

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ БЕЗПЕКИ ТА ОБОРОНИ

ISSN 2311-7249 (Print)

ISSN 2410-7336 (Online)

№ 2(26)
2016

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)-271-09-44, (099)-319-73-51
факс: (044)-271-09-44

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 № 14 від 31 серпня 2016 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:
Citefactor, 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:

Теоретичні основи створення і використання інформаційних технологій

- Гаценко С.С., Наумчак О.М.** Методика визначення та розрахунку характеристик підсистеми розподілу та зберігання інформації системи підтримки та прийняття рішень 5
- Горський О.М.** Соціонічно-інформаційний підхід до забезпечення функціональної стійкості авіаційно-космічної бойової системи 15
- Захарченко Н.В., Гордейчук В.В., Севастеев Е.А.** Увеличение информационной емкости найквистового элемента при передаче 2-х символьных ансамблей таймерными сигналами 21
- Кивлюк В.С., Клонцук М.Я.** Імітаційна модель функціонування системи тимчасового перевагуючого району 26
- Козубцов І.М.** Аналіз нормативно-правової складової об’єктного компонента методологічної культури ад’юнктів 33
- Косогов О.М., Сірик А.О.** Моделювання процесу оцінювання інформаційної безпеки на основі експертних висновків 39
- Кубявка М.Б., Кубявка Л.Б.** Концептуальна модель визначення необхідних інформаційних впливів на противника 44
- Лебідь Є.В.** Математична модель системи фазової автопідстройки частоти з цифровим фазовим детектором з пристроєм формування неузгодженості та готовності сигналів 48
- Маковецький О.М., Мальцева І.Р., Паламарчук Н.А., Черниш Ю.А., Шемендюк О.В.** Підходи до удосконалення методики оцінки ефективності комплексної системи захисту інформації 54
- Мурасов Р.К., Мельник Я.В.** Завчасне попередження про DDoS атаку на базі методів прогнозування 59
- Маслюк Л.А., Стужук П.І., Челобітченко О.О., Правдивець О.М.** Проблеми та рекомендації зі створення автоматизованих систем управління військами (силами) для збройних сил 63
- Нагорнюк О.А., Павлюк В.В.** Методика автоматизованого розрахунку параметрів частотної маніпуляції в умовах апріорної невизначеності 74
- Овсянніков В.В., Паламарчук С.А., Процюк Ю.О., Штонда Р.М., Островський С.М.** Аналіз алгоритмів обробки логічних сигналів засобів виявлення охоронної сигналізації 81
- Репіло Ю.Є., Тарасов С.В.** Адаптація методу нечітких множин для оцінки корупційних ризиків у збройних конфліктах 87
- Шишанов М.О., Коцюрба В.І.** Балістична модель тралення вибухових пристроїв з натяжним датчиком цілі 95

Інтерактивні моделі розвитку науково-освітнього простору у сфері безпеки та оборони

- Чопа Д.А., Дерев’яничук А.Й., Москаленко Д.Р., Бичко Д.В.** Підхід до створення web-інтерфейсу інформаційно-дистанційно-тренажерної системи 99

Сучасні військово-теоретичні проблеми

- Артюшин Л.М., Куртсейтов Т.Л., Мірненко В.І., Сидорчук О.Л.** Можливості застосування протирадіолокаційних покриттів у антенних системах засобів озброєння та військової техніки з метою зменшення їх радіолокаційної помітності 104
- Бобильов В.Є.** Особливості ведення бойових дій у інформаційному середовищі 110
- Войтко О.В.** Аналіз механізмів запобігання війн і воєнних конфліктів 113
- Головка А.А.** Недержавні суб’єкти протидії загрозам національній безпеці в інформаційній сфері 117
- Даценко І.П.** Методические основы технико-экономической оценки технологических процессов сварки при производстве и модернизации специальных автомобилей 121
- Дачковський В.О., Овчаренко І.В.** Аналіз розвитку бойових броньованих машин 127
- Думенко М.П.** Аналіз функціонування системи кадрового забезпечення під час дії особливого періоду у 2014-2015 роках 132
- Закусило П.С.** Порядок визначення оптимального календарного строку служби перспективних зразків озброєння та військової техніки з урахуванням морального старіння 141
- Майстренко О.В.** Обґрунтування рекомендацій щодо зонального розподілу засобів вогневого впливу та об’єктів для ураження 145

Редакційна колегія

Головний редактор

полковник *Пермяков Олександр Юрійович*,
доктор технічних наук, професор

Заступник головного редактора

полковник *Савченко Віталій Анатолійович*,
доктор технічних наук, старший науковий співробітник

Члени редколегії:

Бутвін Борис Леонідович,
доктор технічних наук, професор

генерал-полковник *Воробйов Генадій Петрович*,
кандидат військових наук

Гавлічек Пьотр, доцент

Дробаха Григорій Андрійович,
доктор військових наук, професор

Жук Сергій Якович,
доктор технічних наук, професор

Загорка Олексій Миколайович,
доктор військових наук, професор

полковник *Катеринчук Іван Степанович*,
доктор технічних наук, професор

Компанцева Лариса Феліксівна,
доктор філологічних наук, професор

Косевцов В'ячеслав Олександрович,
доктор військових наук, професор

Кравченко Юрій Васильович,
доктор технічних наук, професор

полковник *Лобанов Анатолій Анатолійович*,
доктор військових наук, професор

Потій Олександр Володимирович,
доктор технічних наук, професор

Пресналл Аарон, доктор філософії

Репіло Юрій Євгенович,
доктор військових наук, професор

генерал-майор *Риспаев Асхат Науризбайович*,
кандидат військових наук

Романченко Ігор Сергійович,
доктор військових наук, професор

Рубан Ігор Вікторович,
доктор технічних наук, професор

Рябцев Вячеслав Віталійович,
кандидат технічних наук, доцент

Сбітнев Анатолій Іванович,
доктор технічних наук, професор

Семон Богдан Йосипович,
доктор технічних наук, професор

Серватюк Василь Миколайович,
доктор військових наук, професор

Солонніков Владислав Григорович,
доктор технічних наук, професор

Телелим Василь Максимович,
доктор військових наук, професор

Флурі Філіпп,
доктор філософії

Шевченко Віктор Леонідович,
доктор технічних наук,
старший науковий співробітник

Шемаєв Володимир Миколайович,
доктор військових наук, професор

Шиміч Горан,
доктор філософії

Відповідальний секретар

капітан *Судніков Євген Олександрович*

MODERN INFORMATION TECHNOLOGIES IN THE SPHERE OF SECURITY AND DEFENCE

ISSN 2311-7249 (Print)

ISSN 2410-7336 (Online)

№ 2(26)
2016

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)-271-09-44, (099)-319-73-51
Fax: (044)-271-09-44

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

The journal is published
in Russian, Ukrainian and English

The journal is published thrice a year

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

*Recommended to publication
by the Scientific Council of the National
Defence University of Ukraine
named after Ivan Cherniakhovsky
(Protocol No. 14, 31 August 2016)*

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:
*Citefactor, 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:

Theoretical Foundations of Information Technologies Creation and Use

<i>Hatsenko S.S., Naumchak O.M.</i> Method of calculation and determination of the subsystem distribution and storage of information systems and decision support	5
<i>Horskyi O.M.</i> Socionic-informational approach to providing functional stability of aerospace combat system	15
<i>Zakharchenko M.V., Hordiuchuk V.V., Sevastieiev Y.O.</i> Increase the navy element capacity in 2-character ensembles with timing signals transfer	21
<i>Kyviuk V.S., Klontsak M.Y.</i> Simulation model of the system temporary overloading area	26
<i>Kozubtsov I.M.</i> The analysis of regulatory constituent objective component of adjuncts methodological culture	33
<i>Kosohov O.M., Siryk A.O.</i> Modelling based on the expert judgements of the process of informational safety evaluation	39
<i>Kubiavka M.B., Kubiavka L.B.</i> Conceptual model for defining the necessary information impact on the enemy	44
<i>Lebid Y.V.</i> Mathematical model the system phase - locked loop (PLL) with a digital phase detector with the device reshaper of signals disagreement and readiness	48
<i>Makovetskyi O.M., Maltseva I.R., Palamarchuk N.A., Chernysh Y.O., Shemendiuk O.V.</i> Approach to improving efficiency evaluation method of the complex information security	54
<i>Murasov R.K., Melnyk Y.V.</i> Early warning information on DDoS attacks based on the prediction methods	59
<i>Masliuk L.A., Stuzhuk P.I., Chelobitchenko O.O., Pravydvets O.M.</i> Problems and recommendations for the creation automated control systems troops (forces) for Armed Forces	63
<i>Nahorniuk O.A., Pavliuk V.V.</i> Problems and recommendations on creation of automated command and control systems for armed forces	74
<i>Ovsiannikov V.V., Palamarchuk S.A., Protsiuk Y.O., Shtonda R.M., Ostrovskiy S.M.</i> Analysis of logic signals processing algorithms of detection alarm	81
<i>Repilo Y.Y., Tarasov S.V.</i> Adapting the fuzzy sets method for the evaluation corruption risks in conflict environment	87
<i>Shyshanov M.O., Kotsiuruba V.I.</i> Ballistic explosive sweeping model with a pull-action target-sensor	95

Interactive Models of Scientific Educational Environment Development in the Sphere of Security and Defence

<i>Chopa D.A., Derevianchuk A.Y., Moskalenko D.R., Bychko D.V.</i> The approach to the creation of the web-interface information and remote-training systems	99
--	----

Modern Military Theoretical Problems

<i>Artyushyn L.M., Kurtseytov T.L., Mirnenko V.I., Sydorchuk O.L.</i> Application of coatings confusional antenna system weaponry and military equipment to reduce their radar signature	104
<i>Bobylov V.Y.</i> Features of warfare in the information environment	110
<i>Voiiko O.V.</i> Analysis of mechanisms to prevent wars and military conflicts	113
<i>Holovka A.A.</i> Non-governmental actors countering threats of national security threats in the information sphere	117
<i>Datsenko I.P.</i> Methodical bases feasibility assessment welding process in production of modernization of special vehicles	121
<i>Dachkovskiy V.O., Ovcharenko I.V.</i> Analysis of armoured combat vehicles	127
<i>Dumenko M.P.</i> Analysis of the functioning of personnel providing system during the special period in 2014-2015	132
<i>Zakusylo P.S.</i> Procedure for determining optimal policy calendar lifetime of weapons and military equipment with obsolescence	141
<i>Maistrenko O.V.</i> Ground of recommendations in relation to zonality of facilities of fire defeat of opponent and objects for defeat	145

Editorial Board

Chief Editor

colonel *Permiakov Oleksandr Yuriiovych*,
doctor of technical sciences, professor

Deputy Chief Editor

colonel *Savchenko Vitalii Anatoliiovych*,
doctor of technical sciences, senior research fellow

Editorial Board members:

Butvin Borys Leonidovych,
doctor of technical sciences, professor

colonel general *Vorobiov Henadii Petrovych*,
candidate of military sciences

Gawliczek Piotr,
associate professor

Drobakha Hryhorii Andriiovych,
doctor of military sciences, professor

Zhuk Serhii Yakovych,
doctor of technical sciences, professor

Zahorka Oleksii Mykolaiovych,
doctor of military sciences, professor

colonel *Katerynychuk Ivan Stepanovych*,
doctor of technical sciences, professor

Kompantseva Larysa Feliksivna,
doctor of philological sciences, professor

Kosevtsov Viacheslav Oleksandrovych,
doctor of military sciences, professor

Kravchenko Yurii Vasylovych,
doctor of technical sciences, professor

colonel *Lobanov Anatolii Anatoliiovych*,
doctor of military sciences, professor

Potii Oleksandr Volodymyrovych,
doctor of technical sciences, professor

Presnall Aaron,
doctor of philosophy

Repilo Yurii Yevhenovych,
doctor of military sciences, professor

major general *Ryspaiev Askhat Nauryzbaiovych*,
candidate of military sciences

Romanchenko Ihor Serhiiovych,
doctor of military sciences, professor

Ruban Ihor Viktorovych,
doctor of technical sciences, professor

Riabtsev Viacheslav Vitaliiovych,
candidate of technical sciences,
associate professor

Sbitniev Anatolii Ivanovych,
doctor of technical sciences, professor

Semon Bohdan Yosypovych,
doctor of technical sciences, professor

Servatiuk Vasyl Mykolaiovych,
doctor of military sciences, professor

Solonnikov Vladyslav Hryhorovych,
doctor of technical sciences, professor

Telemetry Vasyl Maksymovych,
doctor of military sciences, professor

Fluri Philip,
doctor of philosophy

Shevchenko Viktor Leonidovych,
doctor of technical sciences,
senior research fellow

Shemaiev Volodymyr Mykolaiovych,
doctor of military sciences, professor

Shimic Goran,
doctor of philosophy

Executive Secretary

captain *Sudnikov Yevhen Oleksandrovych*

Сергій Станіславович Гаценко
Олена Михайлівна Наумчак

Національний університет оборони України імені Івана Черняхівського, Київ, Україна
Військова частина А1586, Житомир, Україна

МЕТОДИКА ВИЗНАЧЕННЯ ТА РОЗРАХУНКУ ХАРАКТЕРИСТИК ПІДСИСТЕМИ РОЗПОДІЛУ ТА ЗБЕРІГАННЯ ІНФОРМАЦІЇ СИСТЕМИ ПІДТРИМКИ ТА ПРИЙНЯТТЯ РІШЕНЬ

У статті проводиться визначення та розрахунок власних характеристик підсистеми розподілу та зберігання інформації системи підтримки прийняття рішень автоматизованої системи управління військами та характеристик якості обслуговування інформаційних потоків з метою подальшої практичної реалізації даної підсистеми в інтересах розробки та впровадженні автоматизованої системи управління військами та її функціонування в умовах максимального інформаційного навантаження при різких змінах в оперативній обстановці.

Ключові слова: система підтримки прийняття рішень; характеристики; автоматизована система управління військами; інформаційні потоки.

Вступ

Аналіз війн і збройних конфліктів останніх років переконливо свідчить, що сьогодні зміст парадигми збройного протистояння піддався самим кардинальним, воістину революційним, змінам. Причинами цього стали – бурхливий розвиток електроніки, поява принципово нових інформаційних технологій і мережових інформаційно-керуючих систем, що функціонально об'єднують в собі всі наявні в розпорядженні командувачів і командирів сили і засоби розвідки, управління, ураження і забезпечення. Основу даного об'єднання становить широкомасштабна реалізація системотехнічних рішень, мережових технологій і принципів мережецентричної Концепції ведення операцій (бойових дій). Саме завдяки цьому сьогодні з'явилася реальна можливість організувати комплексне застосування різновидових і різнорідних угруповань військ в єдиному інформаційному і комунікаційному просторі району бойових дій. Все це призвело до істотної трансформації не тільки в змісті збройного протистояння, а й до перегляду самої технології управління військами [1,2].

Постановка проблеми. Не врахування змін, що відбуваються, та відсутність можливостей в пошуку та практичній реалізації нових, таких що відповідають реаліям сьогодення інноваційних рішень, має наслідком велику ступінь відставання від світових тенденцій та ставить під сумнів виконання бойових завдань майбутнього. Прикладом цього є проведення Антитерористичної операції на території Донецької та Луганської областей (АТО), вході якої були виявлені досить серйозні проблеми. Це, перш за все, наявність у військах технічно і морально застарілих засобів розвідки, які не спроможні забезпечити швидкий обмін отриманою

розвідувальною інформацією, відсутність сучасних засобів зв'язку і передачі даних, практично повна відсутність комплексів і засобів автоматизації [3-6].

