпозиція системи пунктів управління ЗС України за рівнями системи управління військами та за структурою Збройних Сил (ЗС) України, а саме: на стратегічному рівні – система ПУ Головнокомандувача ЗС України; на оперативно-стратегічному рівні – системи ПУ командувача Об'єднаних сил, командувачів видів та окремих родів військ; на оперативному рівні – системи ПУ командувачів оперативних командувань та командирів повітряних командувань. Показано, що у наукових працях, присвячених проблемним питанням управління військами під час їх застосування, застосовуються моделі, які описують живучість тільки окремих ПУ. У зв'язку з цим, у статті запропоновано методичний підхід аналізу живучості системи ПУ, який базується на теорії імовірностей. Введено показники живучості – імовірність збереження працездатного стану системою ПУ на відповідному рівні та відповідно до виду, окремого роду військ та оперативного і повітряного командування. Методичний підхід до аналізу живучості системи ПУ дає можливість розрахувати імовірності збереження працездатного стану системою ПУ залежно від рівня управління. Для перевірки адекватності методичного підходу розглянуто типову структуру системи ПУ, яка складається з основного, запасного та резервного ПУ. Показано, що запропонований підхід не суперечить положенням теорії управління військами та дозволяє розробити методичку обґрунтування вимог до живучості системи пунктів управління ЗС України.

**Ключові слова:** система пунктів управління; методичний підхід до аналізу живучості.

### Вступ

**Постановка проблеми.** Система управління ЗС України складається з таких підсистем: пунктів управління органів військового управління та зв'язку і АСУВ. Забезпечення живучості системи управління Збройних Сил неможливе без забезпечення живучості підсистеми ПУ. При цьому, основне призначення системи пунктів управління (система ПУ) – забезпечення стійкого, безперервного та прихованого управління військами в умовах бойової обстановки [1].

В Збройних Силах була створена і функціонує розгалужена система стаціонарних, захищених та рухомих ПУ (в тому числі повітряних і морських), яка мала забезпечувати стійке і безперервне управління військами (силами) у визначених операційних зонах (районах) з урахуванням сучасних викликів і загроз національній безпеці України, як в мирний час, так і особливий період.

Застосування визначених військ у різних операційних зонах (районах) включає створення і

утримання розвиненої системи стаціонарних захищених і рухомих ПУ, яка забезпечить необхідний рівень її живучості.

Стаціонарні захищені ПУ забезпечують найбільш сприятливі умови для роботи оперативного складу, надійний зв'язок, захист людей від вогневого впливу противника.

Під час підготовки ЗС України до застосування здійснюються заходи із завчасної підготовки захищених ПУ, їх вузлів зв'язку та опорних мереж зв'язку. Саме стаціонарні захищені ПУ складають основу системи управління ЗС України на стратегічному і оперативному рівнях. Вони обладнуються завчасно в спеціально вибраних районах. В мирний час на них організовується бойове чергування черговими силами оперативного складу штабів і вузлів зв'язку, а в загрозливий і особливий періоди на цих пунктах розгортаються органи управління в повному складі. З них здійснюється управління військами

(силами) при відбитті нападу противника, веденні операцій і бойових дій на початку війни.

На рис. 1 зображено структуру системи пунктів управління ЗС України, яка включає в себе декілька підсистем ПУ різного рівня. Зазначена структура представляє собою досить складну розгалужену систему, оцінювання живучості якої в сучасних умовах є актуальним науковим завданням, яке потребує серйозного дослідження.

**Аналіз останніх досліджень і публікацій.** Питання живучості системи ПУ досить широко розглядаються у наукових працях. Разом з тим, методичні аспекти оцінювання живучості системно не розглядалися.

Зокрема, аналіз наукових праць [1]–[4], присвячених проблемним питанням живучості системи ПУ свідчить про те, що на даний час розроблені та використовуються моделі, які описують живучість окремих ПУ.

Однак математичних моделей, які б загалом описували живучість багаторівневої системи ПУ, нині немає.

**Метою статті** є розроблення методичного підходу, який дає можливість аналізувати живучість багаторівневої системи пунктів управління.

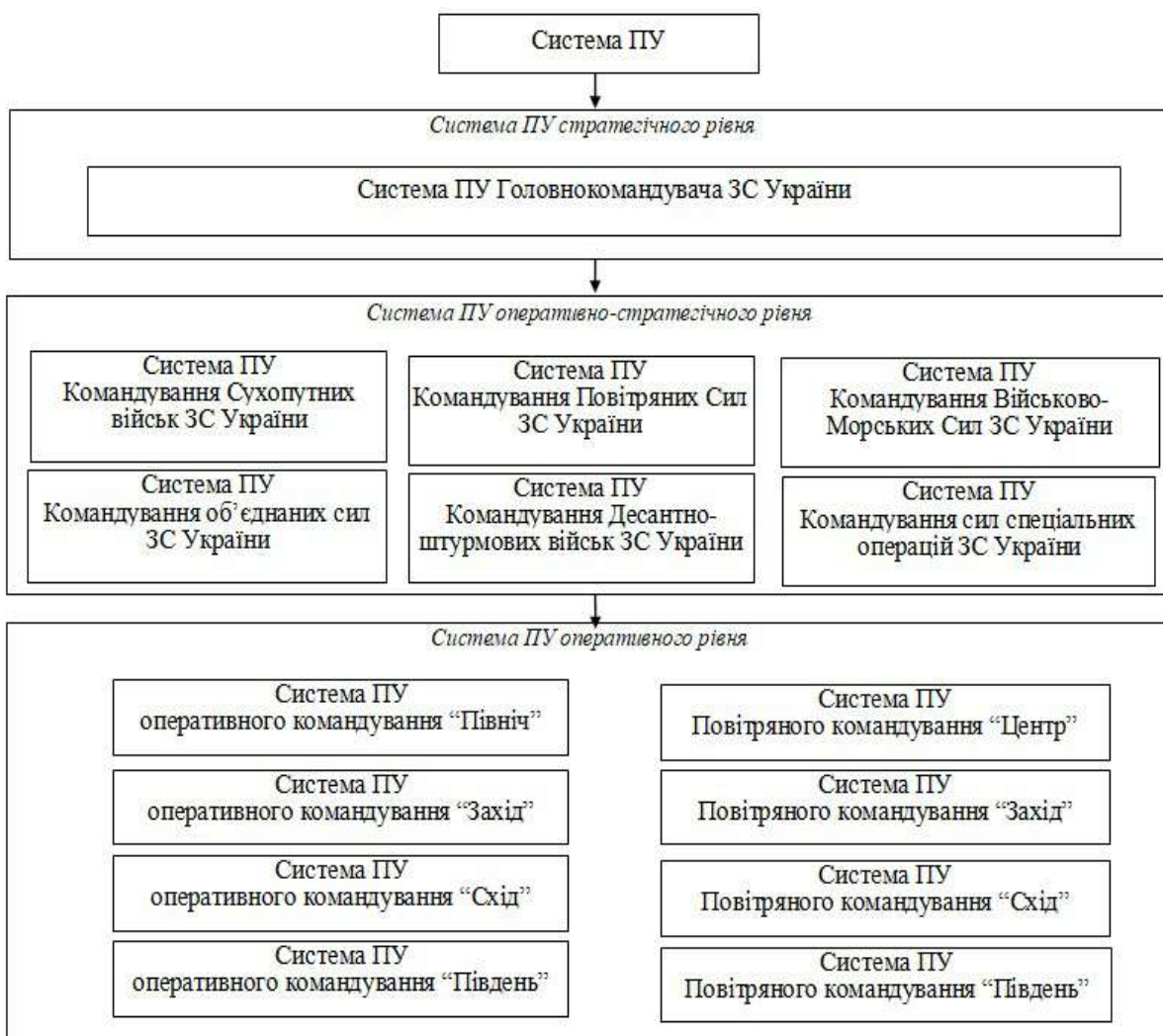


Рис. 1. Структура системи пунктів управління ЗС України

### Виклад основного матеріалу дослідження

У роботах [3] та [4] для оцінювання живучості ПУ під вогневим впливом противника введено імовірність виходу з ладу ПУ  $Q_{пу}$  та імовірність збереження працездатного стану  $P_{пу} = 1 - Q_{пу}$ .

Тоді імовірності збереження працездатного

стану складових системи пунктів управління ЗС України можуть бути визначені за подібними виразами.

Імовірність збереження працездатного стану системи ПУ Головнокомандувача ЗС України становитиме:

$$P_{ГК} = 1 - Q_{ГК} \quad (1)$$

Імовірності збереження працездатного стану



системами ПУ командування Об'єднаних сил, командувань видів ЗС України та окремих родів військ (десантно-штурмових військ і Сил спеціальних операцій) визначатимуться як:

$$P_{oc} = 1 - Q_{oc}, P_{св(пс, вмс)} = 1 - Q_{св(пс, вмс)},$$

$$P_{дшв(ссо)} = 1 - Q_{дшв(ссо)}. \quad (2)$$

Імовірності збереження працездатного стану системами ПУ оперативних (ОК) та повітряних (ПВК) командувань становитимуть:

$$P_{ок\ північ(захід, схід, південь)} = 1 - Q_{ок\ північ(захід, схід, південь)}, \quad (3)$$

$$P_{пвк\ північ(захід, схід, південь)} = 1 - Q_{пвк\ північ(захід, схід, південь)}. \quad (4)$$

Враховуючи (1)–(4) можна записати вирази для імовірностей збереження працездатного стану складових системи ПУ усіх рівнів.

Імовірність збереження працездатного стану системою ПУ стратегічного рівня:

$$P_{ср} = 1 - Q_{ср}, Q_{ср} = Q_{гк}. \quad (3)$$

Імовірність збереження працездатного стану системою ПУ оперативно-стратегічного рівня:

$$P_{оср} = 1 - Q_{оср},$$

$$Q_{оср} = Q_{св} \cdot Q_{пс} \cdot Q_{вмс} \cdot Q_{дшв} \cdot Q_{oc} \cdot Q_{ссо}. \quad (6)$$

Імовірність збереження працездатного стану

системою ПУ оперативного рівня:

$$P_{ор} = 1 - Q_{ор}, Q_{ор} = Q_{ок} \cdot Q_{пвк},$$

$$Q_{ок} = Q_{ок\ північ} \cdot Q_{ок\ захід} \cdot Q_{ок\ схід} \cdot Q_{ок\ південь},$$

$$Q_{пвк} = Q_{пвк\ північ} \cdot Q_{пвк\ захід} \cdot Q_{пвк\ схід} \cdot Q_{пвк\ південь}. \quad (3)$$

Тоді, використовуючи формулу повної імовірності для визначення імовірності збереження працездатного стану системою ПУ ЗС України, маємо:

$$P_{спу} = 1 - Q_{ср} \cdot Q_{оср} \cdot Q_{ор} =$$

$$= 1 - (1 - P_{ср}) \cdot (1 - P_{оср}) \cdot (1 - P_{ор}) = P_{ср} + P_{оср} + P_{ор} -$$

$$- P_{ср} \cdot P_{оср} - P_{ср} \cdot P_{ор} - P_{оср} \cdot P_{ор} + P_{ср} \cdot P_{оср} \cdot P_{ор}. \quad (8)$$

Схема визначення імовірностей збереження працездатного стану складовими системи пунктів управління ЗС України наведена на рис. 2.

Під час проведення операції вихід з ладу того чи іншого ПУ представляє собою випадковий процес. У роботі [5] показано, що для оцінювання живучості системи ПУ в умовах впливу противника можна застосувати математичний апарат теорії марковських процесів.

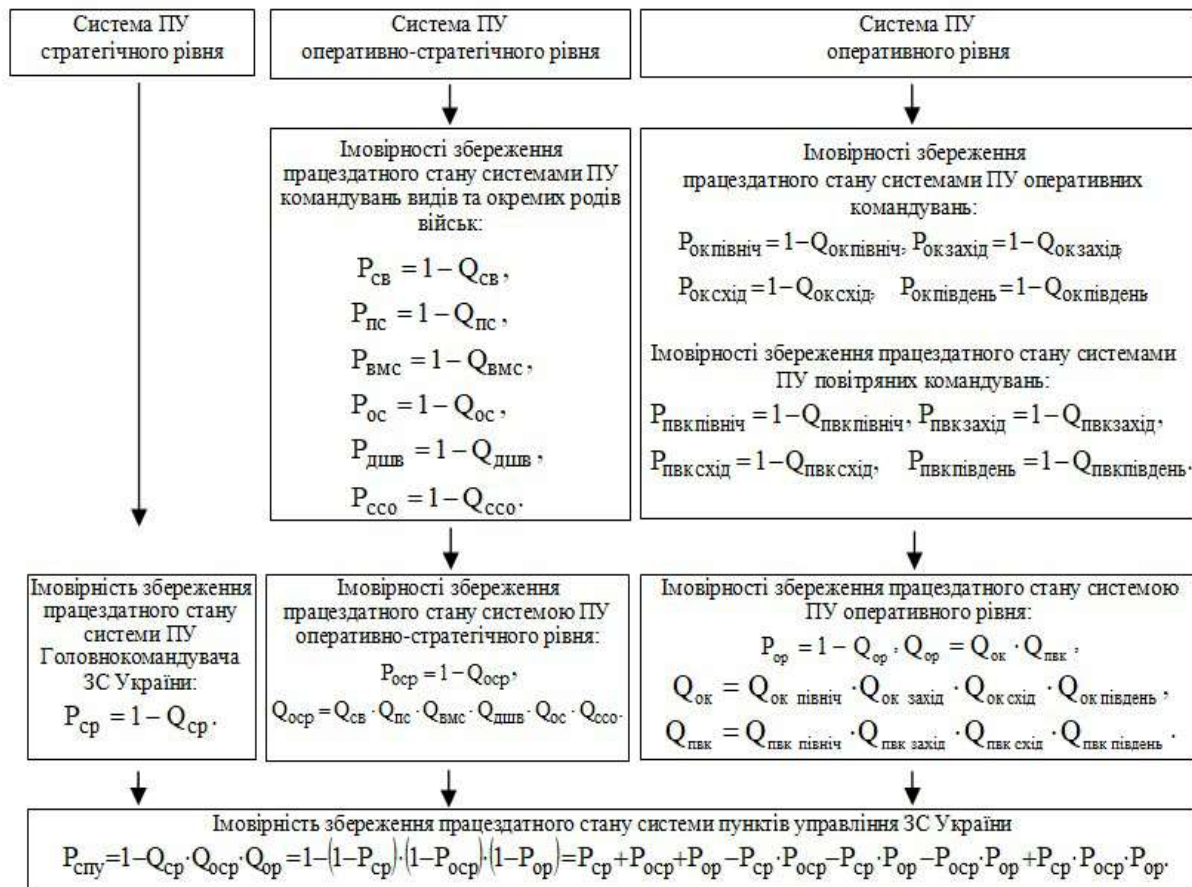


Рис. 2. Схема визначення імовірностей збереження працездатного стану складовими системи пунктів управління ЗС України

системи ПУ необхідно, щоб з усіх  $n$  ПУ здійснювалося безперервне управління військами. Для сталого функціонування системи ПУ завжди є запасні ПУ  $m$ , які можуть бути виведені з ладу під впливом противника, так само, як і основні ПУ, та резервні ПУ  $r$ , які з початку операції не функціонують і тому не можуть бути виведені з ладу противником. Якщо основні ПУ вийшли з ладу, то вони замінюються негайно запасними ПУ, а останні – з резерву.

У такому випадку під живучістю системи ПУ будемо розуміти властивість цієї системи зберігати або своєчасно відновлювати здатність забезпечувати управління військами з  $n$  ПУ в умовах впливу противника. При цьому система ПУ втрачає цю здатність, коли виведено з ладу більше, ніж  $m+r$  ПУ [5].

Позначимо через  $Q_k(t)$  імовірність того, що у момент  $t$  противником виведено з ладу  $k$  ПУ ( $0 \leq k \leq n+m+r$ ). Тоді живучість системи ПУ можна представити виразом [5]:

$$\alpha(t) = \sum_{k=0}^{m+r} Q_k(t) \quad (9)$$

де

$$Q_k(t) = \begin{cases} \frac{[\lambda(n+m)\tau]^k}{k!} Q(t)_0, & \text{якщо } 0 < k \leq r+1, \\ \frac{(\lambda\tau)^k (n+m)^{r+1} (n+m-1) \dots (n+m+r-k+1)}{k!} Q(t)_0, & \text{якщо } r+2 \leq k \leq n+m+r \end{cases}$$

– ймовірність виходу з ладу  $k$ -го ПУ ( $0 \leq k \leq n+m+r$ );

$\lambda$  – інтенсивність впливу противника.

$$Q_0 = \frac{1}{\sum_{k=0}^{n+m+r} \frac{\lambda_0 \lambda_1 \dots \lambda_{k-1}}{k!} \tau^k}$$
 – ймовірність того,

що  $n+m+r$  ПУ не вийдуть з ладу під впливом противника;

$\tau$  – математичне очікування часу відновлення ПУ;

$$\lambda_k = \begin{cases} \lambda(n+r), & \text{якщо } 0 < k \leq r, \\ \lambda(n+r+r-k), & \text{якщо } k > r \end{cases}$$

інтенсивність виходу з ладу  $k$ -го ПУ.

Системи ПУ, які входять до системи ПУ ЗС України мають типову структуру та складаються з основного ( $n = 1$ ), запасного ( $m = 1$ ) та резервного ( $r = 1$ ) ПУ. Тому розглянемо живучість такої системи ПУ.

Тоді, відповідно до виразу (9), живучість системи ПУ у стаціонарному режимі

$$\alpha = \sum_{k=0}^{m+r} Q_k = \sum_{k=0}^2 Q_k = Q_0 + Q_1 + Q_2, \quad (10)$$

$$\text{де } Q_k = \begin{cases} \frac{[2\lambda\tau]^k}{k!} Q_0, & \text{якщо } k = 1, \\ \frac{(\lambda\tau)^k 4(3-k+1)}{k!} Q_0, & \text{якщо } k = 2, \end{cases} \quad (11)$$

$$Q_0 = \frac{1}{\sum_{k=0}^3 \frac{\lambda_0 \lambda_1 \dots \lambda_{k-1}}{k!} \tau^k}, \quad (12)$$

$$\lambda_k = \begin{cases} 2\lambda & \text{якщо } k = 1, \\ (3-k)\lambda & \text{якщо } k = 2. \end{cases} \quad (13)$$

Тоді вираз для живучості системи ПУ прийме наступний вигляд:

$$\alpha = \frac{1 + 2\lambda\tau + (\lambda\tau)^2}{\sum_{k=0}^3 \frac{2(\lambda\tau)^k}{k!}}$$

Графік залежності живучості типової системи ПУ  $\alpha(\lambda)$  від інтенсивності виходу з ладу ПУ  $\lambda$  за умов  $n = 1$ ,  $m = 1$  та  $r = 1$  наведено на рис. 2, а за умов  $n = 1$ ,  $m = 2$  та  $r = 1$  – на рис. 3.

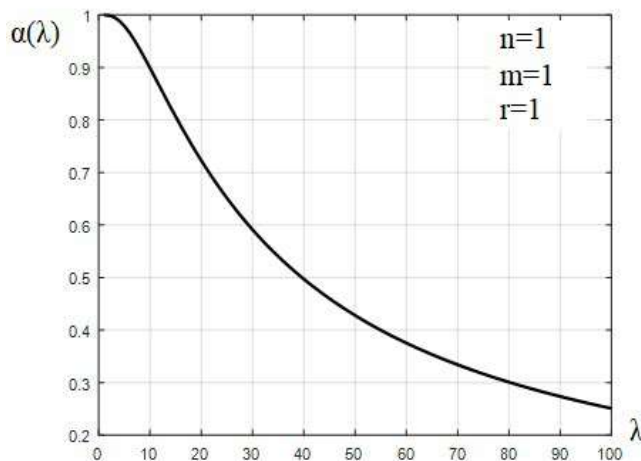


Рис. 2. Графік залежності  $\alpha$  від інтенсивності виходу з ладу ПУ (за умов  $n = 1$ ,  $m = 1$  та  $r = 1$ )

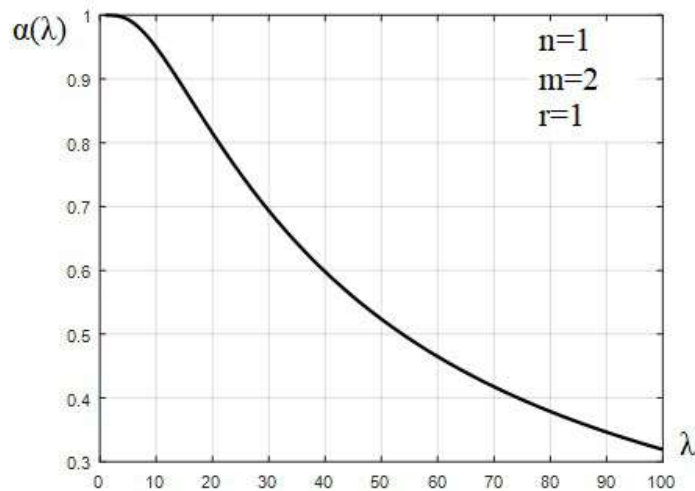


Рис. 3. Графік залежності  $\alpha$  від інтенсивності виходу з ладу ПУ  
(за умов  $n = 1$ ,  $m = 2$  та  $r = 1$ )

Аналіз графіків на рис. 2–3 показує, що живучість системи ПУ, яка складається з 4 ПУ ( $\alpha=0,33$ ), більша ніж у системи ПУ, яка складається з 3 ПУ ( $\alpha=0,26$ ).

Запропонований підхід щодо аналізу живучості системи ПУ адекватно описує залежність живучості типової системи ПУ від кількості ПУ та інтенсивності впливу противника і не суперечить положенням теорії управління військами.

На основі виразу (9) є можливість розрахувати живучість кожної складової системи ПУ ЗС України як ймовірності збереження працездатного стану системи ПУ відповідно до виразів (1)–(8).

### Література

1. Иванов Д. А., Савельев В. П., Шеманский П. В. Основы управления войсками в бою: изд. 2-е, перераб. и доп. Москва: Воениздат, 1977. 389 с. 2. Военный энциклопедический словарь. В 2 т. Москва: БРЭ, Риполклассик, 2001. 848 с. 3. Основы управления войсками / П. К. Алтухов, И. А. Афонский, И. В., Рыболовский, А. Е. Татарченко; под ред.

П. К. Алтухова. Москва, Воениздат, 1984. 221 с. 4. Шуськін В. О. До питання оцінювання ефективності системи управління військами (силами) // Наука і оборона. 2010. № 4. С. 23–28. 5. Гусак Ю. А., Шевченко В. К. Математична модель живучості системи пунктів управління // Збірник наукових праць ЦНДІ ЗС України. 2019. № 3 (89). С. 120–129.

### Висновки і перспективи подальших досліджень

Таким чином, запропонований методичний підхід дає можливість визначити ймовірності збереження працездатності складовими системи пунктів управління ЗС України на стратегічному, оперативно-стратегічному та оперативному рівнях управління.

Запропонований методичний підхід дозволяє аналізувати живучість як системи ПУ ЗС України, так і її складових в залежності від кількості ПУ, які входять до відповідної системи ПУ, так і від інтенсивності впливу противника.

## МЕТОДИЧЕСКИЙ ПОДХОД К АНАЛИЗУ ЖИВУЧЕСТИ СИСТЕМЫ ПУНКТОВ УПРАВЛЕНИЯ

Юрий Аркадьевич Гусак (доктор военных наук, с.н.с.)  
Василий Кузьмич Шевченко

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

В статье рассматривается проблема анализа живучести системы пунктов управления (ПУ) как одна из составляющих проблемы живучести войск (сил). При рассмотрении этой проблемы осуществлена декомпозиция системы ПУ Вооруженных Сил (ВС) Украины по уровням системы управления войсками и по структуре ВС Украины, в частности: на стратегическом уровне – система ПУ Главнокомандующего ВС Украины; на оперативно-стратегическом уровне – системы ПУ командующего Объединенных сил, командующих видов и отдельных родов войск; на оперативном уровне – системы ПУ командующих оперативных командований и командиров воздушных командований. Показано, что в научных работах, посвященных проблемным вопросам управления войсками во время их применения, применяются модели, которые

описывают живучесть только отдельных ПУ. В связи с этим, в статье предложено методический подход к анализу живучести системы ПУ, который базируется на теории вероятностей. Введены показатели живучести – вероятность сохранения работоспособного состояния системой ПУ на соответствующем уровне и в соответствии с видом, отдельным родом войск, оперативным и воздушным командованиями. Методический подход к анализу живучести системы ПУ позволяет рассчитывать вероятности сохранения работоспособного состояния системой ПУ в зависимости от уровня управления. Для проверки адекватности методического подхода рассмотрены типовую структуру системы ПУ, состоящая из основного, запасного и резервного ПУ. Показано, что предложенный подход не противоречит положениям теории управления войсками и позволяет разработать методику обоснования требований к живучести системы пунктов управления ВС Украины.