Проблему комплексної автоматизації вже багато років в Збройних Силах (ЗС) України намагаються вирішити шляхом створення Єдиної автоматизованої системи управління військами (ЄАСУ) ЗС України, основою якої є перехід від концепції “платформо-центричної війни”, де основний акцент робився на кількості озброєння та військової техніки, у бік “мережецентричної війни” [7]. Основою концепції “мережецентричної війни” є комплексна інтеграція сил і засобів оперативно-стратегічної розвідки, спостереження військової розвідки з системами управління, контролю, зв'язку та обчислювальними засобами у єдиному інформаційному просторі, що дозволяє суттєво підвищити ефективність їх бойового застосування. в першу чергу, за рахунок зменшення тривалості циклу бойового управління [7]. У загальному вигляді модель мережецентричної війни – це система, що складається з трьох складових підсистем: інформаційної, сенсорної і бойової. Основу цієї системи складає інформаційна підсистема, на яку накладаються взаємно пересічні сенсорна і бойова. Інформаційна підсистема пронизує собою всю систему в повному обсязі. Обмін зображеннями та текстовою інформацією відбувається в режимі реального часу. розвідувальні дані надходять не конкретному споживачеві, а до загальної бази даних або ресурс відповідного угруповання і стають доступними всім зацікавленим особам (споживачам інформації) [8]. Основними функціями інформаційної підсистеми є передача, зберігання, розподіл інформації при значному інформаційному навантаженні та різких змінах в

оперативній обстановці, що надходить від сенсорної підсистеми, яка в ЗС України являється добувними частинами та підрозділами системи воєнної розвідки держави [9].

Отже виникає актуальне наукове завдання, що на даний час залишається не вирішеним, а саме передачі, зберігання та розподілу розвідувальної інформації в автоматизованій системі управління військами про що свідчать матеріали розроблення ЄАСУ ЗС України. В [10, 11] авторами розроблені математичні моделі інформаційних потоків (ІП), дисципліни обслуговування АСУ військами, що функціонують в системі управління військами ЗС України.

Аналіз останніх досліджень і публікацій [12-15] показує, що удосконалення АСУ проводиться шляхом впровадження нових засобів зв'язку і автоматизації, зокрема, як в напрямку покращення існуючих систем зв'язку, так і створення нових, супутникових, радіорелейних, тропосферних, оптоволоконних і радіосистем (особливо пересувних) для різних ланок військового управління з можливістю загального користування їх послугами. Авторами [10, 16] в інтересах майбутньої ЄАСУ ЗС України запропоновано удосконалення науково-методичного апарату передачі, зберігання, розподілу інформації в АСУ військами, надання рекомендацій в інтересах підтримки прийняття рішень.

Мета статті. На даному етапі вирішення поставленого наукового завдання пропонується шляхом удосконалення методики визначення та розрахунку власних характеристик підсистеми розподілу та зберігання інформації СППР АСУ військами та характеристик якості обслуговування (ІП) з метою подальшої практичної реалізації даної підсистеми в умовах максимального інформаційного навантаження при змінах в оперативній обстановці.

Виклад основного матеріалу дослідження

Відповідно до [16] саме підсистема розподілу та зберігання інформації СППР АСУ військами призначена виконувати функції передачі, зберігання та розподілу ІП. Вона і є об'єктом дослідження в даній статті, а її власні

характеристики та характеристики якості обслуговування ІП – предметом дослідження. На початковому етапі моделювання підсистеми розподілу та зберігання інформації було досліджено можливості технічної реалізації системи передачі потоків розвідувальної інформації від частин розвідки до споживачів інформації. З врахуванням того, що добувні підрозділи розвідки виконують розвідувальні завдання на значному віддаленні від органів управління ними, головною вимогою до системи передачі інформації повинна бути мобільність, достатня пропускна спроможність і дальність, а також економність в експлуатації.

Аналіз сучасних засобів зв'язку та досвід АТО [17-19] показав, що дані вимоги будуть виконані при використанні засобів супутникового зв'язку (СЗ) табл.1. Тому в статті розроблена методика визначення та розрахунку характеристик передачі ІП, що відображає функціонування моделі підсистеми розподілу та зберігання інформації СППР АСУ військами для різних швидкостей обміну даними з використанням різної кількості супутникових ліній зв'язку (СЛЗ).

Удосконалена методика має наступні етапи:

1-й етап: визначення власної характеристики підсистеми розподілу та зберігання інформації – поступаюче (обслужене) навантаження;

2-й етап: визначення власної характеристики підсистеми розподілу та зберігання інформації – середня пропускна здатність;

3-й етап: визначення характеристик якості обслуговування вхідного потоку запитів (ІП);

4-й етап: розробка алгоритму розрахунку власних характеристик та характеристик якості обслуговування вхідного потоку запитів підсистеми розподілу та зберігання інформації з визначенням (встановленням) їх взаємозалежності;

5-й етап: розрахунок характеристик підсистеми розподілу та зберігання інформації СППР АСУ військами;

6-й етап: рекомендації по впровадженню результатів розрахунків характеристик підсистеми розподілу та зберігання інформації при розробці АСУ військами.

Таблиця 1

Вимоги до систем зв'язку

Вимоги Роди зв'язку	Постійна готовність	Мобільність	Стійкість	Пропускна спроможність	Еконо- мічність	Розвід- захищеність	Живучість
Радіозв'язок	середня	середня	низька	середня	середня	низька	середня
Транкінговий радіозв'язок	середня	середня	середня	середня	середня	середня	середня
Радіорелейний зв'язок	середня	середня	низька	середня	середня	висока	середня
Тропосферний зв'язок	середня	середня	середня	середня	середня	висока	середня
Супутниковий зв'язок	висока	висока	висока	середня	середня	середня	висока
Проводовий зв'язок	середня	низька	середня	висока	низька	висока	висока

Реалізація етапів запропонованої методики.

1. Визначення власної характеристики підсистеми розподілу та зберігання інформації – поступаюче (обслужене) навантаження.

Відповідно до [20] при обслуговуванні потоку запитів комутаційною системою (КС), кожен запит займає вихід протягом деякого інтервалу часу. Якщо, наприклад, вихід одночасно обслуговує тільки один запит, то навантаження виходу може характеризуватись сумарним часом обслуговування всіх запитів, а коефіцієнт корисної дії або використання виходу можна оцінювати відношенням сумарного часу обслуговування всіх запитів до часу роботи виходу. Таким чином, сумарний час обслуговування запитів і буде навантаженням. Навантаження поділяється на: поступаюче, обслужене та втрачене.

Поступаюче на КС за інтервал часу $[t_0; t_{св}]$ навантаження $y[t_1; t_2]$ – таке навантаження, яке було б обслужене КС за інтервал часу $[t_1; t_2)$ якби кожному поступаючому запиту негайно було надано з'єднання із вільним виходом. Тобто це є відношення параметру вхідного потоку запитів до параметру закону розподілу тривалості обслуговування запитів в КС. За одиниці виміру прийнято: для поступаючого навантаження – одну година-зайняття, для інтенсивності поступаючого навантаження – один Ерланг (Ерл) – це навантаження в одну годину-зайняття за 1 годину.

Отже для проведення предметної комплексної оцінки підсистеми розподілу та зберігання інформації необхідно оперувати розрахунковими числовими значеннями таких характеристик як навантаження (зокрема **поступаючи** у та **обслужене** y_0 **навантаження**), а також **середня пропускна здатність** η , що і є власними характеристиками підсистеми.

Слід зазначити, що швидкість запису/зчитування даних в КС здійснюється з швидкістю на порядок вищою, ніж швидкість обміну даними в супутникових каналах зв'язку (СКЗ), тому поступаюче у та обслужене y_0 навантаження будуть рівні між собою і їхня величина визначається власне поступаючим навантаженням, тому:

$$y = y_0.$$

Крім того, очевидним є факт, що інтенсивність навантаження значно відрізняється: в різні періоди доби, у випадку проведення заходів оперативної і бойової підготовки (ОБП) збройних сил країн, а також під час підготовчої та основної фаз операцій (наприклад НЗФ на Донбасі) (рис. 1). Також відповідно до цього навантаження донесень від частин та підрозділів розвідки змінюється від часу доби (рис. 2).

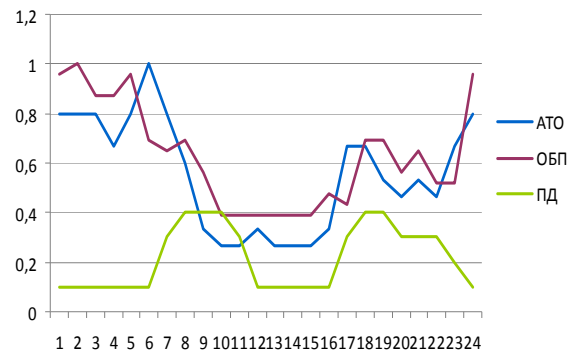


Рис. 1 Графік навантаження каналів передачі даних в залежності від періоду доби

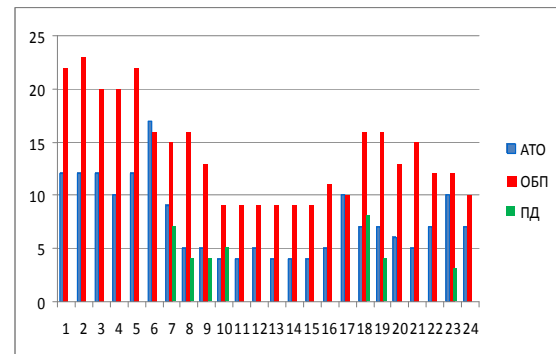


Рис. 2 Графік залежності навантаження донесеннями від часу доби

Виходячи з цього, для функціонування підсистеми розподілу та зберігання інформації СППР АСУ військами для будь-якого з приведених випадків, розрахунок необхідно здійснювати виходячи із значення інтенсивності навантаження тоді, коли воно являється найбільшим.

Період, коли навантаження є найбільшим називається періодом найбільшого навантаження. Нехай даний період дорівнює одній годині. Тоді година найбільшого навантаження – це безперервний інтервал часу тривалістю 60 хвилин, протягом якого середня інтенсивність навантаження є найбільшою.

Визначення необхідних вихідних даних параметрів інтенсивності навантаження:

кількість джерел навантаження (з досвіду АТО) – $n - 100$;

середня кількість запитів, поступаючих від одного джерела навантаження (з досвіду АТО) – $\bar{c} - 10$;

середня тривалість зайняття КС при обслуговуванні одного запиту – \bar{t} ;

Очевидно, що середня тривалість зайняття КС при обслуговуванні одного запиту \bar{t} знаходиться в обернено-пропорційній залежності від швидкості обміну даними R , тобто зі збільшенням швидкості передачі даних в СКЗ R зменшується тривалість зайняття t , і навпаки – при передачі інформаційних повідомлень такого ж інформаційного об'єму на меншій швидкості R значення тривалості зайняття КС t зростає. З урахуванням [11] слідує висновок:

при незмінних значеннях інших параметрів навантаження, пропускна здатність, імовірнісні та часові характеристики підсистеми розподілу та зберігання інформації СППР визначаються швидкістю обміну інформацією в КЗ R (СКЗ).

Для підсистеми розподілу та зберігання інформації тривалість зайняття – це інтервал часу з моменту подачі від підрозділу добування РІ команди на встановлення стійкого зв'язку з метою передачі даних до серверу баз даних до моменту повернення елементів КЗ у вихідне положення. Тривалість зайняття залежить від швидкості передачі даних по ЛЗ R, інформаційного об'єму РІ I, а також частково від складових підсистеми розподілу та зберігання інформації. Як висновок, тривалість зайняття є випадковою величиною і її середнє значення для даної підсистеми може бути визначене тільки на основі обґрунтованого прогнозування, оскільки підсистема знаходиться на етапі проектування і аналогів їй на даний час не існує.

Розглянемо складові середньої тривалості зайняття для можливих видів зайняття:

1. *Запис РІ до бази даних відбувся.* Середня тривалість цього виду зайняття має вигляд:

$$\bar{t}_p = \bar{t}_c + \bar{T} + \bar{t}_0, \quad (1)$$

де \bar{t}_c – середній час на встановлення з'єднання між станцією СЗ добувного підрозділу та СЗ серверу баз даних. Для схеми “супутникова станція – супутник – супутникова станція” цей час становить близько 0,6 секунди, для схеми працюючої по топології “зірка” – близько 2-х секунд;

\bar{t}_0 – середній час повернення СКЗ у вихідний стан після запису інформаційного повідомлення. Тривалість \bar{t}_0 дорівнює тривалості \bar{t}_c оскільки повернення СКЗ у вихідний стан здійснюється аналогічним чином як і встановлення з'єднання між ВЗ добувного підрозділу та ВЗ серверу баз даних \bar{t}_c ;

\bar{T} – середній час передачі інформації.

$$\bar{T} = \frac{\bar{I}}{R}, \quad (2)$$

де \bar{I} – питомий інформаційний об'єм одного р-повідомлення. З досвіду проведення АТО задамо наступні дані для об'ємів інформаційних повідомлень в годину найбільшого навантаження для одного добувного підрозділу розвідки:

\bar{I}_m – середній об'єм передаваного текстового документу - 0,02 Мбайт;

\bar{I}_r – середній об'єм передаваного голосового повідомлення - 2 Мбайт;

\bar{I}_f – середній об'єм передаваної фотодокументу - 1 Мб;

\bar{I}_v – середній об'єм передаваного одного відео-повідомлення - 10 Мб.

Таким чином, до підсистеми розподілу та зберігання інформації будуть надходити інформаційні повідомлення 4-х категорій. Позначимо в загальному виді через \bar{I}_i середній об'єм повідомлення і-ї категорії, \bar{c}_i – середня кількість повідомлень і-ї категорії. Тоді при k категоріях повідомлень питомий інформаційний об'єм повідомлення становитиме:

$$\bar{I} = \frac{\sum_{i=1}^k \bar{I}_i \bar{c}_i}{\sum_{i=1}^k \bar{c}_i}. \quad (3)$$

Як уже було відмічено, з урахуванням можливого збільшення загальної кількості добувних підрозділів в АСУ військами до $n = 100$, з яких 20% становитимуть підрозділи РЕР (у випадку реалізації даної СППР частка голосових повідомлень становитиме до 90%, текстових повідомлень – близько 10%), 80% – підрозділи військової розвідки іншого оперативного призначення (у випадку реалізації даної СППР частка фото- та відео-повідомлень становитиме відповідно по 45%, текстових повідомлень – близько 10%).

Слід зазначити, що дані значення є далеко не остаточними, оскільки отримані шляхом міркувань на основі особистого досвіду оперативного застосування військ при проведенні АТО. В свою чергу, дійсно достовірна кількість добувних підрозділів і відповідно статистичний розподіл р-повідомлень можливий лише в ході тривалого спостереження за функціонуючою підсистемою розподілу та зберігання інформації. Однак, при виборі саме таких числових значень, головним критерієм було забезпечення функціонування підсистеми розподілу та зберігання інформації в умовах передачі великих об'ємів інформації при значній кількості добувних підрозділів в умовах максимального навантаження на СППР.

2. *Запис РМ до бази даних не відбувся з технічних причин.* Середня тривалість даного виду зайняття $\bar{t}_{техн}$ може встановлюватись провайдером та визначатись тривалістю очікування супутниковою станцією підрозділу добування відповіді від супутникової станції серверу баз даних на запит встановлення зв'язку. Для розрахунків приймемо, що тривалість очікування становить 10 секунд.

Таким чином, середня тривалість успішного запису р-повідомлення \bar{t}_p та середня тривалість зайняття КЗ при неможливості встановлення стійкого зв'язку між супутниковими станціями підрозділу добування та серверу баз даних по технічних причинах $\bar{t}_{техн}$ становлять повну групу подій. В сучасних системах супутникового зв'язку імовірність $\bar{P}_{техн} \leq 1\%$ усіх з'єднань. На основі цього середня тривалість одного зайняття може бути розрахована за виразом:

$$\begin{aligned} \bar{t} &= P_p \cdot \bar{t}_p + P_{\text{техн}} \cdot \bar{t}_{\text{техн}} = 0,99 \left(4 + \frac{4,539}{R} \right) + \\ &+ 0,01 \cdot 10 = 3,96 + \frac{4,494}{R} + 0,1 = \quad (4) \\ &= 4,06 + \frac{4,494}{R}. \end{aligned}$$

Величина інтенсивності поступаючого (обслуженого) навантаження буде розраховуватися за формулою, що має вигляд:

$$y = n\bar{c}\bar{t} = n\bar{c} \left(\frac{4,06 + \frac{4,494}{R}}{3600} \right). \quad (5)$$

2. Визначення власної характеристики підсистемі розподілу та зберігання інформації – середньої пропускної здатності, визначення вихідних даних.

Передача РІ від добувних підрозділів на сервер баз даних може здійснюватись з використанням: по одному КЗ для кожного добувного підрозділу; декількох КЗ (один на певну групу добувних підрозділів); одного КЗ на АСУ військами.

З метою демонстрації динаміки зміни пропускної здатності пучка ліній КС підсистеми розподілу та зберігання інформації η необхідно задати наступні дані для υ = 1, 2, 3, 4, 5, 10, 20, 30, 50, 100 ліній пучка, кожна з яких на практиці являє собою СКЗ.

В загальному, пропускна здатність η оцінюється відношенням інтенсивності обслуженого навантаження у₀ до кількості ліній в пучку υ:

$$\eta = \frac{y_0}{\nu}. \quad (6)$$

3. Визначення характеристик якості обслуговування вхідного потоку запитів (ІІІ).

Характеристики якості обслуговування вхідного потоку запитів визначаються дисципліною обслуговування цього потоку запитів [11] підсистемою розподілу та зберігання інформації СППР. Відповідно до вищевикладеного матеріалу в досліджуемій підсистемі буде реалізовано дисципліну обслуговування вхідного потоку запитів з очікуванням.

Для кількісної оцінки якості обслуговування підсистемою розподілу та зберігання інформації вхідного потоку РІ з очікуванням розраховуються [20] наступні характеристики:

1. P(γ > 0) – імовірність очікування для будь-якого поступившого запиту;
2. P(γ > t) – імовірність очікування для будь-якого поступившого запиту більше деякого часу t;
3. P₃(γ > t) – імовірність очікування р-повідомленням, що попало в чергу на обслуговування, більше часу t;

4. $\bar{\gamma}$ – середній час очікування по відношенню до всіх поступивших р-повідомлень;

5. ${}_3\bar{\gamma}$ – середній час очікування по відношенню до поступивших р-повідомлень, що потрапили в чергу на очікування;

6. \bar{r} – середня довжина черги.

Для визначення імовірності очікування для будь-якого поступившого запиту P(γ > 0) буде використано математичний вираз другої формули Ерланга:

$$P_t = P(\gamma > 0) = \frac{E_\nu(y)}{1 - \frac{y}{\nu}(1 - E_\nu(y))} = D_\nu(y). \quad (7)$$

Однак перед цим необхідно визначити за допомогою таблиць Пальма-Ерланга та спеціалізованого програмного забезпечення “ERLANG CALCULATOR 14.0.11” числові значення параметру E_ν(y) – втрат в повнодоступному пучку.

Використовуючи вираз (7) – визначимо для кожного значення пропускної здатності імовірність очікування для будь-якого поступившого запиту P(γ > 0).

Для визначення P(γ > t) – імовірності очікування для будь-якого поступившого запиту більше деякого часу t, необхідним є використання виразу:

$$P(\gamma > t) = P(\gamma > 0)e^{-(\nu-y)t}, \quad (8)$$

де e^{-(ν-y)t} = P₃(γ > t) – імовірність очікування р-повідомленням, що попало в чергу на обслуговування, більше часу t. Слід зазначити, що у виразі (7) за одиницю виміру γ та t прийнято середню тривалість зайняття, що для кожного значення швидкості обміну даними в СКЗ є індивідуальною.

Наступною характеристикою процесу обслуговування поступаючого на вхід підсистеми розподілу та зберігання інформації потоку запитів р-повідомлень є середній час очікування по відношенню до всіх поступивших р-повідомлень $\bar{\gamma}$, визначається виразом:

$$\bar{\gamma} = \frac{P(> 0)}{\nu - y}, \quad (9)$$

де $\bar{\gamma}$ – виражається через середню тривалість зайняття.

Відповідно $\frac{1}{\nu - y} = {}_3\bar{\gamma}$ – середній час очікування

по відношенню до поступивших р-повідомлень, що потрапили в чергу на очікування.

Важливою та необхідною для глибокого та всебічного аналізу підсистеми розподілу та зберігання інформації в цілому є середня довжина черги \bar{r} , що визначається як середній час очікування початку обслуговування по відношенню до всіх поступивших запитів $\bar{\gamma}$

помножений на інтенсивність поступаючого на вхід підсистеми навантаження U визначається за виразом:

$$\bar{r} = \bar{\gamma} \cdot y. \quad (10)$$

4. Розроблення алгоритму розрахунку власних характеристик та характеристик якості обслуговування вхідного потоку запитів підсистеми розподілу та зберігання інформації з врахуванням їх взаємозалежностей.

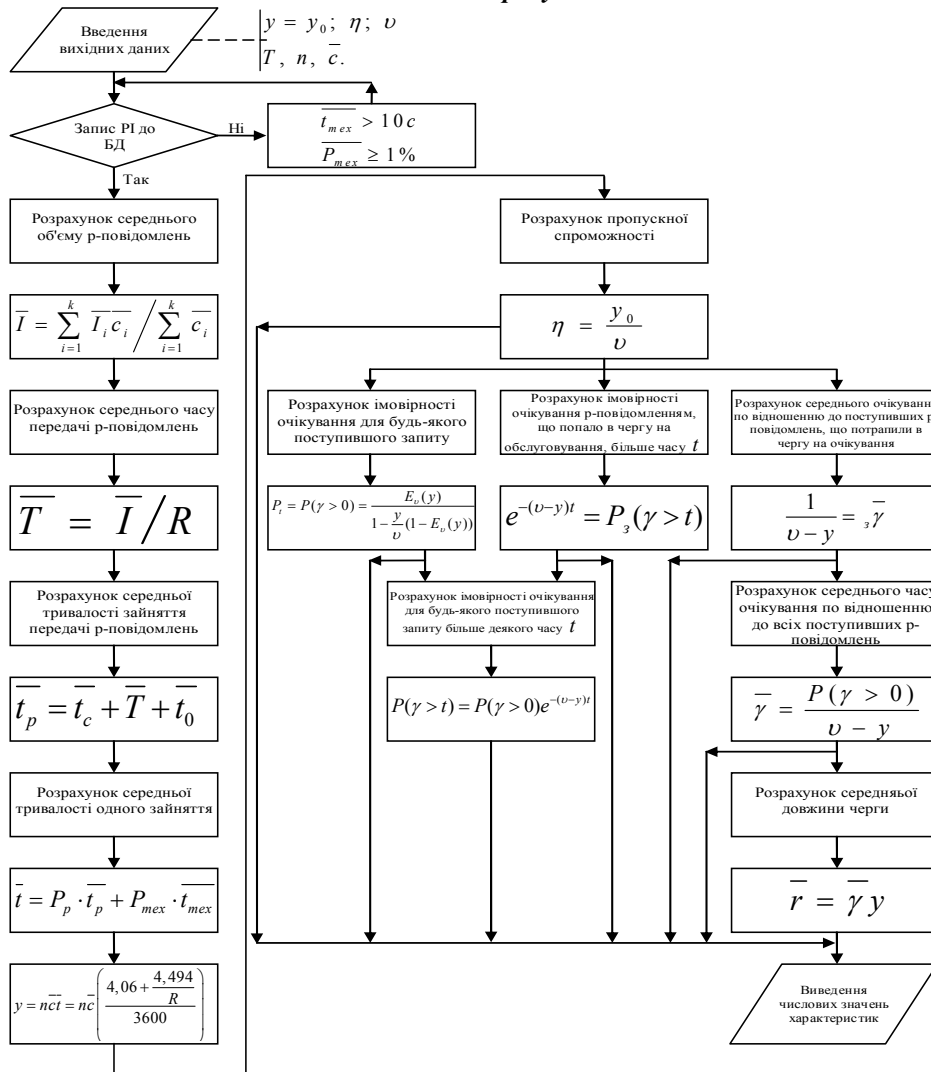


Рис. 3 Алгоритм розрахунку власних характеристик та характеристик якості обслуговування вхідного потоку запитів підсистеми розподілу та зберігання інформації

Таким чином, для удосконаленої методики визначення та розрахунку характеристик передачі інформаційних потоків розроблено алгоритм, що описує кожен крок отримання числових значень характеристик підсистеми розподілу і зберігання інформації ІСППР та характеристик якості обслуговування вхідного потоку даних. Крім того, шляхом розроблення даного алгоритму встановлено взаємозв'язки між характеристиками якості обслуговування вхідного потоку даних, а також яким чином вони слідують із характеристик підсистеми розподілу і зберігання інформації, а саме:

На основі поступаючого (обслуженого) навантаження y_0 визначається пропускна здатність η . Використання отриманих значень для y_0 та η дає можливість визначити такі характеристики якості обслуговування вхідного потоку даних, як: імовірність очікування для будь-

якого поступившого запиту $P(\gamma > t)$; імовірність очікування р-повідомленням, що попало в чергу на обслуговування більше часу $t - P_3(\gamma > t)$, середній час очікування по відношенню до поступивши повідомлень, що потрапили в чергу на очікування ${}_3\bar{\gamma}$.

Шляхом використання отриманих значень $P(\gamma > 0)$ та $P_3(\gamma > t)$ визначається імовірність очікування для будь-якого поступившого запиту більше деякого часу $t - P(\gamma > t)$.

Використанням ${}_3\bar{\gamma}$ визначається середній час очікування по відношенню до всіх поступивши повідомлень $\bar{\gamma}$.

В свою чергу, використання $\bar{\gamma}$ та y_0 дає можливість визначення середньої довжини черги \bar{r} .

5. Результати розрахунків характеристик підсистеми розподілу та зберігання інформації СППР АСУ військами.

Із приведених розрахунків *інтенсивності поступаючого (обслуженого) навантаження* для різних швидкостей обміну даними в СКЗ R слідує наступні висновки:

із збільшенням швидкості передачі даних в КЗ зменшується інтенсивність поступаючого (відповідно і обслуженого) навантаження u ;

величина поступаючого (обслуженого) навантаження обмежується деякою нормованою величиною $u=1,13$, що зумовлене коефіцієнтом 4,06. Фізичний зміст даного коефіцієнта: це час на встановлення зв'язку на запис p -повідомлення та повернення системи в початковий стан після запису;

виходячи з того, що мінімальна величина поступаючого (обслуженого) навантаження не може бути меншою значення $u=1,13$ (для вище заданої кількості засобів добування P_1 в досліджуемій АСУ військами та інформаційного навантаження від них) підсистема розподілу та зберігання інформації при максимальному навантаженні (яке саме і розглядається) буде завантажена на 100%, однак даний факт не означає, що система не буде спроможною відповідати встановленим показникам критеріїв оперативності, оскільки дана СППР є системою з очікуванням, що допускає запис P_1 до бази даних з деякою затримкою в часі без зниження рівня оперативності;

вирішення завдання перевищення значення інтенсивності поступаючого (обслуженого) навантаження при неможливості збільшення швидкості передачі даних в КЗ можливе шляхом збільшення кількості КЗ використовуємих в підсистемі розподілу та зберігання інформації.

Результати розрахунків *пропускної здатності* η , для фіксованих значень швидкості передачі даних (відповідно і поступаючого (обслуженого) навантаження) виявили взаємозалежності груп усіх даних розрахунків, звідки слідує висновок, що із збільшенням кількості СКЗ для фіксованої інтенсивності навантаження, середня пропускна η здатність одного КЗ повно доступного пучка при великих значеннях поступаючого (обслуженого) навантаження u навантаження спочатку стрімко спадає, а потім асимптотично прямує до нуля.

На основі розрахованих даних таких характеристик якості обслуговування вхідного потоку даних, як: імовірність очікування для будь-якого поступившого запиту більше деякого часу t – $P(\gamma > t)$ та імовірність очікування p -повідомленням, що попало в чергу на обслуговування більше часу t – $P_3(\gamma > t)$, можна зробити висновок про наступні закономірності:

із зростанням швидкості передачі даних в СКЗ R при фіксованій ємності повнодоступного пучка

u якість обслуговування покращується, тобто зменшується $P(\gamma > t)$ – відсоток запитів, що очікують початку обслуговування більше деякого часу t для підсистеми розподілу та зберігання інформації по критерію оперативності було прийнято $t=60$ секунд). Так, для пучка ємністю $u=5$ при збільшенні R від 0,4 до $0,5 \frac{\text{Мбайт}}{\text{с}}$ результатом є зменшення $P(\gamma > t)$ з 0,03452 до 0,00072 – в 48 разів;

виходячи з того, що швидкість передачі даних в СКЗ R обернено пропорційна середній тривалості зайняття \bar{t} слідує висновок, що при зменшенні \bar{t} покращується якість обслуговування вхідного потоку p -повідомлень;

із збільшенням швидкості передачі даних в СКЗ R (зменшенні середньої тривалості зайняття \bar{t}) при фіксованій ємності повнодоступного пучка u зменшується значення середньої пропускної здатності η , що припадає на один канал. Так, для пучка ємністю $u=10$ при збільшенні R від 1 до $2 \frac{\text{Мбайт}}{\text{с}}$ результатом є зменшення η з 0,24 Ерл. до 0,175 Ерл. – в 1,37 разів;

із зменшенням середньої величини пропускної здатності η , що припадає на один канал, зменшується імовірність очікування для будь-якого поступившого запиту більше деякого часу t – $P(\gamma > t)$, тобто покращується якість обслуговування. Так, для пучка ємністю $u=2$ при зменшенні η від 0,98 Ерл. до 0,89 Ерл. результатом є зменшення $P(\gamma > t)$ з 0,69039 до 0,10743 – в 6,4 разів;

збільшення кількості СКЗ u в підсистемі розподілу та зберігання інформації покращує якість обслуговування (зменшується імовірність $P(\gamma > t)$). Так, при фіксованій швидкості передачі даних $R=1,5 \frac{\text{Мбайт}}{\text{с}}$ для повнодоступного пучка ємністю $u=2$ $P(\gamma > t)=0,69039$, а для $u=5$ $P(\gamma > t)=0$;

зменшення середньої величини пропускної здатності η , що припадає на один канал, можливе шляхом збільшення кількості СКЗ при незмінних значеннях швидкості передачі даних R (середньої тривалості зайняття \bar{t}). Так, при фіксованій швидкості передачі даних $R=1,5 \frac{\text{Мбайт}}{\text{с}}$ для повнодоступного пучка ємністю $u=2$ $\eta=0,98$ Ерл, а для $u=5$ $\eta=0,39$ Ерл – в 2,5 разів;

якість обслуговування в підсистемі розподілу та зберігання інформації також характеризується $P_3(\gamma > t)$ – імовірністю очікування p -повідомленням, що попало в чергу на обслуговування, більше часу t дана характеристика відноситься лише до запитів, що

відразу потрапляють на очікування). Імовірності $P_3(\gamma > t)$ завжди більші імовірностей $P(\gamma > t)$. Так, при $\nu=2$ та $R=2 \frac{\text{Мбайт}}{\text{с}}$ $P_3(\gamma > t)=0,09271$, а $P(\gamma > t)=0,07627$ – в 1,2 рази.