**Ключевые слова:** система пунктов управления, методический подход к анализу живучести.

## METHODICAL APPROACH TO ANALYSIS OF SURVIVABILITY OF CONTROL POINTS SYSTEM

*Yurii Husak (doctor of military Sciences, senior researcher)*

*Vasiliy Shevchenko*

*Central research Institute of Armed Forces of Ukraine, Kyiv, Ukraine*

*In this article the problem of the analysis of survivability of control point system (CPS) as one of components of a problem of troops (forces) survivability is considered. By consideration of this problem decomposition of control point system of the Armed forces of Ukraine, on levels of a control system, is carried out: at strategic level – it's a CPS of Commander-in-chief of Armed forces of Ukraine; at operatively-strategic level - CPS of Joint forces, armed services and separate arms commanders; at operative level - CPS of operative commands and air commands commanders. It is shown in articles, which are to problem questions of troops management during their deployment devoted, models, which describe survivability separate control points only, are applied. In this connection, there a methodical approach to the analysis of CPS survivability, which is based on probability theory, is offered. Survivability indicators - probability of preservation by CPS in efficient condition at corresponding level and according to a armed service, separate combat arm, operative and air commands are entered. The methodical approach to the analysis of CPS survivability with command level is depending. To check the adequacy of the methodical approach, it is considered a typical CPS main alternate CPS. This method allows to count probabilities of preservation of an efficient condition of CPS on strategic, operatively-strategic and operative levels. It is shown that the presented approach does not contradict to the theory of troops management and allows to develop a technology of requirements to survivability of CPU of the Armed Forces of Ukraine substantiation.*

**Key words:** control points system, methodical approach to the survivebility analysis.

### References

- 1. Ivanov D.A., Savelyev V.P., Shemansky P.V.** Fundamentals of troops control in battle: ed. 2nd, remaking and ext. Moscow: Voenizdat (Military Publishing), 1977. 389 p.
- 2. Military Encyclopedic Dictionary.** In 2 vol. Moscow: BRE, Ripol classic, 2001. 848 p.
- 3. Fundamentals of troop management / P.K. Altukhov, I.A. Afonsky, I.V. Rybolovsky, A.E. Tatarchenko;** ed. by P.K. Altukhov. Moscow, Voenizdat (Military Publishing), 1984. 221 p.
- 4. Shuenkin V.A.** About the question of evaluating the effectiveness of the troops (forces) control system // Science and Defense. 2010. № 4. P. 23–28.
- 5. Gusak, Y. A., Shevchenko V.K.** Mathematical model of survivability of the system of the control points // Coll. of scienc. worksof CSRI of the Armed Forces of Ukraine, Kyiv, No. 3 (89) pp. 120-127.

*Віталій Валерійович Кривошеєв (кандидат військових наук, доцент)*

*Віталій Олександрович Кацалап (кандидат військових наук, доцент)*

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

## АНАЛІЗ ЕКСПЛУАТАЦІЇ ДІЮЧИХ МАКЕТІВ КОМПЛЕКСУ СПЕЦІАЛЬНИХ АПАРАТНИХ ДЛЯ ПІДРОЗДІЛІВ ІНФОРМАЦІЙНО- ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

*У статті порівнюються особливості дослідної експлуатації зразків діючих макетів комплексу спеціальних апаратних для підрозділів інформаційно-психологічних операцій у зоні проведення антитерористичної операції.*

*Наведений досвід експлуатації діючих макетів комплексу спеціальних апаратних дозволив визначити вимоги щодо встановлення на контрольованій території постійної трансляції радіопередачі з необхідним контентом в FM діапазоні. Використовуючи комплекси спеціальних апаратних підрозділи інформаційно-психологічних операцій можуть сформулювати умови вразливості поведінки цільової аудиторії, що відображає залежність зміни уявлень та характеризує соціальну поведінку можливих цільової аудиторії.*

*З'ясовано, що найбільш суттєві недоліки в утворенні завод прийому телевізійного сигналу і як наслідок необхідність розташування станції на відстані, яка забезпечить стійку роботу приймачів телевізійного мовлення за умов коли розподіл радіочастотного простору дозволяють їх ефективно застосовувати в регіонах з повною відсутністю будь-якого покриття. При погіршенні погодних умов було виявлено відсутність можливостей використання супутникового ресиверу для прийому контенту від комплексу спеціальних апаратних для підрозділів інформаційно-психологічних операцій. Придушення мовлення телевізійних каналів на території Донецької та Луганської областей являється одним із елементів захисту особового складу Збройних Сил України від негативного інформаційно-психологічного впливу.*

**Ключові слова:** антитерористична операція; комплекс спеціальних апаратних; інформаційно-психологічний вплив.

### Вступ

Після стабілізації ситуації по лінії розмежування стало очевидним, що більшість основних об'єктів інформаційної інфраструктури, які знаходяться у зоні проведення антитерористичної операції (АТО) (особливо об'єкти Концерну радіозв'язку, радіомовлення та телебачення України), залишилися на території окремих районів Донецької та Луганської областей (ОРДЛО). Особливо це стосується міста ДОНЕЦЬК де теле- та радіомовлення ведеться з щогли висотою в 360 метрів і дозволяє здійснювати мовлення на територію підконтрольній українській владі (зокрема на міста з великою кількістю населення – КРАМАТОРСЬК, СЛОВ'ЯНСЬК, БАХМУТ, ПОКРОВСЬК) за обмежених можливостей держави щодо ефективної протидії негативному інформаційному впливу.

Управлінням інформаційних технологій Міністерства оборони України відповідно до компетенції спільно з іншими структурними підрозділами Міністерства оборони України, Генерального штабу ЗС України, Міністерством інформаційної політики України та волонтерськими організаціями було започатковано проект щодо створення та проведення дослідної експлуатації зразків (діючих макетів) комплексу спеціальних апаратних для підрозділів інформаційно-психологічних операцій [1].

**Постановка проблеми.** Аналіз питань експлуатації макетних комплексів спеціальних апаратних, які можуть використовуватись підрозділами інформаційно-психологічних операцій Збройних Сил України є досить важливими. Актуальність їх зумовлюється тим, що підрозділи інформаційно-психологічних операцій Збройних Сил України є однією із найвагоміших складових сил оборони, адже на них покладається

завдання з протидії негативному інформаційно-психологічному впливу противника. Тому з метою удосконалення спроможностей сил та засобів інформаційно-психологічних операцій Збройних Сил України існує нагальна необхідність проведення аналізу експлуатації діючих макетів комплексів спеціальних апаратних, встановлення сучасного стану та перспектив їх розвитку.

**Аналіз остатніх досліджень і публікацій.** Дослідженнями питань інформаційно-психологічного впливу в операціях (бойових діях) займалось ряд військових фахівців у цієї галузі, результати дослідження яких знайшли своє відображення у наукових видання [2, 3]. Дані результати базуються на аналізі застосування сил та засобів інформаційно-психологічного впливу у збройних конфліктах останніх років. Але при цьому недостатньо уваги приділялось питанням, пов'язаним з розвитком діючих макетів комплексів спеціальних апаратних, які можуть застосовуватись підрозділами інформаційно-психологічних операцій Збройних Сил України.

**Метою статті** є викладення аналізу експлуатації діючих макетів комплексу спеціальних апаратних для підрозділів інформаційно-психологічних операцій.

### Виклад основного матеріалу дослідження

Зусиллями Міністерства інформаційної політики України, Концерну радіозв'язку, радіомовлення та телебачення України у 2015-2016 роках розроблено низьку заходів щодо відновлення мовлення на території підконтрольній бойовикам ОРДЛО, але вони потребували підтримки з боку інших центральних органів виконавчої влади. Разом з тим, досвід застосування Збройних Сил України показує, що у складі частин інформаційно-психологічних операцій існують підрозділи, які реалізують завдання радіомовлення в кризових регіонах за відсутності державного мовлення.

Враховуючи те, що станом на початок 2016 року Управління інформаційних технологій Міністерства оборони України підпорядковувалися військові частини психологічних операцій, даним Управлінням було ініційовано міжвідомчу нараду щодо реалізації проекту ефірного радіомовлення в зоні проведення АТО на території Донецької та Луганської областей та визначено план дій щодо його реалізації [1, 4].

З метою своєчасного та якісного виконання проекту було відпрацьовано:

доручення Міністра оборони України щодо призначення екіпажів апаратних, порядку

підготовки та відправки в зону проведення АТО на території Донецької та Луганської областей;

доручення заступника Міністра оборони України з питань європейської інтеграції щодо конкретизації виконання завдання на території Донецької та Луганської областей;

отримано три комплекти передавачів FM діапазону в захищеному виконанні із залученням іноземних партнерів та проведені заняття по експлуатації основного обладнання апаратних;

досягнута домовленість з комерційними структурами м. КИСВА (у першу чергу з ТОВ “КомТел”) щодо надання спонсорської допомоги та виготовлення дослідного зразка комплексної апаратної для підрозділів інформаційно-психологічних операцій, підібрані екіпажі для апаратних;

розроблена та затверджена програма дослідної експлуатації комплексу спеціальних апаратних для підрозділів інформаційно-психологічних операцій;

розроблений та затверджений наказ Міністра оборони України від 07.04.2016 року № 186 “Про призначення комісії з проведення дослідної експлуатації комплексу спеціальних апаратних для підрозділів інформаційно-психологічних операцій”.

Проект комплексної апаратної передбачає наявність наступного обладнання (рис. 1):

радіопередавач FM діапазону (шифр FM-25), був наданий іноземними партнерами з діапазоном робочих частот 88,0 – 108,0 МГц та вихідною потужністю 300 Вт;

супутниковий ресивер для прийому основного контенту (спочатку був спланований як окрема студія “Голос Донбасу”, згодом – “Громадське радіо”);

супутникова станція зв'язку для дублювання отримання сигналу та оперативного зв'язку з екіпажем;

передавачі постановки завад телевізійному мовленню з території ОРДЛО в аналоговому та цифровому форматах;

робочі місця операторів;

щогла для антени [1].

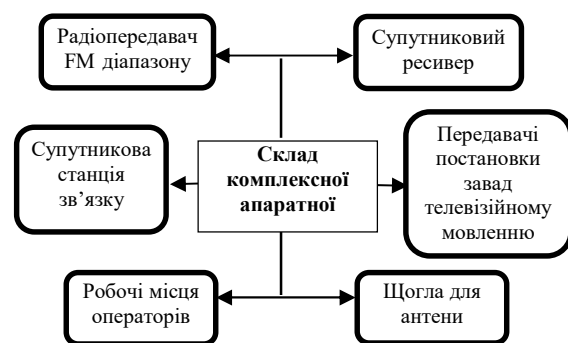


Рис. 1. Проект комплексної апаратної

Зазначена комплексна апаратна передбачала трьохмашинний варіант, в дослідному зразку виконана з використанням транспортної бази ЗіЛ-131.

Загалом обладнання апаратної дозволяло транслювати радіопередачі з необхідним контентом в FM діапазоні на відстань до 30 км та придушувати до 40 телевізійних каналів (8 аналогових каналів та 4 мультиплекси (32 телевізійних цифрових каналів), здійснювати трансляцію місцевих новин, проводити зустрічі з ключовими особами в студії, проводити заходи підтримки морально-психологічного стану особового складу ЗС України. За необхідності можливо було оперативно змінювати покриття, структуру та зміст розгорнутої системи радіомовлення та радіоелектронного придушення за рахунок мобільності комплексу.

Іноземними партнерами обладнання було передане в скороченому варіанті (тільки передавачі FM діапазону). Загалом же зазначені станції дозволяли вести передачі в усьому радіодіапазоні (середньохвильовому, короткохвильовому та ультракороткохвильовому) та навіть розсилати короткі текстові повідомлення для мобільного стільникового зв'язку. Попередньо досягнута домовленість, що після успішного освоєння та встановлення наданого обладнання, доцільно було ініціювати питання щодо подальшої передачі решти комплектуючих.

З використанням промислових можливостей ТОВ "КомТел" було виготовлено один зразок комплексної апаратної, два інші передавачі було заплановано застосовувати з використанням місцевих споруд. Дослідний зразок було виготовлено з використанням транспортної бази ЗіЛ-131 (2 од.) від демонтованих апаратних зв'язку. Загальна вартість відновлення транспортної бази (АБШ та кузовів К-131), їх переобладнання складала понад 250 тис. грн. і здійснювалось в якості волонтерської допомоги.

Розгортання апаратних здійснювалося з дотриманням низки вимог:

встановлення на контрольованій території (пункти управління підрозділів ЗС України, місцеві військово-цивільні адміністрації, державні установи тощо);

наявність промислового живлення 220 В;

можливість встановлення антени на висотних будівлях та на переважаючих висотах;

наявність опалювального приміщення для екіпажу станції та обладнання [5].

Перший етап передбачав розгортання комплексної апаратної на території базового табору з метою тестування обладнання та підтвердження основних характеристик. Зона

впевненого прийому сигналу радіомовлення здійснювалась на відстані – до 30 км, радіоелектронного придушення телевізійних каналів противника – до 20 км, в окремих випадках за рахунок особливостей рельєфу місцевості зона прийому радіомовлення досягала до 50 км (наприклад прийом здійснювався на верхніх поверхах висотних будівель м. ПОКРОВСЬКА).

Цей етап також передбачав пошук можливих місць встановлення з використанням можливостей зведеного загону інформаційно-психологічних операцій за допомогою фахівців Національного університету оборони України імені Черняхівського, на яких було покладено наукове супроводження проекту [6].

Було підібрано декілька місць встановлення – першим було визначено ТПУ омпбр (ОЧЕРЕТИНО) та розгорнуто рухому апаратну FM діапазону з використанням висотної споруди колишнього цегельного заводу та перевірено дальність мовлення. За рахунок вдалого розташування отримано можливість доведення інформації до військових частин ЗС України та місцевих жителів у населених пунктах АВДІВЦІ, ПІСКАХ, ВОДЯНОМУ.