На основі розрахунків якості обслуговування вхідного потоку даних – *середнього часу очікування по відношенню до всіх поступивших р-повідомлень* $\bar{\gamma}$ слідує висновок, що за одних і тих самих умов (при однакових значеннях швидкості передачі даних R , (середніх час тривалостей зайняття \bar{t}) із збільшенням інтенсивності поступаючого навантаження U на вхід підсистеми розподілу та зберігання інформації зростає середній час очікування по відношенню до всіх поступивших повідомлень $\bar{\gamma}$. Однак, при одночасному збільшенні кількості СКЗ ν в АСУ військами, інтенсивність зростання величини $\bar{\gamma}$ суттєво зменшується. Так, при $u=1,91$ Ерл. для $\nu=2$ $\bar{\gamma}=10,44444$, а $\nu=5$ $\bar{\gamma}=0,01628$ (в 641,55 разів). Це пояснюється тим, що із збільшенням ν зменшується середня пропускна здатність на один канал η , а отже зростають пропускні можливості всієї підсистеми розподілу та зберігання інформації. Крім того, слід зазначити, що при умові виконання нерівності $\eta > 1$ середній час очікування по відношенню до всіх поступивших запитів $\bar{\gamma}$ буде зростати з погано прогнозуємою інтенсивністю та достовірністю, однак можливість в СППР отримання інформації із затримкою в часі не позначиться негативно на оперативності.

Отримані значення *середньої довжини черги* \bar{r} показали, що із збільшенням інтенсивності поступаючого навантаження u на вхід підсистеми розподілу та зберігання інформації зростає середня довжина черги \bar{r} . Однак, при одночасному збільшенні кількості СКЗ ν в АСУ військами, інтенсивність зростання величини \bar{r} суттєво зменшується. Так, при $u=1,91$ Ерл. для $\nu=2$ $\bar{r}=19,94888$, а $\nu=5$ $\bar{r}=0,03109$ (641,65 разів). Це пояснюється тим, що із збільшенням ν зменшується середня пропускна здатність на один канал η , а отже зростають пропускні можливості всієї підсистеми розподілу та зберігання інформації. Крім того, слід зазначити, що при умові виконання нерівності $\eta > 1$ середня довжина

черги \bar{r} буде зростати з погано прогнозуємою інтенсивністю та достовірністю, однак можливість в СППР отримання інформації із затримкою в часі не позначиться негативно на оперативності.

6. Рекомендації по впровадженню результатів розрахунків характеристик підсистеми розподілу та зберігання інформації при розробці АСУ військами.

Ведення операцій (бойових дій) ХХІ століття ставить досить жорсткі вимоги до інформаційних систем управління та розвідки, а також щодо використання всієї повноти їхнього потенціалу. Даний факт потрібно обов'язково врахувати при створенні АСУ ЗС України, що можливо лише при глибокому та всебічному оцінюванні системи на етапі проектування. Так для розглянутої підсистеми розподілу та зберігання інформації СППР із заданими вихідними параметрами, максимальне вхідне навантаження не може становити менше $u=1,13$, однак шляхом застосування розробленого алгоритму удосконаленої методики встановлено, що використання для вхідного потоку дисципліни обслуговування з очікуванням, при функціонуванні в умовах максимального навантаження, не знижує оперативності СППР АСУ військами.

Висновки й перспективи подальших досліджень

Таким чином в статті приведена удосконалена методика визначення та розрахунок власних характеристик підсистеми розподілу та зберігання інформації системи підтримки прийняття рішень автоматизованої системи управління військами та характеристик якості обслуговування інформаційних потоків з метою подальшої практичної реалізації даної підсистеми в інтересах розробки та впровадженні автоматизованої системи управління військами та її функціонування в умовах максимального інформаційного навантаження при різких змінах в оперативній обстановці.

При реалізації удосконаленої методики при проектуванні Єдиної автоматизованої системи управління військами Збройних Сил України буде вирішене актуальне наукове завдання передачі, зберігання та розподілу розвідувальної інформації в автоматизованій системі управління військами органів військового управління.

Література

1. Снявский В. К. Влияние содержания и принципов “сетевидной войны” на процессы управления войсками (силами) // Наука и военная безопасность. - 2010. - №4. 2. Горбунов В. Н. О характере вооруженной борьбы в ХХІ веке // Военная мысль. - 2009. - №3. 3. Гаценко С. С. Єдина автоматизована система управління сектором безпеки і оборони України: ефективність за рахунок гнучкості структури інформаційного забезпечення / О. Ю. Пермяков, І. Д. Варламов, С. С. Гаценко // Збірник матеріалів науково-практичного семінару “Проблемні питання розвитку інформаційного забезпечення Єдиної автоматизованої системи Збройних Сил України”. Київ:

НУОУ, 2013. – С. 11-13. 4. Гаценко С. С. Проблема розподілу інформаційних потоків в автоматизованих системах управління військами (силами) Збройних Сил України / С. С. Гаценко, Ю. М. Кальницький, О. М. Гельвейчук // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ ім. Черняховського – 2014. № 2 (51). – С. 107-112. 5. Гаценко С. С., Варламов І. Д. Аналіз проблем інформаційного забезпечення органів військового управління при плануванні оборонної операції за досвідом проведення Антитерористичної операції на сході України / Варламов І. Д., Гаценко С. С. // Матеріали науково-практичного семінару “Основні

напрямки застосування космічних систем та геоінформаційного забезпечення в інтересах національної безпеки і оборони” – Київ: НУОУ, 2015.– С. 35-41. **6. Гаценко С. С.** Аналіз існуючого стану автоматизованих систем управління військами Збройних Сил України та шляхи їх удосконалення / Гаценко С. С. // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ ім. Черняхівського. – 2015. № 2 (54). – С. 85-91. **7. Нізієнко Б. І.** Напрямки розвитку автоматизованих систем управління, що залучаються до виконання завдань протиповітряної оборони Збройних сил України / Б. І. Нізієнко, В. В. Камінський, О. В. Сісков, Александров О. В. // Збірник наукових праць Харківського університету Повітряних Сил. – 2010. випуск 2(24) С. 18-21. **8. Кириченко І. О., Ярош С. П.** Принципи створення та організації функціонування розвідувально-управляючих інформаційних систем ППО / І. О. Кириченко, С. П. Ярош // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2011. – С. 28-36. **9. Гаценко С. С.** Шляхи удосконалення ведення радіоелектронного моніторингу засобів повітряного нападу / Варламов І. Д., Устименко О. В., Гаценко С. С. // Збірник матеріалів 10 наукової конференції Новітні технології – для захисту повітряного простору.– Харків: ХУПС, 2014.–С. 232-233. **10. Гаценко С. С., Варламов І. Д.** Математична модель нестационарних інформаційних потоків в автоматизованій системі управління військами / Варламов І. Д., Гаценко С. С. // Збірник наукових праць ЦНДІ ОВТ ЗСУ. – 2015 - № 4 (59). – С. 107-112. **11. Гаценко С. С.** Математична модель дисципліни обслуговування інформаційних потоків / Гаценко С. С. // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ ім. Черняхівського. – 2015. № 3 (55). – С. 70-78. **12. Зотова І. Г.** Стан та перспективи розвитку автоматизованих систем управління військами (зброєю) передових країн світу / Зотова І. Г., Голобородько М. Ю., Поривай О. В. // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України. - К: ЦВСДНУОУ, 2013. -№ 2 (48). – С. 33-36. **13. Янов О.**

Система боевого управления Сухопутных войск США в звене “Бригада и ниже” / Янов О. // Зарубежное военное обозрение. - 2012. -№ 2. - С. 43-50. **14. Янов О.** Сухопутные войска США: основные направления строительства / Янов О. // Основные направления строительства// Зарубежное военное обозрение. -2012. - № 7. -С. 21-27. **15. Пашетник О. Д.** Аналіз світових тенденцій розвитку автоматизованих систем управління військами і зброєю / Пашетник О. Д. // Наука і техніка Повітряних Сил Збройних Сил України, 2015, -№2(19). - С. 64-68. **16. Гаценко С. С., Варламов І. Д.** Удосконалення інформаційного забезпечення органів військового управління в інтересах сектору безпеки та оборони держави / Варламов І. Д., Гаценко С. С. // Збірник матеріалів міжнародної науково-практичної конференції Проблеми будівництва сектору безпеки і оборони України та шляхи їх вирішення.– Київ: НУОУ, 2016.–С. 136-138. **17. Плуговий Ю. А.** Сучасний стан та перспективи розвитку системи зв'язку Збройних Сил України / Плуговий Ю. А. // Збірник матеріалів VIII Науково-практичної конференція „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення з урахуванням досвіду АТО”.– Київ: ВІТІ, 2015.–С. 31-33. **18. Драглюк О. В., Івахненко Т. О., Шугалій О. О.** Проблемні питання застосування інформаційних систем для забезпечення процесів управління під проведення АТО та шляхи їх вирішення / Драглюк О. В., Івахненко Т. О., Шугалій О. О. // Збірник матеріалів VIII Науково-практичної конференція „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення з урахуванням досвіду АТО”. – Київ: ВІТІ, 2015.–С. 94-95. **19. Макаруч О. М., Наконечна А. М.** Застосування систем супутникового зв'язку під час проведення антитерористичної операції / Макаруч О. М., Наконечна А. М. // Збірник матеріалів VIII Науково-практичної конференція „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення з урахуванням досвіду АТО”.– Київ: ВІТІ, 2015.– С. 127-129. **20. Лившиц Б. С.** Теорія телетрафіка / Лившиц Б. С., Учебник для вузов. 2-е изд., перераб. и доп. М.: Связь, 1979. 224 с.

МЕТОДИКА ОПРЕДЕЛЕНИЯ И РАСЧЕТА ХАРАКТЕРИСТИК ПОДСИСТЕМЫ РАСПРЕДЕЛЕНИЯ И ЗБЕРЕЖЕНИЯ ИНФОРМАЦИИ СИСТЕМЫ ПОДДЕРЖКИ И ПРИНЯТИЯ РЕШЕНИЙ

*Сергей Станиславович Гаценко
Елена Михайловна Наумчак*

*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина
Воинская часть А1586, Житомир, Украина*

В статье проводится определение и расчет собственных характеристик подсистемы распределения и хранения информации системы поддержки принятия решений автоматизированной системы управления войсками и характеристик качества обслуживания информационные потоки с целью дальнейшей практической реализации данной подсистемы в интересах разработки и внедрении автоматизированной системы управления войсками и ее функционирования в условиях максимального информационного нагрузки при резких изменениях в оперативной обстановке.

Ключевые слова: система поддержки принятия решений; характеристики; автоматизированная система управления войсками; информационные потоки.

METHOD OF CALCULATION AND DETERMINATION OF THE SUBSYSTEM DISTRIBUTION AND STORAGE OF INFORMATION SYSTEMS AND DECISION SUPPORT

*Serhiy S. Hatsenko
Olena M. Naumchak*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine
Military unit A1586, Zhytomyr, Ukraine*

In the article the definition and calculation of own characteristics of subsystems distribution and storage system to support decision-making automated system and characteristics of service quality information flows to further the practical implementation of subsystems for the benefit of developing and implementing the automated system and its operation under conditions of maximum information loads with sharp changes in the operational environment.

Keywords: decision support system; features; automated system; information flows.

References

- 1. Synyavskyy V.K.** (2010), Influence of the content and principles of "network-centric warfare" on the command and control processes (forces). [*Vlyyanye soderzhannya y pryntsyypov "setetsentrycheskoy voynu" na protsessu upravleniyya voyskamy (sylamy)*], Nauka y voennaya bezopasnost. No. 4. **2. Gorbunov V.N.** (2009), About the nature of warfare in the XXI century. [*O haraktere vooruzhennoy borby v XXI veke*], Voennaya mysl, No.3.
- 3. Hatsenko S.S.** (2013), The only automated system of the security sector in Ukraine: efficiency through flexible structure of information provision. [*Yedyna avtomatyzovana sistema upravlinnya sektorom bezpeky i oborony Ukrainy: efektyvnist' za rakhunok hnuchkosti struktury informatsiyного zabezpechennya*], Permyakov O.Yu., Varlamov I.D., Zbirnyk materialiv naukovopraktychnoho seminaru Problemni pytannya rozvytku informatsiyного zabezpechennya Yedynoyi avtomatyzovanoi systemy Zbroynykh Syl Ukrainy. Kyiv: NUOU, pp. 11-13.
- 4. Hatsenko S.S.** (2014), The problem of the distribution of information flow in automated control systems of troops (forces) of the Armed Forces of Ukraine. [*Problema rozpodilu informatsiyных potokiv v avtomatyzovanykh systemakh upravlinnya viys'kamy (sylamy) Zbroynykh Syl Ukrainy*], Kal'nyts'kyy Yu.M., Hel'veychuk O.M., Zbirnyk naukovykh prats' Tsentru voyenno-stratehichnykh doslidzhen' NUOU im. Chernyakhov's'koho, No.2 (51), pp. 107-112. **5. Hatsenko S.S.**, Varlamov I.D. (2015), Analysis of problems of information support of command and control in the planning of defense operations for the experience of anti-terrorist operation in eastern Ukraine. [*Analiz problem informatsiyного zabezpechennya orhaniv viys'kovoho upravlinnya pry planuvanni oboronnoyi operatsiyi za dosvidom provedennya Antyterrorystichnoyi operatsiyi na skhodi Ukrainy*], Materialy naukovopraktychnoho seminaru Osnovni napryamky zastosuvannya kosmichnykh system ta heoinformatsiyного zabezpechennya v interesakh natsional'noyi bezpeky i oborony, Kyiv: NUOU, pp. 35-41.
- 6. Hatsenko S.S.** (2015), Analysis of the current state of automated control systems for the Armed Forces of Ukraine and ways to improve them. [*Analiz isnyuchoho stanu avtomatyzovanykh system upravlinnya viys'kamy Zbroynykh Syl Ukrainy ta shlyakhy yikh udoskonalennya*], Zbirnyk naukovykh prats' Tsentru voyenno-stratehichnykh doslidzhen' NUOU im. Chernyakhov's'koho, No. 2 (54), pp. 85-91. **7. Niziyenko B.I.** (2010), Areas of automated control systems involved in the tasks of air defense Armed Forces of Ukraine. [*Napryamky rozvytku avtomatyzovanykh system upravlinnya, shcho zaluchayut'sya do vykonannya zavdan' protypovitryanoi oborony Zbroynykh syl Ukrainy*], Kamins'kyy V.V., Siskov O.V., Aleksandrov O.V., Zbirnyk naukovykh prats' Kharkiv's'koho universytetu Povitryanykh Syl, No. 2(24) pp. 18-21. **8. Kyrychenko I.O.**, Yarosh S.P. (2011), The principles of creation and operation of surveillance and control information systems defense. [*Pryntsypy stvorennya ta orhanizatsiyi funktsionuvannya rozviduval'no-upravlyayuchykh informatsiyных system PPO*], Nauka i tekhnika Povitryanykh Syl Zbroynykh Syl Ukrainy, Kharkiv: KhUPS, pp. 28-36. **9. Hatsenko S.S.** (2014), Ways of improving the conduct of electronic monitoring of air attack. [*Shlyakhy udoskonalennya vedennya radioelektronnoho monitorynhu zasobiv povitryanoho napadu*], Varlamov I.D., Ustymenko O.V., Zbirnyk materialiv 10 naukovoyi konferentsiyi Novitni tekhnolohiyi – dlya zakhystu povitryanoho prostoru, Kharkiv: KhUPS, pp. 232-233. **10. Hatsenko S.S.**, Varlamov I.D. A mathematical model of unsteady flow of information in automated system. [*Matematychna model' nestatsionarnykh informatsiyных potokiv v avtomatyzovaniy systemi upravlinnya viys'kamy*], Zbirnyk naukovykh prats' Tsentru voyenno-stratehichnykh doslidzhen' NUOU im. Chernyakhov's'koho, No.3. **11. Hatsenko S.S.** (2015), Mathematical model of discipline service information flow. [*Matematychna model' dystsypliny obsluhovuvannya informatsiyных potokiv*], Zbirnyk naukovykh prats' Tsentru voyenno-stratehichnykh doslidzhen' NUOU im. Chernyakhov's'koho, No.3 (55), pp. 70-78. **12. Zotova I.H.** (2013), State and prospects of development of automated control of troops (arms) advanced countries. [*Stan ta perspektyvy rozvytku avtomatyzovanykh system upravlinnya viys'kamy (zbroyeyu) peredovykh krayin svitu*], Holoborod'ko M.Yu., Poryvay O.V., Zbirnyk naukovykh prats' Tsentru voyenno-stratehichnykh doslidzhen' Natsional'noho universytetu oborony Ukrainy, Kyiv: TsVSDNUOU, No.2 (48), pp. 33-36. **13. Yanov O.** (2012), US Ground Forces command and control system in the link "brigade and below". [*Sistema boevogo upravlinnya Suhoputnykh voysk SShA v zvene "Brigada i nizhe"*], Zarubezhnoe voennoe obozrenie, No.2, pp. 43-50. **14. Yanov O.** (2012), US Army: the main directions of construction. [*Suhoputnyye voyska SShA: osnovnyie napravleniya stroitelstva*], Osnovnyie napravleniya stroitelstva, Zarubezhnoe voennoe obozrenie, No.7, pp. 21-27. **15. Pashchetnyk O.D.** (2015), Analysis of world trends in the development of automated control of troops and weapons. [*Analiz svitovykh tendentsiy rozvytku avtomatyzovanykh system upravlinnya viys'kamy i zbroyeyu*], Nauka i tekhnika Povitryanykh Syl Zbroynykh Syl Ukrainy, No.2(19), pp. 64-68. **16. Hatsenko S.S.**, Varlamov I.D. (2016), Improving information support of command and control in the interests of the security sector and defense. [*Udoskonalennya informatsiyного zabezpechennya orhaniv viys'kovoho upravlinnya v interesakh sektoru bezpeky ta oborony derzhavy*], Zbirnyk materialiv mizhnarodnoyi naukovopraktychnoyi konferentsiyi Problemy budivnytstva sektoru bezpeky i oborony Ukrainy ta shlyakhy yikh vyrishennya, Kyiv: NUOU, pp. 136-138. **17. Pluhovyy Yu.A.** (2015), The current state and prospects of development of the Armed Forces of Ukraine communication. [*Suchasnyy stan ta perspektyvy rozvytku systemy zv'yazku Zbroynykh Syl Ukrainy*], Zbirnyk materialiv VIII Naukovopraktychnoyi konferentsiyi „Priorityetni napryamky rozvytku telekomunikatsiyных system ta merezh spetsial'noho pryznachennya z urakhuvanniam dosvidu ATO”, Kyiv: VITI, pp. 31-33. **18. Drahlyuk O.V.**, Ivakhnenko T.O., Shuhaliy O.O. (2015), Problems of the use of information systems to provide for the management of ATO during and solutions. [*Problemni pytannya zastosuvannya informatsiyных system dlya zabezpechennya protsesiv upravlinnya pid provedennya ATO*], Zbirnyk materialiv VIII Naukovopraktychnoyi konferentsiyi „Priorityetni napryamky rozvytku telekomunikatsiyных system ta merezh spetsial'noho pryznachennya z urakhuvanniam dosvidu ATO”, Kyiv: VITI, pp. 94-95. **19. Makarchuk O.M.**, Nakonechna A.M. (2015), The use of satellite communications during the antiterrorist operation. [*Zastosuvannya system suputnykovoho zv'yazku pid chas provedennya antyterrorystichnoyi operatsiyi*], Zbirnyk materialiv VIII Naukovopraktychnoyi konferentsiyi „Priorityetni napryamky rozvytku telekomunikatsiyных system ta merezh spetsial'noho pryznachennya z urakhuvanniam dosvidu ATO”, Kyiv: VITI, pp. 127-129. **20. Livshits B.S.** (1979), Teletraffic Theory. [*Teoriya teletrafika*], Pshenichnikov A.P., Harkevich A.D. Uchebnik dlya vuzov. 2-e izd., pererab. i dop. Moscow: Svyaz., 224 p.

Отримано: 04.08.2016 року.

СОЦІОНІЧНО-ІНФОРМАЦІЙНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ АВІАЦІЙНО-КОСМІЧНОЇ БОЙОВОЇ СИСТЕМИ

Розглянуті питання методології забезпечення функціональної стійкості складних систем. Показано, що в складних організаційних ерготехнічних системах важливе місце в забезпеченні їх функціональної стійкості займатимуть процеси інформаційного метаболізму в системі. На основі соціонічного підходу до функціонування складних систем, визначені закономірності бойової роботи операторів системи, що задовольняють умовам забезпечення функціональної стійкості авіаційно-космічної бойової системи. Наведені критерії оцінки ефективності роботи оператора та показана можливість проведення процедури валідації тезаурусу авіаційно-космічної бойової системи. Запропоновано визначення вирішальної функції як результуючої функціонування тезаурусу, внаслідок чого обирається варіант застосування угруповання за призначенням.

Ключові слова: соціоніка; функціональна стійкість; авіаційно-космічна бойова система.

Вступ

Постановка проблеми. Сучасними закономірностями збройної боротьби, які визначені змінами в озброєнні і способах ведення бойових дій можна вважати:

ведення збройної боротьби із застосуванням засобів нового технологічного рівня з використанням сучасних авіаційно-космічних та інформаційних технологій і широким застосуванням високоточних засобів ураження, систем управління військами, розвідки та інших систем забезпечення;

ураження на відповідних етапах бойових дій у першу чергу не угруповань сухопутних військ, а систем їх матеріально-технічного забезпечення, важливих центрів державного та військового управління, об'єктів військово-промислового комплексу.

Аналіз останніх досліджень і публікацій.

Аналіз війн та конфліктів кінця ХХ-го початку ХХІ-го сторіччя показує, що на сьогоднішній день провідними в військовому та економічному положенні державами створена глобальна інформаційна система космічного базування квазіреального масштабу часу, яка дозволяє використовувати збройні сили практично у будь-якій точці земної кулі. Ця система удосконалюється у напрямках підвищення розрізняючої здатності, швидкості доставки і обсягу інформації, гнучкості управління і маневреності. При цьому, для забезпечення швидкості функціонування здійснюється перехід від багатofункціональних (великих за розміром) до вузькопрофільованих космічних апаратів (міні і мікросупутники), що, безумовно призводить до ускладнення систем бойового застосування військ (сил).

Все це на даний час призвело до виникнення нових організаційних структур у складі збройних

сил провідних держав – авіаційно-космічні експедиційні сили (США), повітряно-космічні сили (РФ).

Подальший розвиток воєнних дій експерти пов'язують з підвищенням ефективності застосування сил та засобів оперативного та тактичного призначення на підставі подальшого удосконалення засобів космічного забезпечення, концепції розвитку “малих супутників”, розробки та застосування засобів ураження з космічним базуванням [1].

Сучасні бойові дії є мережецентричними та гібридними, що висуває нові вимоги до підготовки і застосування угруповань військ (сил), як складних ерготехнічних систем.

По перше, потрібно створити ефективні інформаційні комплекси, реалізованих у засобах розвідки й управління, а також у силах і засобах РЕБ. Космічні засоби розвідки поступово стають основним джерелом інформації як під час планування, так і під час організації і ведення бойових дій. [2, 3].

По друге, управління військами здійснюється в умовах лавиноподібного збільшення потоків інформації через велику кількість ліній зв'язків з командних пунктів на землі, але через повітряно-космічні засоби. При цьому значно збільшиться кількість літаків управління і дальнього радіолокаційного виявлення, тобто ускладнюється елементний склад системи. Інформаційний обмін відбувається між усіма ланками і рівнями командування за допомогою автоматичних чи автоматизованих систем, які поступово переміщуються на повітряні і космічні засоби.

Ці характерні риси збройної боротьби дають нам підстави дійти висновку, що для досягнення рішучої переваги над противником та стратегічних цілей війни [2] потрібно проводити руйнування інформаційного поля противника і збереження свого інформаційного поля.

Виклад основного матеріалу дослідження

Ведення бойових дій у нових умовах потребує нової парадигми з такими основними положеннями [4]:

кожен компонент системи є важливим для визначення результату;

передбачувані та непередбачувані явища співіснують і взаємодіють, приводячи до створення комплексних мереж із величезною кількістю змінних величин, що унеможлиблює прогнозування результату;

незначна зміна в системі входу може привести до непропорційно великих змін у результатах;

системи постійно еволюціонують;

комплексні системи через вплив викликів здатні реорганізовуватися.

Суперництво або бойові дії в межах цієї парадигми найімовірніше здатні набути форми інформаційної війни – конфлікту, пов'язаного з інформацією на стратегічному рівні (між державами або суспільствами).

Одним із чинників інформаційної війни є необхідність знання архітектури і параметрів ворожої системи. Сторона, яка краще розуміє мотивацію, структуру і мету ворога, краще підготовлена до конфлікту.

Виходячи з наведеного, можна сказати, що ведення сучасних бойових дій комплексний та динамічний процес великої складності. У попередніх дослідженнях [5] доводиться, що військове угруповання за своїми ознаками є складною ерготехнічною системою і може бути розкладено на низку підсистем, які функціонують заради досягнення єдиної мети. Сукупність організаційно пов'язаних елементів, що ведуть та забезпечують бойові дії угруповання авіації та космічних засобів в інтересах Збройних Сил, пропонується називати авіаційно-космічною бойовою системою (АБС).

При цьому АБС структурно складається з авіаційних частин (які в свою чергу – з ескадрилій, літаків, льотчиків), космічних засобів (спутників різного призначення, космічних кораблів – пілотованих та непілотованих), сил і засобів забезпечення та управління.

Як видно з наведеного, при незмінності форм та способів застосування, ефективність застосування АБС зростає за рахунок вдосконалення структури та функціональних зв'язків між елементами системи. Однією із важливіших властивостей системи є її стійкість, тобто здатність системи зберігати свої властивості, функції та задану ступінь ефективності застосування при впливі противника та структурній деградації системи.

Необхідною та достатньою умовою функціональної стійкості АБС можна покласти існування такого складу елементів і зв'язків між ними, при якому система продовжує виконувати хоча б мінімально необхідні функції з заданою ефективністю, а також мала б достатню

надмірність для парирування наслідків структурної деградації.

Тобто, необхідно виявити надмірність системи (структурну, інформаційну, енергетичну, функціональну, часову та ін.) та реалізувати шляхом перерозподілу ресурсів в системі.

З метою вирішення проблеми забезпечення функціональної стійкості АБС пропонується підхід, який містить в собі сукупність математичних моделей, необхідних і достатніх умов функціональної стійкості, ознак, показників, критеріїв, області, границі і запасу функціональної стійкості системи, та який може бути застосованим для будь-яких складних людино-машинних систем з інтенсивно циркулюючою інформацією. Цей підхід базується на концепції забезпечення функціональної стійкості, яка передбачає забезпечення оптимального (субоптимального) рівня циркулюючої в системі інформації та максимального рівня засвоєння інформації керуючим елементом (так званого тезаурусу системи). Валідація тезаурусу дозволяє ефективніше використовувати існуючу надмірність та за рахунок цього підвищити значення показників функціональної стійкості до необхідного рівня без значних витрат [6].

Крім того, АБС - єдина поліергатична та ерготехнічна система, тому об'єднання людини і технічних засобів доцільно ґрунтувати на концепції цілісності, що передбачає створення органічно-цілісних структур, функціональні властивості яких принципово сприяють безпомилковій роботі особи-оператора. Основною методологією цілісної побудови АБС є організмичний підхід, суть якого полягає у використуванні досягнень еволюції живих організмів для побудови людино-машинних систем. Правомірність такого підходу обґрунтована тим, що в існуючому середовищі (природному і штучному) є самі різні системи (організми), що досягають власну мету, борються за своє існування, але підкоряються загальним, неминучим і єдиним законам природи [7].

Застосовуючи організмичний підхід, можна дійти наступних результатів [8]. Поведінка оператора при виконанні обов'язків чи веденні бойової роботи (БР) визначається моделлю зовнішнього світу, що опрацьовується ним на основі придбаних знань, проведеної підготовки, тренувань, випробувань, проб і помилок, аналогій і т.п. Деталізація моделі зовнішнього світу, ступінь її спільності і адекватності залежить від конкретної особи, тобто внутрішнього світу оператора. Відношення внутрішнього і зовнішнього світів конкретного оператора визначають його власне "Я" і його типологічні характеристики. Підсвідомо, але широко що використовуються оператором образи зовнішнього світу сприяють великій гнучкості в способах переробки ним інформації. В цьому ж і причина можливості рішення оператором іноді нечітко сформульованих задач, що стосуються проведення

БР. Оператор усвідомлено або неусвідомлено доповнює постановку задачі, виходячи з своєї моделі (образу) зовнішнього світу, точніше, його частини, що включає все, що стосується постановки і проведення БР. Оператор виступає також в ролі “цільового фільтру” можливих варіантів рішення при проведенні БР. Варіації реальних умов проведення експерименту умножають можливі варіанти його проведення, а комбінації варіантів по деталях і умовах роблять число рішень вельми значним. Оператор, користуючись своїми моделями зовнішнього і внутрішнього світів, враховуючи поставлену мету, зменшує безліч варіантів рішення задачі до практично прийняттого числа. Прикладом цільової фільтрації є такий сенсор як око людини, яка сприймає своїми чутливими елементами (рецепторами) не менше 10 гігабіт/сек інформацію, з яких в мозок передається лише 10-20 біт/сек. При цьому відбирається інформація лише потрібна для задачі, вирішуваної в даний момент.