Крім того, станція радіоелектронного придушення була переміщена до м. ПОКРОВСЬКА та встановлена на вежі місцевого комерційного телевізійного оператора ТОВ "КАПРІ", керівництво якого демонструвало проукраїнську позицію та підтримувало зазначені заходи, але було занепокоєне питаннями охорони та оборони своєї споруди при здійсненні придушення телеканалів на території окремих районів.

Було продовжено пошук місць розгортання станцій радіомовлення. Друга станція була розгорнута у КРАСНОГОРІВЦІ з використанням можливостей місцевої військово-цивільної адміністрації та пункту управління бригад.

Станція покривала не лише територію підконтрольну українській владі, але і за інформацією від джерел, що мешкають на тимчасово окупованій території, приймається у Петровському районі м. ДОНЕЦЬКА.

Було продовжено пошук місць розгортання третьої станції радіомовлення. У взаємодії з військово-цивільною адміністрацією Луганської області було запропоновано встановлення радіостанції у м. НОВОТОШКІВСЬКЕ – як майбутньому логістичному центрі, з можливістю доведення необхідної інформації до населення, що мешкає в окремих районах (рис.2).

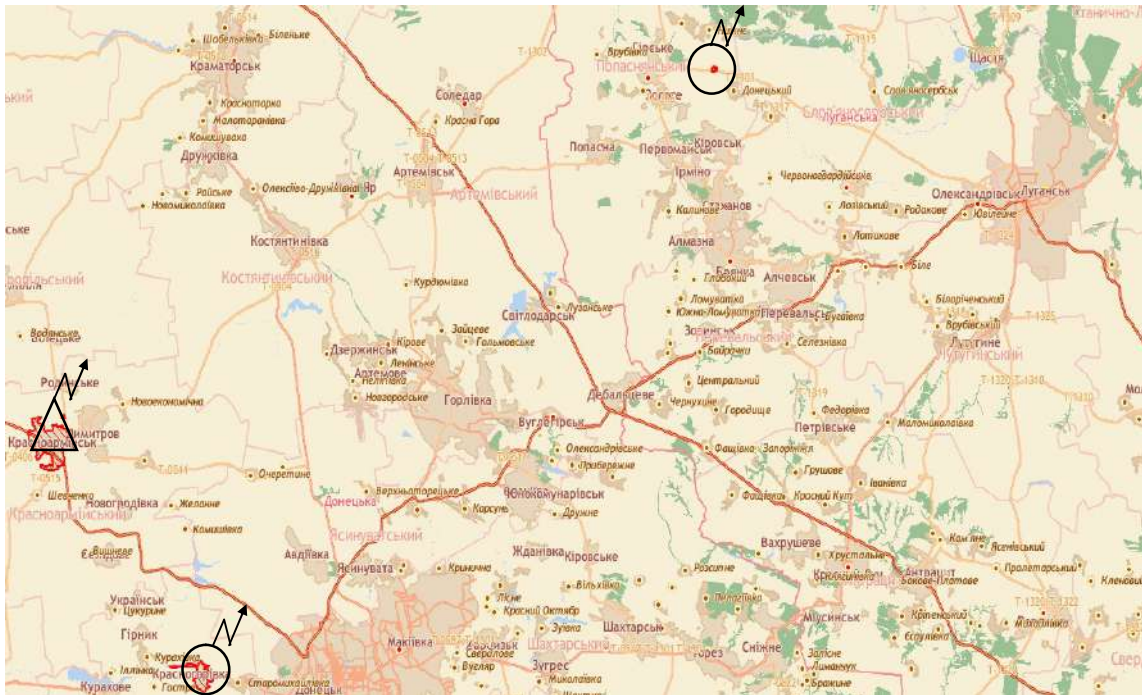


Рис. 2. Дальність дії перешкод

За попередніми результатами роботи станцій радіомовлення FM діапазону найбільш суттєвим недоліком було утворення завад прийому телевізійного сигналу і як наслідок необхідність розташування станції на відстані від 3 км до приймачів телевізійного мовлення (партнерами, що надали станції, це пояснюється плануванням їх застосування в регіонах з повною відсутністю державного покриття). При погіршенні погодних умов спостерігалася неможливість використання супутникового ресиверу для прийому контенту.

Зважаючи на відсутність фінансування, запланований комплекс був створений в одному екземплярі, решта станцій радіомовлення FM діапазону застосовувалась у переносному варіанті (у контейнерах), що зменшує оперативність застосування та мобільність станцій.

За для дослідної експлуатації станції радіоелектронного придушення телевізійного мовлення противника не було заплановано виділення екіпажу станції (передбачалось, що обслуговування буде здійснюватися паралельно екіпажем радіостанції), але при роздільному застосуванні це неможливо або складно, як наслідок – станція працювала в автономному режимі без відповідної охорони та оборони.

Враховуючи наведений досвід експлуатації зразків (діючих макетів) комплексу спеціальних апаратних для підрозділів інформаційно-психологічних операцій рис.2 показав, що наведений розподіл спеціальних апаратних забезпечував стійке покриття території та надійно створював комунікацію між місцевими мешканцями та державними установами [7].

Впровадження проукраїнського FM радіомовлення та радіоелектронного придушення мовлення телевізійних каналів противника на території Донецької та Луганської областей вкрай позитивно сприймалось військовослужбовцями сил АТО, керівниками місцевих військово-цивільних адміністрацій, місцевими жителями.

### Висновки й перспективи подальших досліджень

Таким чином, дослідний зразок (діючий макет) комплексу спеціальних апаратних для підрозділів інформаційно-психологічних операцій виконав основні функції та був рекомендований до проведення державних випробувань.

Органи військового управління ЗС України, яким підпорядковані частини інформаційно-психологічних операцій, продовжують роботу щодо впровадження зазначених комплексних апаратних з метою подальшого застосування наданих партнерами передавачів FM діапазону (зважаючи на наявність завад телевізійному мовленню), розглянули можливість переміщення радіостанцій у райони, де не існує впливу на прийом телевізійного мовлення (промислові квартали населених пунктів) та використали смугові фільтри для вказаних радіостанцій.

З метою насичення зони проведення ООС на території Донецької та Луганської областей зазначеним комплексом здійснені зміни в штаті Головного центру інформаційно-психологічних операцій та частинах інформаційно-психологічних операцій щодо нарощування можливостей за вказаним напрямом з розгортанням власної



телерадіостудії, створенні підрозділів експлуатації теле/радіовипромінюючих засобів та засобів придушення теле/радіосигналу противника.

Під час коригування тактико-технічних вимог передбачене доведення необхідного контенту до станцій FM діапазону не тільки за допомогою

супутникового ресиверу, але і з використанням мережі Інтернет.

На базі однієї з частин інформаційно-психологічних операцій ЗС України створена студія для формування необхідного контенту для радіомовлення з урахуванням цільових аудиторій та виконання запланованих завдань.

### Література

1. Горбулін В. П., Світова гібридна війна: український фронт: монографія. Київ : Національний інститут стратегічних досліджень, 2017. 496 с. 2. Даник Ю. Г., Биченок, М. М., Кацалап В. О. Інформаційна безпека держави у воєнній сфері : навч. посіб. Київ : НУОУ ім. І. Черняховського 2019. 301 с. 3. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони : підручник. ОНАЗ ім. О.С. Попова 2018. 228 с. 4. Кацалап В.О., Войтко О.В., Цурко Ю.В. Методичний підхід до визначення джерел загроз інформаційній безпеці у воєнній сфері / В.О. Кацалап, О.В. Войтко, Ю.В. Цурко // Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони" К.: НУОУ. – 2019. – №1(34). – С. 103-108. 5. Кацалап В.О., Войтко О.В., Рахімов В.В. Аналіз особливостей

маніпуляції, як інструменту психологічного впливу на свідомість / В.О. Кацалап, О.В. Войтко, В.В. Рахімов // Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони" К.: НУОУ. – 2019. – №2(35). – С. 121-126. 6. Кацалап В.О., Войтко О.В., Чернега В.М. Методика оцінки загроз інформаційній безпеці України у воєнній сфері / В.О. Кацалап, О.В. Войтко, В.М. Чернега // Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони" К.: НУОУ. – 2018. – №1(31). – С. 149-154. 7. Військовий стандарт 01.004.004 (Видання 1) Воєнна політика, безпека та стратегічне планування: Інформаційна безпека держави у воєнній сфері. – К.: ЦУМС ЗС України, 2014.

## АНАЛИЗ ЭКСПЛУАТАЦИИ ДЕЙСТВУЮЩИХ МАКЕТОВ КОМПЛЕКСОВ СПЕЦИАЛЬНЫХ АППАРАТНЫХ ПОДРАЗДЕЛЕНИЙ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ ОПЕРАЦИЙ

*Виталий Валерийович Крывошеєв (кандидат военных наук, доцент)*

*Виталий Александрович Кацалап (кандидат военных наук, доцент)*

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

*В статье приведен анализ проведения опытной эксплуатации образцов (действующих макетов) комплекса специальных аппаратных для подразделений информационно-психологических операций в зоне проведения антитеррористической операции.*

*Приведенные характеристики классифицируют комплексы специальных аппаратных по определенным показателям дистанционного информационного управления социальной и индивидуальной поведением возможных объектов информационно-психологического воздействия. Используя комплексы специальных аппаратных подразделения информационно-психологических операций могут сформировывать условия уязвимости поведения целевой аудитории, отражающий зависимость изменения представлений и характеризует социальное поведение возможных целевой аудитории.*

*Результаты анализа предоставили возможность оценить информационно-психологическое воздействие от станций радиовещания FM диапазона. Также выяснено наиболее существенные недостатки в образовании помех приема телевизионного сигнала и как следствие необходимость расположения станции на расстоянии от 3 км до приемников телевизионного вещания в условиях, когда партнерами станции позволяют их эффективно применять в регионах с полным отсутствием какого-либо покрытия.*

*При ухудшении погодных условий было выявлено отсутствие возможностей использования спутникового ресивера для приема контента от комплекса специальных аппаратных для подразделений информационно-психологических операций. Подавление речи телевизионных каналов на территории Донецкой и Луганской областей является одним из элементов защиты личного состава Вооруженных Сил Украины от негативного информационно-психологического воздействия.*

**Ключевые слова:** антитеррористическая операция; комплекс специальных аппаратных; информационно-психологическое воздействие.

**ANALYSIS OF OPERATION OF EXISTING MODELS OF THE COMPLEX OF SPECIAL MACHINERY FOR INFORMATION-PSYCHOLOGICAL OPERATIONS SUBSECTION**

*Vitaliy Krivosheiv (Candidate of Military Sciences, Associate Professor)*

*Vitaliy Katsalap (Candidate of Military Sciences, Associate Professor)*

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

*The article provides an analysis of the experimental exploitation of samples (operating models) of a complex of special hardware for the units of information and psychological operations in the area of anti-terrorist operation.*

*The above characteristics classify complexes of special hardware according to certain indicators of remote information management of social and individual behavior of possible objects of information and psychological influence. Using complexes of special hardware units of information and psychological operations can formulate conditions of vulnerability of behavior of target audience, which reflects dependence of change of ideas and characterizes social behavior of possible target audience.*

*The results of the analysis provided an opportunity to evaluate the information and psychological impact of the FM radio stations. The most significant deficiencies in the formation of TV reception interference were also identified, and as a consequence the need for the station to be located 3 km away from television broadcast receivers, provided that the partners of the station allow them to be effectively used in regions with no coverage at all.*

*With the deterioration of weather conditions, it was revealed that there is no possibility of using a satellite receiver to receive content from a set of special hardware for the units of information and psychological operations. Suppression of broadcasting of television channels on the territory of Donetsk and Luhansk regions is one of the elements of protection of the personnel of the Armed Forces of Ukraine from negative information and psychological influence.*

**Keywords:** *anti-terrorist operation; complex of special hardware; information-psychological influence.*

### **References**

1. Gorbulin V, World Hybrid War: Ukrainian Front: Monograph. Kyiv: National Institute for Strategic Studies, 2017. 496 p.
2. Danik YG, Bychenok, MM, Katsalap VA Information security of the state in the military sphere: textbook. tool. Kyiv: I. Chernyakhovsky 2019. 301 p.
3. Danik Yu. G., Vorobienko PP, Chernega VM Fundamentals of cyber security and cyber defense: a textbook. ONAZ them. OS Popova 2018. 228 p.
4. Katsalap V, Voitko O, Tsurko Y. Methodical approach to identification of sources of threats to information security in the military sphere / V.Katsalap, O.Voitko, Y.Tsurko // Scientific journal "Modern information technologies in the field of security and defense" K. : NDUU. - 2019. - №1 (34). - P. 103-108.
5. Katsalap V, Voitko O, Rakhimov V. Analysis of the features of manipulation as a tool of psychological influence on consciousness / V.Katsalap, O.Voitko, V. Rakhimov // Scientific journal "Modern information technologies in the field of security and defense" K. : NDUU. - 2019. - №2 (35). - pp. 121-126.
6. Katsalap V, Voitko O, Chernega V. Methods of assessment of threats to information security of Ukraine in the military sphere / V.Katsalap, O.Voitko, V.Chernega // Scientific journal "Modern information technologies in the field of security and defense" K. : NDUU. - 2018. - №1 (31). pp. 149-154.
7. Military Standard 01.004.004 (Edition 1) Military Policy, Security and Strategic Planning: Information Security of the State in the Military Sphere. - K. : TsUMS AF of Ukraine, 2014.