Крім цільової фільтрації для оператора характерна і функція звичайної фільтрації шумів, перешкод. Загальна структура функцій оператора може бути схемно представлений наступними його фазами взаємодії з технічною частиною системи [8]:

сенсорні входи (зір, слух, дотик, нюх, смак) забезпечують виявлення і прийом індикаторних сигналів від деякої сукупності пристроїв довільної природи, через які оператору пред'являється службова інформація, і описуються вхідними змінними;

вирішальна функція (аналітичні відділи центральної нервової системи та пам'ять); забезпечує визначення інформації, яку несуть сигнали, необхідні розрахунки, оцінки і логічні операції, внаслідок чого знаходиться рішення виникаючої задачі, а потім відбувається пошук засобів реалізації рішення;

моторні виходи (рухи, мова) ведуть до реалізації результату рішення і описуються вихідними змінними.

Вирішальна функція є відображенням безлічі вхідних змінних на безліч змінних вихідних. Така інтерпретація корисна для побудови математичної моделі операторської діяльності льотчика або члена розрахунку пункту управління, але вона є зовнішньою узагальненою характеристикою оператора. Внутрішню його характеристику зручно давати в термінах “інформаційного метаболізму”.

Суть теорії інформаційного метаболізму полягає в тому, що “зовнішні інформаційні сигнали, що приймаються психікою, уподібнюються їжі, яку для процесу енергетичного метаболізму одержує організм, тобто, як їжа необхідна для енергетичного метаболізму організму, так і інформаційні сигнали для інформаційного метаболізму психіки”. А. Аугустінавічюте [9], використовуючи теорію

інформаційного метаболізму, удосконалила психологічну типологію К.Г. Юнга і тим самим створила науку, яку назвала соціонікою або теорією типів інформаційного метаболізму. Згідно А. Аугустінавічюте, основна відмінність між типами людей - різниця в способах і характері обміну інформацією із зовнішнім світом: “Одні з них краще відбирають з оточення одні сигнали, інші - інші. Що доступно одним, недоступно іншим”. Безліч вхідних сигналів, що поступають людині, розщеплюється його психікою на складові, причому функції Юнга (логіка - етика, інтуїція - сенсорика, в термінах соціоніки) забезпечують фільтрацію, яка згадується вище.

Спробуємо тепер перевести опис “інформаційного метаболізму” оператора з внутрішньої мови соціоніки на зовнішню мову вирішальної функції, тобто відображення вхідних змінних в змінні вихідні. Шукане відображення починається з виявлення і прийому сигналу сенсорним входом і зводиться до введення в дію керуючих пристроїв, а також до безпосереднього відчуття сигналу, що вимагає збудження пам'яті і аналітичних відділів центральної нервової системи. При виявленні сигналу оператор встановлює його ознаки, що відрізняють даний сигнал від всіх інших. Прийом (сприйняття) сигналу, несучого інформацію про хід БР і умови його проведення, супроводжується звичайно отриманням інформації у вигляді завдань і вказівок оператора ПУ. Далі відбувається визначення повідомлення: отримання повідомлювальної інформації, чи співвідноситься сигнал з ознакою явища (образу), інформація про яке повинна передаватися. За цим етапом слідує аналіз інформації, що поступила, на основі наявних знань про закономірності протікання процесу.

Рішення задачі, що виникає як результат отримання повідомлювальної інформації, включає в необхідних випадках обчислення і логічні висновки. Цей процес характерний інтенсивним обміном інформацією між основними відділами головного мозку і підвищеними вимогами до об'єму оперативної пам'яті оператора. Тому не тільки для проведення БР, але і для всієї діяльності операторів використовуються інструкції, схеми і т.п. Відзначимо причини, що впливають на процес “інформаційного метаболізму” [10]:

емоційні (швидкі і нестійкі зміни перетворюючих властивостей оператора, викликані сильно діючими зовнішніми або внутрішніми причинами);

інтуїтивні (досвід, що не формалізується у вирішальній функції оператора);

еволюційні (повільні зміни перетворюючих властивостей оператора в результаті навчання, тренувань або забувають).

Дії цих причин можуть викликати:

втрату частини корисної інформації;

неадекватність перетворення інформації (залежить від соціонічного типу оператора);

внесення додаткової (корисної або шкідливої) інформації, що безпосередньо не міститься в тій, що поступає на сенсорний вхід сигналі (позитивний досвід і інтуїція або, навпаки, закріплені помилкові уявлення і навик), причому ця інформація може як збільшувати, так і компенсувати спотворення.

Процес формулювання рішення є виразом рішення на мові моторних виходів оператора (рух і мова). Результатом є формування, а потім видача командної інформації (вихідних змінних).

Приведений короткий опис структури вирішальної функції показує, що в навіть дуже простому випадку прийому сигналу сенсорним входом і перетворення його в моторний вихід є достатньо складним не всі механізми вказаних процесів достатньо вивчені. Проте, потрібні практичні функціональні критерії оцінки взаємодії оператора з технічними приладами.

Очевидно, такі критерії повинні об'єднувати показники, що характеризують сенсорні входи, вирішальну функцію і моторні виходи оператора.

“Інформаційний метаболізм” міг би служити одним з таких показників, якби не відсутність кількісної міри для нього.

Проте можна спробувати ввести ряд оцінюваних, а краще - вимірних параметрів “інформаційного метаболізму”. Соціонічна характеристика оператора є таким оцінюваним параметром. Але існують і вимірні параметри:

- кількість інформації, яку повинен обробити оператор при проведенні БР

$$I(t) = I_c(t) + I_p(t) + I_m(t), \quad (1)$$

де $I(t)$ - кількість статистичної інформації Шеннона-Вінера;

$I_c(t)$ - кількість інформації, сприйнята сенсорним входом;

$I_p(t)$ - кількість інформації, що використовується вирішальною функцією;

$I_m(t)$ - кількість інформації, формована для моторного виходу;

t - поточний час.

Число керуючих рухів у оператора обмежено. Тіло людини по своїй природі в природних умовах здатний виконувати від 10 до 20 різних керуючих рухів одночасно тоді як при управлінні різними системами і механізмами може скоювати одночасно не більше двох рухів.

Моторні виходи оператора при виконанні БР фактично зводяться в кожний момент до одного руху і мови. Мову можна описувати через інформаційні характеристики (швидкість подачі інформації, коефіцієнт втрат інформації, залежний від виразності мови, і т.д.). Але вимірні параметри рухів оператора вимагається встановлювати експериментально. Вимірним параметром моторних виходів оператора можуть служити:

число і характер рухів, супутніх процесу обробки інформації;

точність дій оператора.

Відзначені вимірні параметри дозволяють сформулювати критерії ефективності проведення БР оператором. Введемо наступні критерії ефективності дій оператора.

Критерій перший - час дій оператора

$$\tau_{оп} = \alpha I(t) + \tau_m, \quad (2)$$

де $\tau_{оп}$ - час дій оператора;

$I(t)$ - кількість інформації, що визначається за формулою (1);

t - час;

α - коефіцієнт стиснення/розширення часу виконання вирішальної функції;

τ_m - час, затрачуваний на моторні реакції, супутні обробці інформації $I(t)$.

Час $\tau_{оп}$, затрачуване оператором на проведення тих або інших операцій при проведенні БР, виявляється одним з найважливіших критеріїв в умовах бойової діяльності, де час є надзвичайно дорогим і обмеженим ресурсом. Проте практичне застосування даного критерію вимагає високої досконалості методик враховуючи відсутність кількісних заходів для багатьох психологічних характеристик оператора. Насправді, коефіцієнт α є функцією ряду параметрів, деякі з яких не формалізовані

$$\alpha = f(\beta, \kappa, \lambda, \sigma, \mu, \pi, \varepsilon, \gamma, \phi, \omega), \quad (3)$$

де β - значущість і цінність інформації, що приймається;

κ - спосіб кодування інформації (структура сигналу);

λ - вид алгоритму роботи;

σ - сенсорні властивості оператора;

π - обсяг і властивості пам'яті;

ε - адаптивні якості;

γ - тип мислення;

ϕ - показник стомлюваності;

ω - показник емоційної сфери.

Час τ_m - функція від тих же параметрів, і крім того від характеристик рухових реакцій μ оператора

$$\tau_{оп} = f(\beta, \kappa, \lambda, \sigma, \mu, \pi, \varepsilon, \gamma, \phi, \omega), \quad (4)$$

де μ - характеристики моторних, переважно рухових реакцій (число і характер рухів, точність дій оператора).

Розглянемо тепер параметр μ , звівши його для простоти до точності дій оператора. Під точністю розумітимемо ступінь наближення параметрів, що характеризують ергатичну систему проведення БР. Її визначимо величиною, зворотною до погрішності δ :

$$\delta = |x - x_0| = 1/\mu, \quad (5)$$

де x і x_0 - відповідно поточне і задане значення певного параметра.

На значення δ , а значить, і на точність μ дій оператора впливають стан зовнішнього

середовища, взаємодія ергатичних та технічних елементів АБС, а також час $\tau_{оп}$.

Погрішності, що допускаються оператором в процесі роботи, звичайно випадкові по величині і підкоряються нормальному закону розподілу, проте, можуть мати місце і інші закони розподілу залежні від соціонічного типу оператора у зв'язку з дорученням йому проводити БР певного вигляду. Тут може мати місце скорочення і спрощення сигналу, втрата подробиць спотворення вихідного сигналу у бік більш "правильного, симетричного сигналу", перебільшення одних відмінностей в сигналах і зменшення інших. Зустрічається зсув до центральної тенденції: наприклад більш довгі вхідні сигнали скорочуються, а більш короткі подовжуються. Може відбуватися спотворення сигналу минулих подій, наприклад, почастішання помилкових фіксацій якогось явища (індикації, звукових сигналів) після вказівки на пропуск.

Помітимо, що хоча параметр μ входить як аргумент в першій критерій ефективності τ_{II} , його можна застосовувати і як самостійний другий критерій, оскільки, фактично, це основна кваліфікаційна характеристика. Очевидно, що зміна вимог до точності δ до однієї і тієї ж діяльності різко змінює її характер.

Критерій третій - інформаційна пропускна спроможність оператора. Формула для оцінки пропускної спроможності має вигляд

$$\rho = I(t) / \tau_{оп}, \quad (6)$$

де $I(t)$ - кількість інформації, визначувана формулою (1);

$\tau_{оп}$ - час дій оператора, що визначається за формулою (2).

Не слід змішувати поняття пропускної спроможності і продуктивності, що визначається за формулою

$$v = I_c(t) / \tau_{оп}, \quad (7)$$

Критерій четвертий - надійність оператора. Оцінюватимемо надійність через вірогідність $q(t)$

виникнення помилки в процесі сприйняття інформації (сенсорна помилка), при ухваленні рішення (аналітична, логічна або обчислювальна помилка), при передачі інформації на моторні виходи (моторна помилка).

Таким чином, можна припустити, що для забезпечення функціональної стійкості АБС потрібно реалізовувати інформаційну надмірність, яка максимізується при врахуванні особливостей функціонування ергатичної частини системи (операторів), а саме оптимізації вирішальної функції оператора залежно соціонічного типу. Час, що витрачається на формування моторних виходів, визначається пропускною спроможністю оператора і також повинен бути оцінений експериментально як для рухових, так і для мовних реакцій. Необхідно експериментальним шляхом встановити вплив на надійність оператора його сенсомоторних можливостей, об'єму пам'яті, властивостей мислення, емоційної стійкості, а також компенсаторних можливостей, що виявляється в тим більшому ступені, чим вище рівень підготовки оператора, більше його досвід по виконанню тих або інших операцій і уміння знаходити способи отримання бракуючої інформації.

Висновки й перспективи подальших досліджень

Використовуючи наведений підхід, можливо провести процедуру поетапної валідації тезауруса АБС, як сукупності інформації, знань та понять операторів, що проводять БР певного вигляду. Ця процедура дозволить встановити значущі зв'язки між елементами тезаурусу, зменшити невизначеність в системі, підвищуючи її надійність, швидкість реагування на збурюючі впливи, економність витрати ресурсів що базується на особливостях перерозподілу інформації в системі та забезпечити АБС властивість функціональної стійкості при виконанні завдань за призначенням.

Література

1. **Комаров В. С.** Аналіз застосування космічних засобів в інтересах ведення збройної боротьби. // Системи озброєння і військова техніка, 2007, випуск 1(9) – с.34-37. 2. **Пермяков О. Ю.** Інформаційні технології та сучасна збройна боротьба / О. Ю. Пермяков, А. І. Сбітнев. – Луганськ: Знання, 2008. – 204 с. 3. **Кларк Р.** Третья мировая война: какой она будет? / Р. Кларк, Р. Нейк; пер. с англ. Е. Карманова. – СПб.: Питер, 2011. – 336 с. 4. **Пермяков О. Ю.** Використання інформаційних технологій та застосування космічних систем в інтересах військ (сил): підручник / [О. Ю. Пермяков, В. Г. Солонніков, Ю. Б. Прибілев та ін.] – К.: НУОУ ім. Івана Черняхівського, 2014. – 208 с. 5. **Воронин А. Н., Зиятдинов Ю. К., Харченко А. В., Осташевский В. В.** Сложные технические и эргатические системы: методы исследования. – Х.: Факт, 1997. – 240 с. 6. **Обідін Д. М.** Інтелектуалізація системи управління складним динамічним об'єктом на

основі нечітких семантичних мереж / Д. М. Обідін, В. А. Савченко // Моделювання та інформаційні технології: Зб. наук. пр. – К.: Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, 2012. – Вип. 63. – С. 81–85. 7. **Сакач Р. В., Зубков Б. В., Давиденко М. Ф.** Безопасность полетов: Учебник для вузов. – М.: Транспорт, 1989, – 239 с. 8. **Павлов В. В.** Начала теории эргатических систем. – Киев, Наукова думка, 1975 – 186 с. 9. **Прокофьева Т. Н.** Соционика. Алгебра и геометрия человеческих взаимоотношений. – М., Алмаз, 2005. – 356 с. 10. **Батурин Ю. М.** Типологические характеристики и критерии эффективности космонавта как оператора при проведении научных экспериментов в космическом полете. // Пилотируемые полеты в космос. – ФГБУ "НИИ ЦПК имени Ю.А. Гагарина", 2011 – № 1(1) – С. 104-122.

СОЦИОНИЧНО-ИНФОРМАЦИОННЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ФУНКЦИОНАЛЬНОЙ СТОЙКОСТИ АВИАЦИОННО-КОСМИЧЕСКОЙ БОЕВОЙ СИСТЕМЫ

Алексей Николаевич Горский (канд. техн. наук)

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Рассмотрены вопросы методологии обеспечения функциональной устойчивости сложных систем. Показано, что в сложных организационных эрготехнических системах важное место в обеспечении их функциональной устойчивости будут занимать процессы информационного метаболизма в системе. На основе соционического подхода к функционированию сложных систем определены закономерности боевой работы операторов системы, удовлетворяющие условиям обеспечения функциональной устойчивости авиационно-космической боевой системы. Приведены критерии оценки эффективности работы оператора и показана возможность проведения процедуры валидации тезауруса авиационно-космической боевой системы. Предложено определение решающей функции как результирующей функционирования тезауруса, вследствие чего выбирается вариант применения группировки авиации по предназначению.

Ключевые слова: соционика; функциональная устойчивость; авиационно-космическая боевая система.

SOCIONIC-INFOMATIONAL APPROACH TO PROVIDING FUNCTIONAL STABILITY OF AEROSPACE COMBAT SYSTEM

Oleksiy M. Horskyi (Candidate of Technical Sciences)

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

The questions of methodology of providing complex systems functional stability are considered. It is shown, that in providing of the complex organizational ergotechnical systems functional stability important role will be played by the processes of information metabolism in the system. On the basis of the socionic approach to functioning of the complex systems, management laws of the system operators combat work, that fulfil conditions of providing functional stability of the aerospace combat system, are defined. Main results allow to find optimum algorithms of operator actions for functioning of the aerospace combat systems with maximum efficiency of own functions implementation.

Such approach allows to make the aerospace combat system function more effectively using most common principles of information distributing within system, which allows to make aerospace systems more perfect through the thesaurus expansion procedures. Realization of offered procedure of system management laws determination that fulfil conditions of providing functional stability for the aerospace combat system allows to use achieved results for prognostication of dynamics of the aerospace forces warfare in the determined conditions, and to decrease probability of erroneous and inefficient actions by operators or persons, that make decision over all area of aerospace combat system using.

Keywords: socionic; functional stability; aerospace combat system.

References

1. Komarov V.S. (2007), Analysis of space facilities application for warfare conducting aims. [Analiz zastosuvannya kosmichnyh zasobiv v interesah zbroinoi borot'by], Armaments and military technique systems, No.1(9), pp. 34-37.
2. Permiakov O.U., Sbitnev A.I., (2008), Information technologies and modern warfare. [Informaciyni tehnologii ta suchasna zbroina borot'ba], Luhansk: Knowledge, 204 p.
3. Clark R., R. Nake (2011), Third world war: what it will be? [Tretia mirovaia voina: kakoi ona budet?], trans. E. Karmanova, SPt.: Piter, 336 p.
4. Permiakov O.U., Solonnikov V.G., Pribylev U.B., (2014), Information technologies using and space systems application in interests of troops (forces). [Vycorystannia informaciynyh tehnologiy ta zastosuvannya kosmichnyh system v interesah viys'k (syl)]: handbook, Kyiv: NDU of Ukraine named after Ivan Cherniakhovskiy, 208 p.
5. Voronin A.N., Ziyatdinov Y.K., Kharchenko A.V., Ostashevskiy V.V., (1997) Complex technical and ergatic systems: research methods. [Slozhnyie tehnicheckie I ergaticheckiye sistemy: metody issledovaniya], Fact, Kharkiv, 240 p.
6. Obidin D.M., Savchenko V.A., (2012), Intellectualization of the system of management by a complex dynamic object on the basis of fuzzy semantic networks. [Intellectualizaciya systemy upravlinnia skladnym dinamichnym ob'ektom na osnovi nechitkih semantichnyh merezh], Modelling and information technologies: Coll. scien. works, Kyiv: Institute of modelling in energetic problems named after G.E. Puhov of NSA of Ukraine, No.63, pp. 81-85.
7. Sakach R.V., Zubkov B.V., Davidenko M.F., (1989) Flight safety. [Bezopasnost poliotov: Uchebnik dlya vuzov], Transport, Moscow, 239 p.
8. Pavlov V.V. (1975), Beginnings of ergatic systems theory [Nachala teorii ergaticheckih system], Kiev, Scientific thought, 186 p.
9. Procofiyeva T.N. (2005), Socionic. and geometry of human relationship [Socionika. Algebra i geometriya chelovecheskih vzaimootnosheniy], Moscow, Almaz, 356 p.
10. Baturin U.M. (2011), Typological characteristics and criteria of cosmonaut effectiveness as operator while scientific experiments conducting in spaceflight. [Tipologicheskie harakteristiki i kriterii effektivnosti kosmonavta kak operatora pri provedenii nauchnyh eksperimentov v kosmicheskom polete], The piloted flights in space. – FSBU “SRI CPC named after U.A. Gagarin”, No.1(1), p. 104-122.

Отримано: 29.06.2016 року.

*Николай Васильевич Захарченко (д-р техн. наук, профессор)
Валерий Валентинович Гордейчук
Евгений Александрович Севастеев*

Одесская национальная академия связи имени А.С. Попова

УВЕЛИЧЕНИЕ ИНФОРМАЦИОННОЙ ЕМКОСТИ НАЙКВИСТОВОГО ЭЛЕМЕНТА ПРИ ПЕРЕДАЧЕ 2-Х СИМВОЛЬНЫХ АНСАМБЛЕЙ ТАЙМЕРНЫМИ СИГНАЛАМИ

На сегодняшний день все информационные системы используют принципы позиционного кодирования информации, остро стоит вопрос увеличения скорости передачи. В работе проведен анализ эффективности передачи нескольких символов первичного алфавита одной комбинацией. Показано, что информационная емкость найквистовского элемента в позиционных системах в случае укрупнения есть величина постоянная и зависит от основания алфавита, а в таймерных конструкциях - переменная и зависит от ряда информационных параметров. Предложен метод синтеза используемого кодового множества за счет подмножеств с различным числом информационных отрезков в кодовых словах, реализованных на одном и том же интервале m -найквистовых элементов. Данный метод обеспечивает большую информационную емкость на один найквистовый элемент, чем в привычных позиционных системах.

Ключевые слова: информация; энтропия; информационная емкость найквистового элемента; интервал реализаций; таймерные сигналы; момент модуляции.

Вступление.

Постановка проблемы. Анализ последних исследований и публикаций. На сегодняшний день при передаче больших массивов цифровой информации используется позиционная система кодирования, основанием которой служит позиционность канала - число различных значений информационного параметра a .

Недостатком таких систем является постоянство информационной емкости найквистовского элемента $I_n = \log_2 a$ при любой длине кодового слова [1]. В работе рассмотрен метод увеличения информационной емкости одного найквистовского элемента при постоянной длине кодового слова $T_c = nt_0$, где n - количество найквистовских элементов в кодовом слове и постоянном числе различных значений информационного параметра a .

Цель статьи. Описание увеличения информационной емкости найквистовского элемента при неизменном числе различных значений информационного параметра сигнала $a = \text{const}$ и длине кодового слова $T_c = mt_0 = \text{const}$.

Изложение основного материала

Бинарные таймерные сигнальные конструкции (ТСК) отличаются от конструкций позиционного кодирования (ПК) [1] следующими параметрами:

1. Расстояние между моментами модуляции при ПК кратное длительности элемента найквиста

$$\tau_{СП} = Kt_0, \quad (1)$$

где t_0 - длительность элемента найквиста, равная величине обратной полосе пропускания $\Delta F, (t_0 = 1/\Delta F)$;

K - число единиц или нулей следующих подряд в двоичном представлении номера символа.

2. Исходя из (1). минимальное энергетическое расстояние между кодовыми словами равно энергии одного найквистового элемента - t_0 . Меньше значения t_0 длительность сигнала не может быть, так как процессы установления сигнала на выходе канала не будут окончены, что приведет к межсимвольным искажениям.

1. Недостатки позиционного кодирования дискретных сообщений

В теории и технике связи различают два вида сообщений:

1. Непрерывные сообщения, характеризующиеся бесконечным числом значений на конечном интервале времени (например, количество различных значений амплитуды сигнала на выходе микрофона тем больше, чем выше точность измерительного прибора);

2. Дискретные сообщения, характеризующиеся конечным числом значений на бесконечном интервале времени (например, количество символов русского языка равно 32 символа m в любом многотомном издании). K числу дискретных источников в системах связи относится телеграфный текст, датчики команд в системах телекодовой связи, цифровые телеметрические датчики и др.

Преобразование отдельных символов в дискретные сигналы включает два этапа:

1. Нумерацию в десятичной системе всех символов;

2. Представление десятичных чисел в системе исчисления, согласованной с каналом: система исчисления определяется числом различных значений информационного параметра “а” (если информационный параметр равен $a=2$, то канал “двоичный”, если $a=3$, то канал троичный и т.д.)

Любое десятичное число N_{10} представляется в системе с основанием a .

$$N_{10} = \alpha_K a^K + \alpha_{K-1} a^{K-1} + \dots + \alpha_2 a^2 + \alpha_1 a^1 + \alpha_0 a^0, \quad (2)$$

При этом коэффициенты $\alpha_i \in \{0, 1, \dots, a-1\}$. Так, для двоичной системы $\alpha_i \in \{0, 1\}$, для троичной $\alpha_i \in \{0, 1, 2\}$, а при $a=4$ - $\alpha_i \in \{0, 1, 2, 3\}$.

В таблице 1 представлено десятичные числа $N_{10} \in \{1 \div 4\}$ в двоичной и троичной системах

Таблица 1

Десятичные числа в двоичной и троичной системах

№ п/п	a = 4	a = 3	a = 2
1.	1	1	0001
2.	2	2	0010
3.	3	10	0011
4.	10	11	0100
5.	11	12	0101
6.	12	20	0110
7.	13	21	0111
8.	20	22	1000
9.	21	100	1001
10.	22	101	1010

Из таблицы 1 следует:

1. В любой системе счисления каждому десятичному числу N_{10} однозначно соответствует определенная комбинация цифр из возможных коэффициентов для данной системы. С ростом десятичного числа N_{10} , число цифр увеличивается при $a = \text{const}$, и уменьшается при росте a ;

2. Так как число цифр в кодовых словах с ростом N_{10} увеличивается, то такой код называется неравномерным. Для того чтобы преобразовать его в равномерный необходимо в каждом кодовом слове слева от последней цифры “1” добавить соответствующее количество “0” до максимального значения цифр для N_{10} (в таблице 1 добавленные “0” слева от пунктирной линии).

Система называется позиционной, потому что записанные десятичные числа в позиционной системе при любом основании a однозначно соответствует десятичному числу только при записи коэффициентов α_i в указанных местах (позициях): крайний левый коэффициент соответствует a^0 (все следующие коэффициенты имеют степень на единицу больше). Если в

выражении (2) слагаемое какой-то степени отсутствует, то коэффициент α_i будет равным нулю.

Максимальное число реализаций различных кодовых конструкций равной длины n определяется как

$$n_1 = E^+(\log_2 N_{10}), \quad (3)$$

где E^+ - символ ближайшего большего значения логарифма.

Для первичного алфавита русского языка, состоящего из 32 букв $n = \log_2 32 = 5$. При передаче двухсимвольных ансамблей число их $N(2)$ равно $N(2) = 32 \cdot 32 = 1024$.

Следовательно, число элементов в кодовом слове при позиционном кодировании для двухсимвольных ансамблей будет $n_2 = \log_2 1024 = 10$ элементов.

Аналогично рассуждая, можно показать при передаче трехсимвольных ансамблей кодовых слов, будет $N(3) = (32)^3 = 32768$, что существенно затрудняет построение декодера.

Не трудно заметить, что при создании Z -символьных ансамблей общее число реализаций кодовых слов при позиционном кодировании увеличивается в 32 раза при увеличении Z на единицу.

Таким образом общим недостатком Z -символьных ансамблей при позиционном кодировании можно считать увеличение длин кодового слова при увеличении Z на единицу на $\log_2 32$ элементов.

Так как энтропия кодового слова русского языка $H = \log_2 32$, то при передаче посимвольно отдельных букв в каждом кодовом слове, состоящего из 5 двоичных единиц содержится 5 бит информации, следовательно, информационная емкость одного найквистового элемента будет $I_H = \frac{\log_2 32}{5} = 1$ дв.ед.

Учитывая то, что элементность кодовых слов, увеличивается на 5 элементов при увеличении Z на единицу (число Z определяет число объединяемых символов), то длина кодового слова объединенного множества линейно зависит от числа объединяемых символов, следовательно информационная емкость одного найквистового элемента для объединенного множества при позиционном кодировании остается равной $\log_2 a$.

Для увеличения информационной емкости одного найквистового элемента необходимо чтобы число реализаций увеличивалось более чем в 2 раза при увеличении интервала реализаций на один элемент

$$\frac{Np(m+1)}{Np(m)} > 2, \quad (4)$$

Оценим эффективность использования для этих целей таймерных сигнальных конструкций

2. Преимущества таймерных сигнальных конструкций.

В таймерных сигнальных конструкциях в отличие от позиционного кодирования информация заложена не в виде сигнала на интервале найквистового элемента, а в длительностях отдельных отрезков сигнала (i) и местах их положения. Требование к отрезкам, из которых состоят кодовые слова следующие:

$$t_0 \leq \tau_{ci} = t_0 + K\Delta, \quad (5)$$

1. Каждый из отрезков в кодовом слове где $K \in 0 \div K_0$ - целые числа;

$$\Delta = \frac{t_0}{S}, \quad (6)$$

где $S \in 1 \div S_0$ - целые числа

2. Число отрезков в кодовом слове длиной m элементов $1 < i < m$. При $i = m$ возможна одна реализация.

Величина Δ определяет минимальную величину длин отдельных отрезков в одной или

различных кодовых комбинациях и должны обеспечивать минимальную вероятность измерения длины отрезка на приеме $P_{0изм} \geq P_{зад}$.

Таким образом уравнение (5) обеспечивает установление переходного процесса на приеме, а элемент Δ - различимость длин отрезков в кодовом слове.

На рис.1 показано:

а. интервал реализации позиционных и таймерных кодовых конструкций $T_c = 6t_0$;

б. сигнальная конструкция позиционного кода "010011";

в. Кодовая конструкция позиционного кода "001010";

г. таймерная сигнальная конструкция с тремя отрезками $t_{ci} = t_0$ с минимальными значениями $t_{1min} = t_0, t_{2min} = 2t_0, t_{3min} = 3t_0$;

д. таймерная сигнальная конструкция, в которой первый отрезок $\tau_{c1max} = 3t_0, (t_{1max} = 3t_0), t_{2max} = 4t_0$ и $t_{3max} = 5t_0$.

е. таймерная сигнальная конструкция в которой: $\tau_{c1} = t_0 + \Delta, \tau_{c2} = t_0, \tau_{c3} = t_0 + 2\Delta$.