*Владислав Григорович Солонніков (доктор технічних наук, професор)*

*Олександр Володимирович Войтко (кандидат військових наук)*

*Тетяна Павлівна Пащенко (кандидат технічних наук)*

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

## ОБҐРУНТУВАННЯ РЕАЛІЗАЦІЇ СТРАТЕГІЧНОГО НАРАТИВУ ДЕРЖАВИ

*Для досягнення мети статті авторами розглядається завдання щодо наукового обґрунтування особливостей впровадження стратегічного нарративу держави на підставі аналізу статистичних даних громадської думки та прогнозування сценаріїв її розвитку.*

*Для досягнення мети статті авторами оброблені та узагальнені статистичні данні громадської думки населення України щодо вступу до ЄС, НАТО та позаблокового статусу за минулі роки. Використовуючи метод статистичної екстраполяції побудовано графіки статистичного ряду зміни громадської думки, визначено апроксимуючі функції для тренда зміни громадської думки. Проведено обчислення параметрів апроксимуючої функції та здійснено точковий прогноз зміни громадської думки. Проведений аналіз надає можливість визначити особливості впровадження стратегічного нарративу держави системою стратегічних комунікацій та реалізувати інтереси держави у вигляді підтримки населення щодо її стратегічного курсу на набуття повноправного членства України в ЄС та НАТО. Отриманий точковий прогноз зміни громадської думки вказує на необхідне мінімальне значення ефективності, якої має досягти система стратегічних комунікацій, при проведенні відповідних заходів щодо популяризації та підтримки населенням відповідного курсу держави не тільки на підконтрольній території а й на тимчасово окупованих територіях Донецької та Луганської областей, а також Автономної республіки Крим.*

***Ключові слова:** стратегічний нарратив, цільова аудиторія, інформаційно-психологічний вплив, стратегічні комунікації.*

### Вступ

Вступ до НАТО та Євроінтеграція – цивілізаційний вибір України, одна з ключових вимог Революції гідності. Відтепер це закріплено у основному Законі України. Верховна Рада ухвалила внесення змін до Конституції України щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору [1]. Звісно, це не означає ані негайного вступу до цих міжнародних організацій, ані навіть початку формалізованого процесу, але це має принципово змінити атмосферу навколо цього питання як і в Україні, так і в світі.

Тому влада зобов'язана наближати Україну до ЄС і НАТО, зміцнювати економіку, розбудовувати сучасну інфраструктуру, медицину, освіту, сильну армію за стандартами НАТО. Тепер це конституційний обов'язок будь-якої влади, всіх її гілок, незалежно від політичних спектрів, оскільки саме влада має будувати шлях до вступу держави в Євросоюз і НАТО. Так, це зазначено в Основному Законі України.

**Постановка проблеми.** В новій редакції Военної доктрини України визначені напрямки забезпечення военної безпеки та завдання щодо набуття критеріїв, необхідних для членства в Європейському Союзі та Організації Північноатлантичного договору [2].

Відповідно до Военної доктрини України та Стратегічного оборонного бюлетня України Міністром оборони України 22 листопада 2017 року було затверджено Концепцію стратегічних комунікацій Міністерства оборони України та Збройних Сил України №612 [3]. В цьому документі зазначено, що використання всіх комунікативних можливостей держави спрямовується на досягнення її цілей.

Стратегічні комунікації на сьогоднішній день перебувають в стадії становлення, при чому цей процес, на відміну від провідних країн світу, відбувається в реальних бойових умовах. Тому наявні проблеми та труднощі потребують оперативного визначення та вирішення. В основу побудови стратегічних комунікацій входить формування стратегічного нарративу.

**Аналіз останніх досліджень і публікацій.** В останні роки з'явилося багато матеріалів досліджень, які проводили різні міжнародні та українські фонди, центри та інститути, щодо оцінки громадської думки [6-11]. Однак праць, які визначали би стратегічний нарратив чи завдання держави для досягнення своїх цілей в співпраці НАТО та ЄС, немає. Багато матеріалів присвячено різним опитуванням громадської думки (населення України) щодо європейської інтеграції. Однак порівняльної статистики та прогнозування зміни громадської думки населення систематично не проводилось та не використовувалось при плануванні стратегічних

цілей держави. Як наслідок не визначались конкретні завдання, які стоятимуть перед системою стратегічних комунікацій Міністерства оборони та Збройних Сил України.

В попередніх працях [4,5] авторами було розглянуто підходи щодо оцінки ефективності функціонування системи стратегічних комунікацій Міністерства оборони та Збройних Сил України і оцінки загроз інформаційній безпеці України у війсьній сфері. Також зазначено, що існуюча система Стратегічних комунікацій є неефективною [4]. Все це відбувається через відсутність наукових підходів щодо визначення стратегічного нарративу держави.

**Метою статті** є наукове обґрунтування особливостей впровадження стратегічного нарративу держави на підставі аналізу статистичних даних громадської думки та прогнозування сценаріїв її розвитку.

### **Виклад основного матеріалу дослідження**

Шостий рік війни з агресором на Донбасі та тимчасово окуповані території дали нашій державі «кривавий урок» щодо пізнання ціни незалежності та територіальної цілісності. З кожним днем наша держава здобуває все більше нових спроможностей у боротьбі з Російською

Федерацією. Особливої актуальності та важливості в сучасних умовах отримують дослідження інформаційно-психологічного впливу на населення тимчасово окупованих територій з боку противника та побудова науково-обґрунтованої дієвої системи інформаційної безпеки України у війсьній сфері у формі реалізації стратегічних комунікацій Міністерства оборони та Збройних Сил України.

Як було зазначено, український правочин передбачає стратегічний курс держави на набуття повноправного членства України в ЄС та НАТО.

З моменту незалежності в українському суспільстві виникали суперечки щодо визначення та облаштування свого громадського і політичного світогляду – національного самовизначення.

Дослідження громадської думки населення України проводились не систематично та не узагальнювалися, а здійснювалися тільки для визначення підтримки програми різних політичних партій, які приходили або були при владі. Тому авторами з метою проведення системного та науково-обґрунтованого аналізу було зібрано всі наявні статистичні дані щодо визначення зміни громадської думки населення стосовно стратегічного курсу держави, починаючи з 2002 року, в залежності від воєнно-політичних, економічних та соціальних умов життєдіяльності населення України в зазначений період часу [6-11]. Ці дані відображено в таблиці 1.

Таблиця 1

Узагальнені статистичні дані щодо вступу до ЄС, НАТО та позаблоковий статус

рік	к-ть населення	Вступ до ЄС			Вступ до НАТО				Позаблоковий статус		
		За %	к-ть	Проти %	к-ть	За %	к-ть	Проти %	к-ть	%	к-ть
2002	48457,1	61,35	29728,4	14,55	7050,5	-	-	-	-	-	-
2003	48003,5	61,55	29546,2	15,88	7623,0	-	-	-	-	-	-
2004	47622,4	52,2	24858,9	23,6	11238,9	-	-	-	-	-	-
2005	47280,8	45,9	21701,9	32,5	15366,3	-	-	-	-	-	-
2006	46929,5	48,5	22760,8	32	15017,4	-	-	-	-	-	-
2007	46646,0	51,4	23976,0	30,7	14320,3	18,9	8816,1	31,3	14600,2	30,7	14320,3
2008	46372,7	50,9	23603,7	29,2	13540,8	-	-	-	-	-	-
2009	46143,7	44,4	20487,8	38,3	17673,0	18	8305,9	30	13843,1	-	-
2010	45962,9	52,8	24268,4	24,2	11123,0	18	8273,3	29	13329,2	-	-
2011	45778,5	51,2	23438,6	30,3	13870,9	18	8240,1	27	12360,2	-	-
2012	45633,6	46,1	21037,1	32,9	15013,5	13	5932,4	26,2	11956,0	42,1	19211,7
2013	45553,0	49,2	22412,1	34,4	15670,2	19	8655,1	21	9566,1	-	-
2014	45426,2	57	25892,9	28,6	12991,9	40,7	18488,5	12,6	5723,7	23,8	10811,4
2015	42929,3	52,7	22623,7	29,1	12492,4	45,7	19618,7	8,2	3520,2	22,6	9702,0
2016	42760,5	54,1	23133,4	30,9	13213,0	44,1	18857,4	6,4	2736,7	26,4	11288,8
2017	42584,5	56,5	24060,2	26,8	11412,6	38,5	16395,0	5,3	2257,0	28,6	12179,2
2018	42386,4	52	22040,9	-	-	46,1	19540,1	7,2	3051,8	24,1	10215,1
2019	42153,2	52	21919,7	25	10538,3	40,9	17240,7	7,4	3119,3	35,9	15133,0

Приєднання України до НАТО – це найкращий спосіб гарантувати національну безпеку України. Такої думки в 2018 році дотримувалось 46% населення. Підтримка населення щодо членства в Альянсі почала стрімко зростати у 2014 р. і стала тенденцією. Так, якщо у 2012 р. на НАТО як джерело безпеки поклалися лише 13% українців, то у травні 2014 р. – вже 33%, у грудні 2014 р. – 44% і листопаді 2015 р. – 46%.

В той же час кардинально втратила свою привабливість ідея позаблоковості та

військового союзу з Росією й іншими країнами СНД. Зокрема, у 2012 р. саме позаблоковий статус був лідером за рівнем підтримки у суспільстві: 42% населення вбачали в ньому гарантію національної безпеки. Після анексії Криму та початку війни на Донбасі частка прибічників позаблоковості різко скоротилася спочатку до 28% у травні 2014 р. і до 23% у листопаді 2015 р. Підтримка військового союзу з Росією та іншими країнами СНД різко впала після анексії Криму та агресивних дій Росії на Донбасі. Якщо у квітні 2012 р. альянс з Росією як джерелом безпеки вважали 26% українців, то у

травні 2014 р. – 13%, а у листопаді 2015 р. прихильників такого варіанту лишилося 8% [6].

Якщо розглядати питання євроінтеграції, то протягом довоєнних років (2011-2013рр.) частка прихильників вступу до ЄС складала близько третини респондентів, а з початком Російської агресії частка симпатиків Євразійського економічного союзу (колишнього Митного союзу країн СНД) впала – у 2015р. до 15,9%, а в 2017 ще знизилася до 7,8%. Відповідно зросла частка прихильників євроінтеграційного шляху.

З 2014р. спостерігається тенденція зростання європейських симпатій в суспільстві. В грудні 2017р. вже майже 60% українських громадян підтримували вступ України до ЄС [7].

Дуже різких змін в бік європейського та північноатлантичного співробітництва громадська думка набула з початком збройної агресії Російської Федерації. За роки війни українське суспільство не отримало бажаного результату, щодо належної підтримки та забезпечення національної безпеки України від ЄС та НАТО. Тому, починаючи з 2017 року, прихильників такої інтеграції почало поступово зменшуватись. З викладеного зрозуміло, що громадська думка щодо вступу до ЄС та НАТО дещо змінювалася в залежності від політичних, воєнних та економічних процесів, що відбувалися протягом останніх двох десятиріч в Україні. Все це підтверджують наведені результати проведеного аналізу статистичних даних. Але для досягнення сформульованої мети дослідження нам недостатньо оцінити тільки сучасний розподіл громадської думки щодо зазначених питань. Необхідно виявити загальні тенденції її зміни по кожному з них в майбутньому. Вибрати ті, що спрямовані у бажаному для нас напрямку і характеризуються найбільшою достовірністю. Досягнути цього можна з використанням наукового прогнозування, а саме - методу статистичної екстраполяції. Особливістю наукового прогнозування є те, що воно спрямовано у майбутнє, а основною його задачею є визначення тенденцій, логіки розвитку процесу, який прогнозується. Це дозволяє зменшити невизначеності майбутньої ситуації на результати рішень, що приймаються.

Метод статистичної екстраполяції полягає у визначенні на підставі достовірних статистичних даних про об'єкт (процес), що прогнозується, його детермінованої (невипадкової) основи (тренда) і наступного обчислення його значень для заданого майбутнього моменту часу, а також оцінки інтервалу можливого розкидання відносно середнього значення.

Рішення задачі екстраполяційного прогнозування здійсимо в такій послідовності: а) побудова графіка статистичного ряду зміни громадської думки; б) вибір апроксимуючої функції для тренда процесу, що досліджується; в) обчислення параметрів апроксимуючої

функції; г) отримання точкового прогнозу та його достовірності.

Початкову інформацію подамо у виді статистичного ряду  $n$  значень функції  $y(t)$ , що задані таблицею 1.

Використання екстраполяції в прогнозуванні ґрунтується на припущенні про те, що процес, який досліджується, може бути поданим сполученням двох складових: регулярної та випадкової (рис. 1).

Регулярна складова - тренд  $f(\bar{a}, t)$  являє собою гладку функцію від аргументу  $t$  і параметра  $\bar{a}$  ( $a_1, a_2, \dots, a_m$ ), що зберігає свої значення на період упередження прогнозу. Випадкова складова  $\eta(t)$  вважається некорельованим випадковим процесом із нульовим математичним очікуванням.

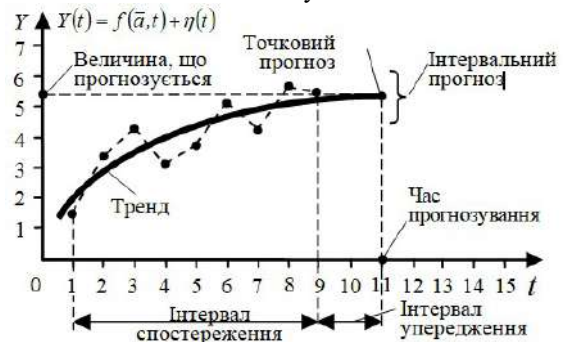


Рис. 1. Графічна інтерпретація екстраполяційного методу прогнозування.

Екстраполяційні методи прогнозування полягають у виділенні тренда та екстраполяції його значень на проміжку упередження. Значення тренда, що екстрапольовано, відповідає точковому прогнозу.

При виборі функції, яка апроксимує тренд процесу, що досліджується, повинна бути вивчена логіка здійснення процесу, в тому числі і припущення щодо його розвитку у майбутньому.

В якості тренда в залежності від особливостей статистичних проявів поведінки досліджуваної функції  $y(t)$  частіше всього вибирається: лінійна, степенева, експоненціальна, логарифмічна або поліноміальна функція.

При обчисленні параметрів тренда необхідно, використовуючи дослідні дані, розрахувати значення цих параметрів, які забезпечать оптимальну апроксимацію. Критерієм оптимальності служить та або інша міра відхилення точок дослідного ряду від апроксимуючої функції.

Будемо використовувати в якості критерію оптимальності метод найменших квадратів. Метод ґрунтується на мінімізації алгебраїчної суми квадратів відхилень дослідних точок від апроксимуючої кривої

$$S = \sum_{i=1}^n [y_i - f(t_i, a_1, a_2, \dots, a_m)]^2 \rightarrow \min,$$

де  $y_i, t_i$  – ордината та абсциса  $i$ -ої точки ряду;

$a_1, a_2, \dots, a_m$  – невідомі параметри апроксимуючої кривої.

Практична реалізація методу при визначенні параметрів  $a_1, a_2, \dots, a_m$  полягає у розв'язанні системи рівнянь:

$$\frac{ds}{da_1} = 0, \quad \frac{ds}{da_2} = 0, \dots, \quad \frac{ds}{da_m} = 0.$$

Апроксимуюча функція, що описує тренд або регулярну складову процесу, є математичним очікуванням цього випадкового процесу на інтервалі спостереження.

Для отримання точкового прогнозу ця функція екстраполюється на інтервалі упередження. Її значення в кінці цього інтервалу при  $t = t_{np}$  відповідає точковому прогнозу:  $\tilde{y}(t_{np}) = f(t_{np}, a_1, a_2, \dots, a_m)$ .

Для визначення інтервального прогнозу потрібно знати характеристики точності та надійності прогнозу. За умови  $M[\eta] = 0$  оцінка дисперсії визначається за формулою математичної статистики:

$$\tilde{D}[\eta] = \frac{1}{n-1} \sum_{i=1}^n [y_i(t_i) - \tilde{y}(t_i)]^2.$$

Точність прогнозу визначається середнім квадратичним відхиленням  $\tilde{\varepsilon}_{np} = \sqrt{\frac{\tilde{D}(\eta)}{n}}$ .

Інтервальный прогноз визначається за формулою:

$$P[\tilde{y}(t_{np}) - t\beta\tilde{\varepsilon}_{np} \leq y_{np} \leq \tilde{y}(t_{np}) + t\beta\tilde{\varepsilon}_{np}] = \beta,$$

де  $\beta$  - довірча імовірність,  $(\tilde{y}(t_{np}) - t\beta\tilde{\varepsilon}_{np}, \tilde{y}(t_{np}) + t\beta\tilde{\varepsilon}_{np})$  - довірчий інтервал прогнозу.

При малому числі спостережень у початковому статистичному ряді  $t_\beta$  - визначається за розподілом Стьюдента. При достатньо великому числі спостережень  $t_\beta$  визначається за нормальним законом розподілу.

Достовірність апроксимації визначається за допомогою коефіцієнта детермінації:  $R^2 = 1 - \varphi^2$ , чим ближче цей коефіцієнт до одиниці, тим точніша модель.

$$\varphi^2 = \frac{\sum_{i=1}^n (y_i - \tilde{y}_i)^2}{\sum_{i=1}^n (y_i - \bar{y}_i)^2} - \text{коефіцієнт збіжності, де } \bar{y}_i$$

- середнє арифметичне значення вибірки.

З метою скорочення часу розрахунків і підвищення їх безпомилковості всі математичні процедури будемо здійснювати з використанням програмного продукту Microsoft Office Excel.

Процес прогнозування громадської думки щодо вступу до ЄС, НАТО та щодо позаблокового статусу України здійснимо по черзі у відповідності зі зазначеними раніше етапами.

1. Прогнозування громадської думки щодо вступу України до ЄС на 2020-2021 роки:

а) побудова графіка статистичного ряду зміни громадської думки щодо вступу в ЄС в період з 2002 по 2019 роки.

Процес побудови графіку (рис.2) був реалізований з використанням програмного продукту Microsoft Office Excel на основі статистичних даних таблиці 2.

Таблиця 2

Статистичні данні громадської думки щодо вступу в ЄС

Кількість опитаних	Інтервал спостереження (Роки)																			Прогноз		Приріст	
	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2020	2021	
“за”	29728,4	29546,2	24858,9	21701,9	22760,8	23976,0	23603,7	20487,8	24268,4	23438,6	21037,1	22412,1	25892,9	22623,7	23133,4	24060,2	22040,9	21919,7	24363,3	25037,6	2443,6	674,3	
%	61,35	61,55	52,2	45,9	48,5	51,4	50,9	44,4	52,8	51,2	46,1	49,2	57	52,7	54,1	56,5	52	52	58,3	60,4	6,32	2,10	
“проти”	7050,5	7623,0	11238,9	15366,3	15017,4	14320,3	13540,8	17673,0	11123,0	13870,9	15013,5	15670,2	12991,9	12492,4	13213,0	11412,6	-	10538,3	7841,2	6187,1	-2697,1	-1654,1	
%	14,55	15,88	23,6	32,5	32	30,7	29,2	38,3	24,2	30,3	32,9	34,4	28,6	29,1	30,9	26,8	-	25,07	20,1	16,8	4,97	-3,3	

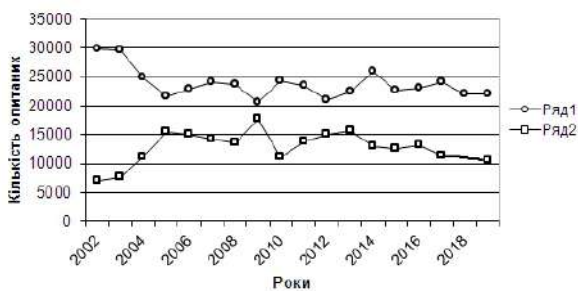


Рис. 2. Статистика даних громадської думки щодо вступу України до ЄС.

В отриманому графіку ряд 1 показує тенденції зміни громадської думки за підтримку курсу

держави щодо вступу в ЄС. Відповідно ряд 2 показує тенденції зміни громадської думки, які виступили проти цього курсу.

б) вибір тренда (апроксимуючої функції), виходячи з бажаних перспектив розвитку процесу, що досліджується і достовірності вибраної апроксимації досліджуваної функції.

Ця процедура також здійснювалася з використанням програмного продукту Microsoft Office Excel послідовно для декількох можливих варіантів трендів. В нашому випадку при дослідженні в якості апроксимуючих функції тренду розглядалися три функції: степенева, експоненціальна і поліноміальна функція другого порядку (рис. 3-5).

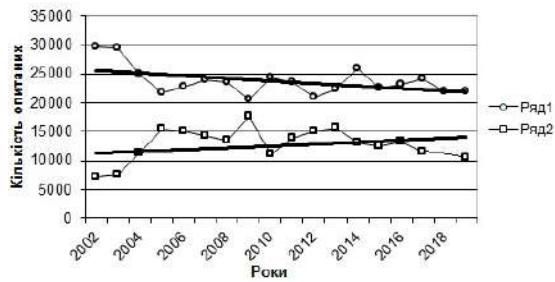


Рис. 3. Апроксимація тренду степеневую функцією.

При обчисленні параметрів тренду степеневую функцією рівняння тренду ряду 1 матиме вигляд  $y = 27993x^{-0,084}$ , де достовірність апроксимації  $R^2 = 0,4432$ , відповідно ряд 2 рівняння тренду -  $y = 8984,4x^{0,1675}$ , достовірність апроксимації  $R^2 = 0,3002$ . Це значення є недопустимим в зв'язку тим, що обраний тренд вказує на зменшення підтримки курсу держави до ЄС та збільшення його противників, а також вказує на низьку достовірність апроксимації, тому розглянемо апроксимацію трендів зміни громадської думки щодо вступу в ЄС за допомогою експоненціальної функції (рис. 4).

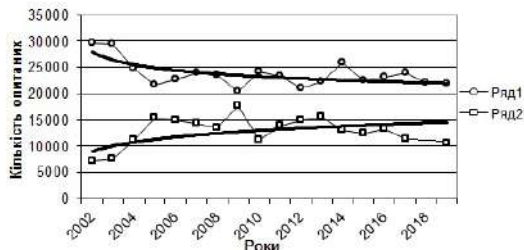


Рис. 4. Апроксимація тренду експоненціальною функцією.

При обчисленні параметрів тренду експоненціальною функцією рівняння тренду ряду 1 матиме вираз  $y = 25819e^{-0,009x}$ , достовірність апроксимації  $R^2 = 0,2431$ , для ряду 2 рівняння тренду -  $y = 11131e^{0,0129x}$ , достовірність апроксимації  $R^2 = 0,0731$ . Це значення також є недопустимим, тому розглянемо апроксимацію трендів зміни громадської думки щодо вступу в ЄС за допомогою поліноміальною функцією другого порядку (рис. 5).

При обчисленні параметрів тренду поліноміальною функцією другого порядку рівняння тренду ряду 1 матиме вигляд  $y = 45,734x^2 - 1109,3x + 28930$ , де достовірність апроксимації  $R^2 = 0,4569$ , відповідно ряд 2 рівняння тренду має вигляд  $y = -85,618x^2 + 1685x + 6734,3$ , а достовірність апроксимації  $R^2 = 0,5836$ .

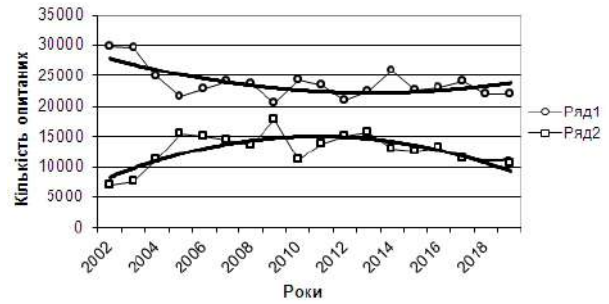


Рис.5. Апроксимація тренду поліноміальною функцією другого порядку.

Порівняльний аналіз закономірностей поведінки ліній вибраних трендів в залежності від часу, зображених на рис. 3-5, переконує у доцільності вибору в якості апроксимуючої функції саме поліноміальну функцією другого порядку.

Як бачимо, тенденції перспектив розвитку змін громадської думки щодо вступу до ЄС при апроксимації процесу змін степеневую і експоненціальною функціями не відповідають положенням Конституції України. Тенденція за вступ до ЄС знижується, а проти вступу - зростає. Крім того достовірність прогнозу з використанням таких трендів надзвичайно низька. При апроксимації тренда степеневую функцією  $R^2 = 0,4432$  для тренда громадської думки за вступ до ЄС і  $R^2 = 0,3002$  для тренда громадської думки проти вступу до ЄС. Аналогічно при апроксимації тренда експоненціальною функцією достовірність апроксимації відповідно  $R^2 = 0,2431$  та  $R^2 = 0,0734$ . Що ж стосується апроксимації процесу розвитку з використанням поліноміальної функції другого порядку, то тенденції перспектив розвитку змін громадської думки щодо вступу до ЄС задовольняють і достовірність апроксимації достатньо висока ( $R^2 = 0,4569$  та  $R^2 = 0,5836$ ). Тому в якості апроксимуючої функції досліджуваного процесу обираємо поліноміальну функцію другого порядку.

в) обчислювання параметрів апроксимуючої функції (тренда);

Цей процес розрахунку при використанні програмного продукту Microsoft Office Excel відбувається одночасно з побудовою вибраного тренда на графіку статистичного ряду процесу, що досліджується. Як бачимо, під графіками наведені рівняння апроксимуючих функцій.

г) отримання точкового прогнозу та його достовірності.

При наявності рівняння тренду процес розрахунку його значення в точці прогнозу можна отримати аналітичним способом, підставивши в рівняння тренду відповідне значення  $x$ . Але при використанні програмного продукту Microsoft Office Excel це відбувається в автоматичному режимі і на графіку тренда з'являються відповідні позначки точкового прогнозу, а у таблиці статистичних даних досліджуваного процесу фіксуються їх числові значення на 2020 і 2021 роки (рис.6, таблиця 2).

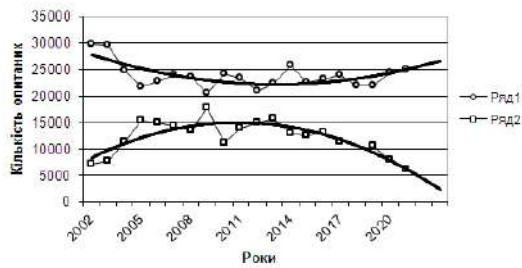


Рис. 6. Прогноз громадської думки населення щодо вступу до ЄС на 2020-2021 роки при апроксимації тренду поліноміальною функцією другого порядку.

Достовірність здійсненого точкового прогнозу для ряду 1 характеризується прогнозом  $R^2 = 0,4661$  відповідно ряд 2:  $R^2 = 0,7217$ .

Отримані числові значення точкового прогнозу громадської думки населення щодо вступу до ЄС на 2020 і 2021 роки відображаємо в таблицю 2. Різниця між показниками величин за 2019 рік та прогнозу відображається у таблиці в стовпчику приріст та вказує на необхідне мінімальне значення ефективності, якої має досягти система стратегічних комунікацій, при проведенні відповідних заходів щодо популяризації та підтримки населенням відповідного європейського курсу держави.

2. Прогнозування громадської думки щодо вступу до НАТО на 2020-2021 роки:

а) побудова графіка статистичного ряду зміни громадської думки щодо вступу до НАТО в період з 2007 по 2019 роки реалізується на основі даних таблиці 3 за допомогою програмного продукту Microsoft Office Excel (рис.7).

Таблиця 3

Статистичні данні громадської думки щодо вступу в НАТО

Кількість опитаних	Інтервал спостереження (Роки)																			Прогноз		Приріст	
	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2020	2021	
“за”	.	.	.	.	.	8816,1	.	8305,9	8273,3	8240,1	5932,4	8655,1	18488,5	19618,7	18857,4	16395,0	19540,1	17240,7	30887,9	32860,0	13647	1972	
%	.	.	.	.	.	18,9	.	18	18	18	13	19	40,7	45,7	44,1	38,5	46,1	40,9	76,5	81,8	35,6	5,34	
“проти”	.	.	.	.	.	14600,2	.	13843,1	13329,2	12360,2	11956,0	9566,1	5723,7	3520,2	2736,7	2257,0	3051,8	3119,3	0,0	0,0	-3119,3	0,0	
%	.	.	.	.	.	31,3	.	30	29	27	26,2	21	12,6	8,2	6,4	5,3	7,2	7,4	0,0	0,0	-7,4	0,0	

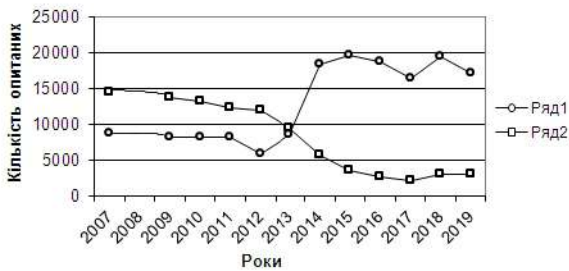


Рис. 7. Статистика даних громадської думки щодо вступу України до НАТО.

В отриманому графіку ряд 1 показує тенденції зміни громадської думки за підтримку курсу держави щодо вступу в НАТО. Відповідно ряд 2 показує тенденції зміни громадської думки проти цього курсу. З отриманої статистики прослідковуються тенденції щодо зниження чисельності населення, яке підтримує зовнішньо політичний курс нашої держави щодо вступу в НАТО. Тому для системи стратегічних комунікацій буде поставати завдання щодо популяризації серед населення відповідного курсу держави та визначення відповідних показників, яких необхідно досягти при виконанні цих заходів.

б,в) вибір апроксимуючої функції та обчислювання параметрів тренда.

Цей етап виконується з використанням програмного продукту MS Office Excel при врахуванні бажаних перспектив розвитку процесу, що досліджується, та достовірності

апроксимації. В якості апроксимуючих функцій розглядалися: лінійна, степенева та поліноміальна функції (Рис. 8-10).

Аналіз отриманих графіків за попередньою схемою показав доцільність вибору в якості апроксимуючої функції досліджуваного процесу лінійної або поліноміальної функції другого порядку. Розвиток процесу в часі відбувається в обох випадках в бажаному стратегічному напрямку і достовірність апроксимації досліджуваного процесу достатньо висока.

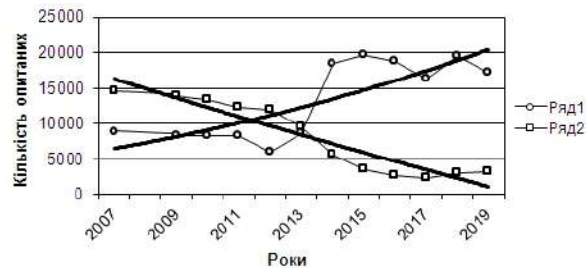


Рис. 8. Апроксимація тренду поліноміальною функцією другого порядку.

Дійсно, при обчисленні параметрів тренду поліноміальною функцією другого порядку рівняння тренду ряду 1 матиме вигляд  $y = 32,468x^2 - 705,77x + 5757,4$ , а достовірність апроксимації  $R^2 = 0,6449$ . Для ряду 2 рівняння тренду  $y = 8,6723x^2 - 1387,9x + 17710$ , достовірність апроксимації  $R^2 = 0,8914$ . При апроксимації досліджуваного процесу лінійною функцією (Рис.9)



рівняння тренду ряду 1 матиме вигляд  $y = 1172,8x + 4498,6$ , а достовірність апроксимації  $R^2 = 0,6391$ . Для ряду 2 рівняння тренду в цьому випадку має вигляд  $y = -1263,2x + 17374$ , а достовірність апроксимації  $R^2 = 0,8909$ .

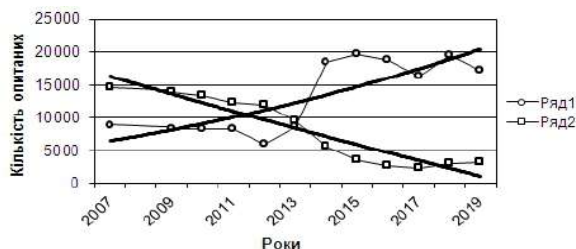


Рис. 9. Апроксимація тренду лінійною функцією.

При обчисленні параметрів тренду степеневою функцією (рис.10) рівняння тренду ряду 1 і 2 мають вигляд:  $y = 5842,2x^{0,3989}$  та  $y = 28170x^{-0,8156}$  відповідно, а достовірність апроксимації набирає значень  $R^2 = 0,4213$  та  $R^2 = 0,6448$ .

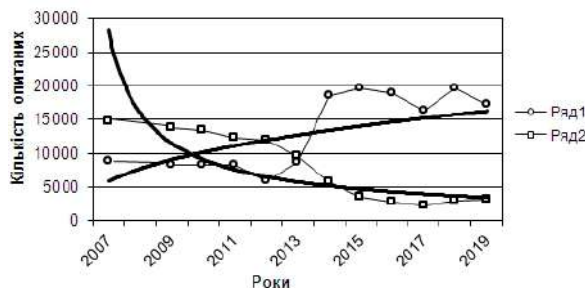


Рис. 10. Апроксимація тренду експоненціальною функцією.

Як бачимо, значення достовірності апроксимації в двох перших варіантах перевищують відповідні показники достовірності апроксимації досліджуваного процесу при

використанні у якості тренду степеневої функції, але оскільки достовірність апроксимації при використанні поліноміальної функції дещо вища ніж у лінійної, віддаємо перевагу поліноміальній функції другого порядку.

г) здійснення точкового прогнозу та оцінювання його достовірності теж відбувалося з використанням програмного продукту Microsoft Office Excel. Результати цього процесу наведені на рис. 11 та у таблиці 3. Достовірність здійсненого точкового прогнозу для ряду 1 характеризується значенням  $R^2 = 0,7602$ , відповідно для ряду 2:  $R^2 = 0,9255$ .

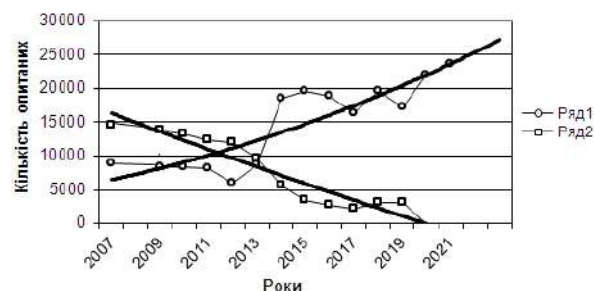


Рис. 11. Прогноз громадської думки населення щодо вступу до НАТО на 2020-2021 роки при апроксимації тренду поліноміальною функцією другого порядку.

Отримані числові значення точкового прогнозу громадської думки населення щодо вступу до НАТО на 2020 і 2021 роки відображаємо в таблицю 3. Також в цій таблиці відображено приріст прогнозних показників на 2020-2021 роки у порівнянні з попередніми роками.

3. Прогнозування громадської думки щодо позаблокового статусу України на 2020-2021 роки.

а) побудова графіку статистичного ряду зміни громадської думки щодо позаблокового статусу України в період з 2007 по 2019 роки.

Ця операція була реалізована (рис.12) за допомогою програмного продукту Microsoft Office Excel з використанням статистичних даних, наведених у таблиці 4.

Таблиця 4

Статистичні дані громадської думки щодо позаблокового статусу

Кількість опитаних	Інтервал спостереження (Роки)																		Прогноз		Приріст	
	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2020	2021
“за”	.	.	.	.	.	14320,3	.	.	.	.	19211,7	.	10811,4	9702,0	11288,8	12179,2	10215,1	15133,0	14684,8	12441,3	-448,2	-2243,5
%	.	.	.	.	.	30,7	.	.	.	.	42,1	.	23,8	22,6	26,4	28,6	24,1	35,9	34,3	29,6	-1,6	-4,7

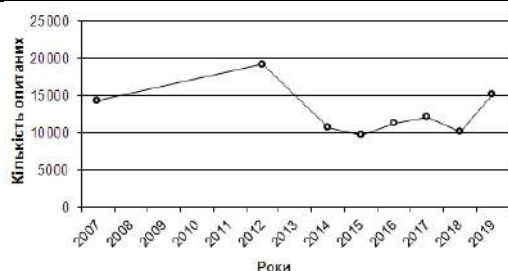


Рис. 12. Статистичні дані громадської думки щодо позаблокового статусу України

б) вибір тренда (апроксимуючої функції).

Порівняльний аналіз побудованих трендів статистичного ряду громадської думки щодо позаблокового статусу України, проведений за визначеними критеріями, показав, що в якості апроксимуючої функції досліджуваного процесу в даному випадку найбільш доцільно обрати поліноміальну функцію четвертого порядку (рис.13). Нажаль, менш складні апроксимуючі функції досліджуваного процесу не відповідають стратегічним завданням політичного розвитку України.

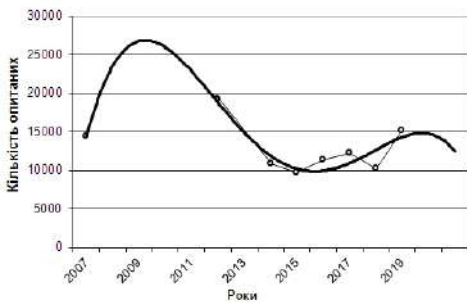


Рис. 13. Апроксимація тренду поліноміальною функцією четвертого порядку

При обчисленні параметрів тренду поліноміальною функцією четвертого порядку рівняння тренду матиме вираз  $y = -13,096x^4 + 465,39x^3 - 5467,4x^2 + 22539x - 3185$ . Такий тренд відповідає всім вимогам і характеризується високим рівнем достовірності апроксимації  $R^2 = 0,8382$ .

Обчислювання параметрів вибраного тренда, реалізація точкового прогнозу та оцінювання його достовірності ( $R^2 = 0,8453$ ) здійснювалося аналогічним чином. Результати цього процесу наведені на рис.14 та у таблиці 4.

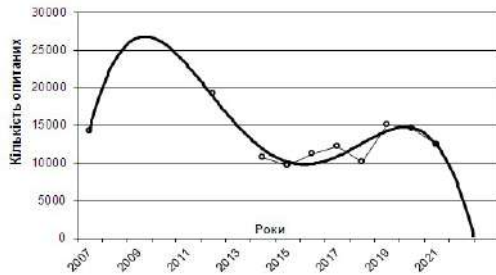


Рис. 14. Прогноз громадської думки населення щодо позаблокового статусу України на 2020-2021 роки при апроксимації тренду поліноміальною функцією четвертого порядку.

Отримані числові значення точкового прогнозу громадської думки населення щодо позаблокового статусу на 2020 і 2021 роки відображаємо в таблицю 4. Аналогічно в цій таблиці відображено приріст прогнозних показників на 2020-2021 роки у порівнянні з попередніми роками.

Узагальнюючи результати дослідження щодо прогнозування громадської думки за трьома напрямками: щодо вступу до ЄС, НАТО та щодо позаблокового статусу України, можна зробити наступні висновки.

1. Завдяки обґрунтованому вибору трендів (апроксимуючих функцій) процесів зміни громадської думки щодо вступу до ЄС (поліноміальна функція другого порядку), до НАТО (поліноміальна функція другого порядку) та щодо позаблокового статусу України (поліноміальна функція четвертого порядку) вдалося спрогнозувати бажані загальні тенденції її зміни по кожному з цих напрямків в 2020-2021 роках.

2. Визначені точкові прогнозні дані значень громадської думки щодо визначеної тематики опитування на 2020-2021 роки.

Проведені розрахунки показують, що при відповідній організації і реалізації інформаційно-психологічного впливу на визначені цільові аудиторії кількість прихильників вступу до ЄС буде зростати і досягне значення у 2020 році 24,4 млн. чол.(58,3%), у 2021 році перетне позначку у 25 млн. чол.(60,4%). Кількість населення, яка б проголосувала за вступ України до НАТО, теж зростатиме і досягне значення 30,9 млн. чол.(76,5%) у 2020 році та 32,9 млн. чол. (81,8%) у 2021 році. Кількість прихильників позаблокового статусу України у 2020 році відповідно до прогнозу зменшиться до 14,7 млн. чол.(34,3%), а у 2021 році – до 12,4 млн. чол. (29,6%).

3. Розраховані прогнозні дані щодо зростання (зменшення) кількісної оцінки розподілу громадської думки щодо зазначених питань у 2020 і 2021 роках порівняно з 2019 роком.

Аналіз цих даних свідчить про те, що для забезпечення в подальшому позитивного прогнозного розвитку громадської думки населення України щодо вступу до ЄС та НАТО необхідно у 2020 та 2021 роках збільшити кількість прихильників розвитку суспільства в цьому напрямку відповідно на 2,4 млн. чол.(6,3%) у 2020 році та 0,7 млн. чол.(2,1%) у 2021 році (за вступ до ЄС) та на 13,7 млн. чол.(35,6%) у 2020 році та на 2,0 млн. чол.(5,3%) у 2021 році (за вступ до НАТО). Що стосується прихильників позаблокового статусу України, то при відповідній організації роботи в інформаційному просторі їх кількість зменшиться у 2020 році на 0,45 млн. чол. (1,6%) та на 2,2 млн. чол.(4,7%) у 2021 році.

4. Для досягнення зазначених результатів система стратегічних комунікацій держави повинна забезпечити:

чітке визначення єдиного загальнодержавного стратегічного нарративу та особливостей його впровадження різними державними інституціями України;

створення механізмів системного, комплексного впливу на конкретні цільові аудиторії шляхом переконання, перевиховання громадськості завдяки розробки та застосування високоякісного інформаційно-психологічного та соціально-патріотичного продукту євро-інтеграційного спрямування і унеможливлення завдяки цьому відхилення від стратегічного нарративу при здійсненні професійної діяльності різними державними інституціями;

скоординовану діяльність в інформаційному просторі всіх державних інституцій України.

### Висновки і перспективи подальших досліджень

Основною ціллю для системи стратегічних комунікацій Міністерства оборони та Збройних Сил України є досягнення стратегічного нарративу. Як зазначалось вище, статистика громадської думки щодо підтримки вступу до ЄС та НАТО дещо

зменшується, тому таким нарративом для цієї системи має бути популяризація проєвропейського стратегічного курсу держави та підтримка його населенням.

Отже, запропонований підхід щодо реалізації стратегічного нарративу держави надасть можливість вірно побудувати та реалізувати систему інформаційної безпеки у воєнній сфері у формі стратегічних комунікацій Міністерства оборони та Збройних Сил України. Проведений аналіз надав можливість визначити основні завдання для системи стратегічних комунікацій та реалізувати інтереси держави у вигляді підтримки населення щодо стратегічного курсу держави на набуття

повноправного членства України в ЄС та НАТО. Подальший розвиток цього дослідження необхідно проводити на основі сучасних наукових методів теорії соціальних досліджень та теорії інформаційних операцій з метою виявлення часових показників, які характеризують розповсюдження матеріалів інформаційних впливів до кожної цільової аудиторії. Особливо важливо таку інформацію отримувати з тимчасово окупованих територій Донецької та Луганської областей, а також Автономної республіки Крим. Це дасть можливість вірно визначити цільові аудиторії, аргументувати тематику повідомлень та канали розповсюдження матеріалів інформаційно-психологічного впливу.

### Література

1. Конституція України від 28.06.1996 № 254к/96-ВР із змінами № 2680-VIII від 07.02.2019, ВВР, 2019, № 9.
2. Указ президента України № 555/2015 24 вересня 2015 року "Про нову редакцію Воєнної доктрини України".
3. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України : Наказ Міністра оборони України від 22.11.2017 р. №612/2017. URL: <http://www.mil.gov.ua>.
4. **Войтко О.В.** Оцінювання ефективності функціонування системи стратегічних комунікацій Міністерства оборони та Збройних Сил України. Науковий журнал "Системи управління, навігації та зв'язку". 2018. – №3(49). – С. 97-99.
5. **Кацалап В.О., Войтко О.В., Чернега В.М.** Методика оцінки загроз інформаційній безпеці України у воєнній сфері. Науковий журнал "Сучасні

інформаційні технології у сфері безпеки та оборони". 2018. – №1(31). – С.149-154.

6. Електронний ресурс режим доступу URL: <https://ukraine-nato.mfa.gov.ua/ua/inform-center/gromadsyka-dumka-shhodo-vstupu-v-nato>
7. Електронний ресурс режим доступу URL: <https://dif.org.ua/article/evropeyska-integratsiya-u-vimiri-gromadskoi-dumki>
8. Електронний ресурс режим доступу URL: <http://razumkov.org.ua/statti/ukraina-na-shliakhu-do-yes-otsinky-dumky-i-spodivannia-hromadian>
9. Електронний ресурс режим доступу URL: [https://dif.org.ua/article/gromadska-dumka-ukraini-na-28-rotsi-nezalezhnosti-derzhavi?fbclid=IwAR0t4aD3U3A9f67v0B\\_jXFgrFkKVcqZRv0mFMUNi5nvv1bk4NG35\\_6eJGzw](https://dif.org.ua/article/gromadska-dumka-ukraini-na-28-rotsi-nezalezhnosti-derzhavi?fbclid=IwAR0t4aD3U3A9f67v0B_jXFgrFkKVcqZRv0mFMUNi5nvv1bk4NG35_6eJGzw)
10. Електронний ресурс режим доступу URL: <https://www.pravda.com.ua/news/2019/06/5/7217188/>
11. Електронний ресурс режим доступу URL: <http://www.ukrstat.gov.ua/>

## ОБОСНОВАНИЕ РЕАЛИЗАЦИИ СТРАТЕГИЧЕСКОГО НАРРАТИВУ ГОСУДАРСТВА

*Владислав Григорьевич Солонников (доктор технических наук)  
Александр Владимирович Войтко (кандидат военных наук)  
Татьяна Павловна Пащенко (кандидат технических наук)*

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

Для достижения цели статье авторами рассматривается задачи по научному обоснованию особенностей внедрения стратегического нарратива государства на основании анализа статистических данных общественного мнения и прогнозирования сценариев ее развития. Для достижения цели статье авторами обработанные и обобщенные статистические данные общественного мнения населения Украины относительно вступления в ЕС, НАТО и внеблокового статуса за прошлые годы. Используя метод статистической экстраполяции построены графики статистического ряда изменения общественного мнения, определены аппроксимирующие функции для тренда изменения общественного мнения. Проведено вычисления параметров аппроксимирующей функции и осуществлено точечный прогноз изменения общественного мнения. Проведенный анализ позволяет определить особенности внедрения стратегического нарратива государства системой стратегических коммуникаций и реализовать интересы государства в виде поддержки населения по ее стратегического курса на обретение полноправного членства Украины в ЕС и НАТО. Полученный точечный прогноз изменения общественного мнения указывает на необходимое минимальное значение эффективности, которой должен достичь система стратегических коммуникаций, при проведении соответствующих мероприятий по популяризации и поддержки населением соответствующего курса государства не только на подконтрольной территории но и на временно оккупированных территориях Донецкой и Луганской областей, а также автономной республики Крым.

**Ключевые слова:** стратегический нарратив, целевая аудитория, информационно-психологическое воздействие, стратегические коммуникации.

REASONS FOR IMPLEMENTATION THE STRATEGIC DRAFT OF THE STATE

Vladislav Solonnikov (Doctor of Technical, Professor)  
Oleksandr Voitko (Candidate of Military Sciences)  
Tatiana Pashchenko (Candidate of Technical Sciences)

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

To achieve the purpose of the article, the authors consider the task of scientifically substantiating the peculiarities of implementing the strategic narrative of the state based on the analysis of public opinion statistics and forecasting the scenarios of its development. In order to achieve the purpose of the article, the authors have compiled and summarized the statistical data of public opinion of Ukraine's population on joining the EU, NATO and non-aligned status over the past years. Using the method of statistical extrapolation, graphs of the statistical series of changes in public opinion were constructed, and the approximation functions for the trend of public opinion change were determined. The parameters of the approximation function are calculated and the point forecast of the change of public opinion is made. The conducted analysis gives an opportunity to determine the peculiarities of implementation of the strategic narrative of the state by the system of strategic communications and to realize the interests of the state in the form of support of the population for its strategic course for the acquisition of full membership of Ukraine in the EU and NATO. The obtained point forecast of the change of public opinion indicates the necessary minimum value of effectiveness, which should be achieved by the strategic communication system, in carrying out appropriate measures to promote and support the population of the respective course of the state not only in the controlled territories but also in the temporarily occupied territories of Donetsk, Luhansk and Luhansk Of the Autonomous Republic of Crimea.

**Key words:** strategic narrative, target audience, information and psychological impact, strategic communications.

References

1. The Constitution of Ukraine of June 28, 1996 No. 254k / 96-BP as amended No. 2680-VIII of February 7, 2019, OJSC, 2019, No. 9.
2. Presidential Decree No. 555/2015 of September 24, 2015 "On the new version of the Military doctrine of Ukraine."
3. On approval of the Strategic Communication Concept of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine: Order of the Minister of Defense of Ukraine dated 06/26/2017 №612 / 2017. URL: <http://www.mil.gov.ua>.
4. Voitko O.V. Evaluation of the effectiveness of the strategic communications system of the Ministry of Defense and the Armed Forces of Ukraine. Scientific Journal of Management, Navigation and Communication. 2018. - №3 (49). - P. 97-99.
5. Katsalap V.A., Voitko O.V., Chernega V.M. Methods for assessing threats to information security of Ukraine in the military sphere. Scientific journal "Modern information technologies in the field of security and defense". 2018. - №1 (31). - P.149-154.
6. Electronic resource access mode URL: <https://ukraine-nato.mfa.gov.ua/en/inform-center/gromadsyka-dumka-shhodo-vstupu-v-nato>.
7. Electronic resource access mode URL: <https://dif.org.ua/article/evropeyska-integratsiya-u-vimiri-gromadskoi-dumki>.
8. Online resource access mode URL: <http://razumkov.org.ua/statti/ukraina-na-shliakhu-do-yes-otsinky-dumky-and-povivannia-chromadian>.
9. Electronic resource access mode URL: [https://dif.org.ua/article/gromadska-dumka-ukraini-na-28-rotsi-nezalezhnosti-derzhavi?fbclid=IwAR0t4aD3U3A9f67v0B\\_jXFgrFkKVcqZRv0mFMUNi5nvv1bk4NG35\\_6eJGzw](https://dif.org.ua/article/gromadska-dumka-ukraini-na-28-rotsi-nezalezhnosti-derzhavi?fbclid=IwAR0t4aD3U3A9f67v0B_jXFgrFkKVcqZRv0mFMUNi5nvv1bk4NG35_6eJGzw).
10. Electronic resource access mode URL: <https://www.pravda.com.ua/news/2019/06/5/7217188/>
11. Electronic resource access mode URL: <http://www.ukrstat.gov.ua/>

## 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**

← (кегль – 11 пт.)

<sup>2</sup> **Інститут..., Київ, Україна**

← 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 підрисунковими 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>*Anatoliy 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 informacijnі 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; науковий 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 Олександрову 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.