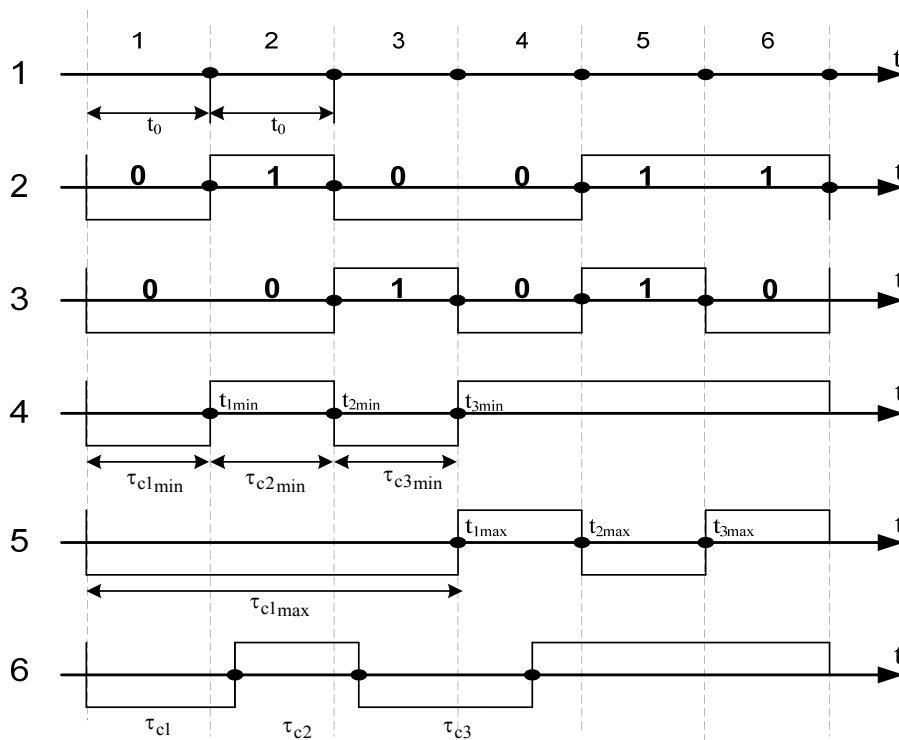


Рис. 1. Реализация таймерных сигнальных конструкций

Можно показать, что меняя длительности отрезков можно резко увеличить число различных комбинаций на заданном интервале m найквистовых элементов [2]

$$N = \frac{(ms - i(S-1))!}{(ms - is)!i!}, \quad (7)$$

Так, при заданном на рис. 1 $S = 5$ и $m = 5$, для $i = 3$ $N_p = 286$, а при $S = 7$ (что апробировано для городской телефонной сети), $N_p = 680$, что в

21, 25 раз больше по сравнению с позиционным кодированием.

Так как для двухсимвольных конструкций $N_p(2) = 1024$, а число реализаций на интервале $T_c = 5t_0$ только 680, что на много меньше необходимого – рассмотрим возможность создать необходимое множество за счет подмножеств реализованных на интервале $T_c = 5t_0$ из кодовых слов с различным числом отрезков. Проанализируем таблицу 2, в которой

представлены числа реализаций при изменении m и i , рассчитанные согласно (7) для $S = 7$

Таблица 2

Число реализаций ТСК при изменении m и i для $S = 7$

$i \backslash m$	4	5	6	7	8	9	10
1	22	29	36	43	50	57	64
2	120	253	435	666	946	1275	1653
3	120	680	2024	4495	8436	14190	22100
4	1	330	3060	12650	35960	82251	163185
5	0	1	11628	65780	65780	237736	658008

Из таблицы 2 следует, что число реализаций с увеличением интервала реализаций увеличивается. Однако коэффициент увеличения уменьшается с ростом m .

В таблице 3 представлены значения коэффициентов $K_y = \frac{N_p(m+1)}{N_{p^m}}$, при $S = 7$ для $i = 3$, и $i = 5$

Таблица 3

$i \backslash m$	4	5	6	7	8	9	10
3	-	5,66	2,97	2,22	1,87	1,68	1,55
5		∞	7,92	14,68	5,65	3,6	2,77

Из таблицы 3 следует, что с увеличением интервала реализаций m при заданных i и S коэффициент роста числа реализаций уменьшается.

В таблице 4 приведено число реализаций кодовых слов для $m = 5$ при $S(2 \div 10)$ и $i \in 1 \div 6$.

Таблица 4

S	I					
	1	2	3	4	5	6
2	9	28	35	15	1	0
3	13	55	84	35	1	0
4	17	91	165	70	1	0
5	21	136	286	126	1	0
6	25	190	455	210	1	0
7	29	253	680	330	1	0
8	33	325	963	495	1	0
9	37	406	1330	715	1	0
10	41	496	1771	1001	1	0

Литература

1. Захарченко М. В. Системы передачи данных. – Т. 1: Задачі кодування: підручник [для студентів вищих технічних навчальних закладів] / Захарченко М. В. – Одеса : Фенікс, 2009. – 448 с.
2. Методи підвищення ефективності використання каналів зв'язку / [Захарченко М. В., Гайдар В. П.,

Из анализа таблицы 4 и требований к создаваемым рабочим ансамблям можно сделать выводы:

1. сигнальные конструкции должны составлять рабочее множество на одном и том же интервале передачи;
2. величины минимального отличия отдельных отрезков i по длительности (или S) должны быть равными;
3. рабочее множество может быть создано при нескольких значениях i для $m = \text{const}$;

и $S = \text{const}$;

Например, рабочее множество для двухсимвольных ансамблей $N_p = 1024$, при $m = 5$, и $S = 7$, может включать (таблица. 4)

$i = 3$ – 680 реализаций;

$i = 4$ – 330 реализаций;

$i = 2$ – 14 реализаций из 253.

Сума этих реализаций дает 1024 на интервале $T_c = 5t_0$, следовательно, информационная емкость

одного элемента будет $I_1 = \frac{\log_2 1024}{5} = 2$ бита на

элемент, что в 2 раза больше чем при позиционном кодировании.

Выводы и перспективы дальнейших исследований

Увеличение информационной емкости найквистовского элемента целесообразно реализовывать за счет ансамблей сигналов с переменным числом отрезков при $m = \text{const}$ и $s = \text{const}$

Улеев О. П., Липчинский О. И.]. – К.: Техніка, 1998, - 248 с. . Захарченко Н. В. Эффективность компенсации избыточности кода при использовании таймерных сигналов / Захарченко Н. В., Басанов В. Е. // Моделирование та інформаційні технології: зб. наук. праць.- Вип. 31. – К.: 2005. – С. 6-13.

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ ЄМНОСТІ НАЙКВІСТОВОГО ЕЛЕМЕНТУ ПРИ ПЕРЕДАЧІ 2-Х СИМВОЛЬНИХ АНСАМБЛІВ ТАЙМЕРНИМИ СИГНАЛАМИ.

*Микола Васильович Захарченко (д-р техн. наук, професор)
Валерій Валентинович Гордійчук
Євген Олександрович Севаст'єєв*

Одеська національна академія зв'язку імені А.С. Попова

На сьогоднішній день всі інформаційні системи використовують принципи позиційного кодування інформації, гостро стоїть питання збільшення швидкості передачі. В роботі проведено аналіз ефективності передачі декількох символів первинного алфавіту однією комбінацією. Показано, що інформаційна ємність найквістового елемента в позиційних системах в разі укрупнення є величина постійна і залежить від підстави алфавіту, а в таймерних конструкціях - змінна і залежить від ряду інформаційних параметрів. Запропоновано метод синтезу використовуємої кодової множини за рахунок підмножин з різним числом інформаційних відрізків в кодових словах, реалізованих на одному і тому ж інтервалі m -найквістових елементів. Даний метод забезпечує велику інформаційну ємність

***Ключові слова:** інформація; ентропія; інформаційна ємність найквістового елемента; інтервал реалізації; таймерні сигнали; момент модуляції.*

INCREASE THE NAYKVIST ELEMENT CAPACITY IN 2-CHARACTER ENSEMBLES WITH TIMING SIGNALS TRANSFER

*Mykola V. Zakharchenko
Valerii V. Hordiichuk
Yevhen O. Sevastieiev*

Odessa National Academy of Telecommunications named after O.S.Popov

To date, all information systems using the principles of positional information coding urgent need to increase the transmission speed. This paper analyzes the efficiency of transferring multiple characters alphabet initial one combination. It is shown that the information capacity of naykvist element in positional systems if enlargement is constant and depends on the grounds of the alphabet, and timer designs - variable and depends on a number of information options. The method of synthesis code set that is used by a number of subsets with different pieces of information in the code word realized in the same interval m -naykvistovyh elements. This method provides greater information capacity

***Keywords:** information; entropy; information capacity of naykvist element spacing implementations; timer signals; time modulation.*

References

- 1. Zakharchenco M.V.** (2009), Systems of data transfer: noiseimmunity coding: textbook [*Sistemy peredachi danih .: Zavadostiyke koduvannya: pidruchnik*], ONAZ, Odesa, 448 p. **2. Zakharchenco M.V.**, Gajdar V.P., Uleev O.P., Lypchynsky O.I. (1998) Methods for improving the efficiency of communication channels. [*Metodi pidvischennya efektyvnosti vikoristannya kanaliv zv'yazku*], Kiev, 248 p. **3. Zakharchenco M.V.**, V.E. Basanov (2006) The effectiveness of the code redundancy compensation when using timing signals. [*Effektyvnost kompensacii izbytochnosti coda pri ispolzovanii taimernyh signalov*], Modelling and Information Technology, No. 31. pp. 6-13.

Отримано: 06.08.2016 року.

ІМІТАЦІЙНА МОДЕЛЬ ФУНКЦІОНУВАННЯ СИСТЕМИ ТИМЧАСОВОГО ПЕРЕВАНТАЖУВАЛЬНОГО РАЙОНУ

У статті розглядається імітаційна модель тимчасового перевантажувального району яка дозволяє оцінити ефективність застосування сил і засобів тимчасового перевантажувального району за відповідними критеріями. Розроблення імітаційної моделі тимчасового перевантажувального району визначається необхідністю дослідження закономірностей динаміки показників тимчасового перевантажувального району залежностей його функціонування від початкових параметрів і ефективності функціонування окремих елементів тимчасового перевантажувального району при стохастичності основних чинників, що впливають на його роботу. Імітаційна модель представлена у вигляді алгоритму функціонування системи тимчасового перевантажувального району, складається із сукупності процесів, математичних моделей які надаються у вигляді блоків та описують основні моменти діяльності тимчасового перевантажувального району, що визначають його поведінку в часі і безпосередньо впливають на результати роботи. Розроблена модель дозволяє імітувати процес функціонування тимчасового перевантажувального району в умовах впливу противника та визначати найбільш раціональні варіанти передавання через бар'єрний рубіж військ та військових вантажів, що надає можливість удосконалити "Методику обґрунтування сил і засобів тимчасового перевантажувального району".

Ключові слова: тимчасовий перевантажувальний район (ТПР); система; показники; імітаційне моделювання.

Вступ

Постановка проблеми. Робота тимчасового перевантажувального району залежить (ТПР) від відповідних пропускної, провізної та перевантажувальної його спроможностей, а отже, від сил і засобів здатних забезпечити потрібні можливості. Існуючі способи визначення сил і засобів тимчасового перевантажувального району не забезпечують проведення розрахунків в цілому, з врахуванням всіх заходів при підготовці та під час його функціонування, наслідків можливого впливу противника [1]. Реальний процес роботи ТПР дуже складний. На функціонування системи додатково впливають особливості технології роботи видів транспорту, а також морально-технологічні та інші чинники. Для пошуку більш досконалих шляхів обґрунтування складу сил і засобів необхідне дослідження процесів які відбуваються в тимчасовому перевантажувальному районі.

Одним з напрямків дослідження роботи тимчасового перевантажувального району при передаванні військ і військових вантажів через бар'єрні рубежі є розроблення і застосування моделей [2], що надають можливість достатньо повно і в певному взаємозв'язку проаналізувати й описати процес перевезення військових ешелонів і транспортів через бар'єрний рубіж, і на цій основі удосконалити методику, яка дозволить розробляти пропозиції щодо складу сил і засобів тимчасового перевантажувального району, а також готувати пропозиції щодо підвищення ефективності їх застосування.

Мета статті – розроблення імітаційної моделі для проведення дослідження функціонування тимчасового перевантажувального району (системи тимчасового перевантажувального району) в умовах впливу противника.

Для цієї мети доцільно мати: дані про хід передавання обсягів перевезень через тимчасово перевантажувальний район за розрахунковий період (це час висування військ (сил) і виконання вантажних евакуаційних перевезень) та виділені для забезпечення роботи тимчасового перевантажувального району сили і засоби.

Ефективністю функціонування системи є міра відповідності її своєму призначенню, це ступінь пристосованості системи до виконання конкретної задачі, ступінь досягнення мети [3,4].

Тобто, ефективністю функціонування тимчасового перевантажувального району є ступінь виконання заданих функцій по передачі військ і вантажів, протягом певного часу, з урахуванням умов функціонування та використання ресурсів.

Оцінку ефективності дій тимчасового перевантажувального району доцільно проводити по двох узагальнених критеріях: оперативному і економічному.

В якості оперативного критерію оцінки ефективності функціонування ТПР виступає максимум ступені виконання комплексу завдань щодо передачі військ і військових вантажів через бар'єрний рубіж у встановлені терміни з урахуванням раціонального використання тих сил і засобів, що є у його складі для їх виконання та

необхідного резерву. Економічний критерій відповідає на питання: якою ціною (витратами) досягається виконання цих завдань.

Виклад основного матеріалу дослідження

Імітаційна модель тимчасового перевантажувального району повинна охоплювати (або базуватися) на двох підсистемах і бути перетином моделей матеріального і транспортного забезпечення військ (сил), що висуваються в призначені райони. Загальним основним чинником, що впливає на ці дві складові, є характер впливу противника на тимчасовий перевантажувальний район під час висування військ (сил), який буде оцінюватися збитком, нанесеним як елементам тимчасового перевантажувального району, так і запасам матеріальних засобів, що перевозяться військами для свого забезпечення.

У цю складову будуть входити і моделювання елементів за функціональною ознакою і відновлення уражених елементів.

Транспортна частина моделі повинна відображати міру ураження кожного транспортного елемента та зниження його здатності щодо передавання військ і військових вантажів через бар'єрний рубіж. На підставі цього повинні визначатися можливості сил і засобів тимчасового перевантажувального району за добу та заходи, необхідні для досягнення добового обсягу передавання військ і військових вантажів через бар'єрний рубіж.

Складові матеріального забезпечення військ, які перевозяться, повинні враховувати втрати (запаси) матеріальних засобів військ (сил), що передаються через тимчасово перевантажувальний район за видами (боєприпаси, пально-мастильні матеріали, військово-технічне майно), визначати обсяги та порядок поповнення цих засобів, якими силами виконати ці види робіт при дотриманні балансу "можливості – потреби". Всі елементи тимчасового перевантажувального району зв'язані між собою та з ділянками по яким поступають і відправляються транспортні засоби, і утворюють складну транспортну систему, що складається з ділянок вивантаження та завантаження, пристроїв прийому транспортних засобів, навантажувально-вивантажувальних (перевантажувальних) місць, пристроїв передавання потоків перевезень в обхід бар'єрного рубежу, пристроїв формування вихідних потоків транспортних засобів.

Для вивчення функціонування цих підсистем пропонується імітаційне моделювання – процес конструювання моделі реальної системи та постановки експериментів на цій моделі з метою або зрозуміти поведінку системи, або оцінити (в рамках обмежень, що накладаються критерієм) різні стратегії, які забезпечують функціонування даної системи [5].

В основу математичного апарату моделі тимчасового перевантажувального району покладений ряд припущень про випадкові процеси, що протікають в даній системі:

- кожної доби закон рівномірного розподілу приймався для випадкових процесів, про які відсутня інформація, окрім діапазонів їх зміни;

- для достатньо вивчених випадкових процесів, які можна охарактеризувати як суму безлічі випадкових підпроцесів, відповідно до центральної граничної теореми теорії ймовірності, приймався нормальний закон розподілу;

- в тому випадку, якщо можливі декілька варіантів проходження випадкових процесів, вибирався як найгірший варіант (з погляду показників функціонування ТПР).

Загальна структура моделі у вигляді блоків (рис. 1) деталізується шляхом вибору керованих і некерованих перемінних, опису функціональних залежностей між ними, обмежень, цільової функції.

Число неуражених об'єктів ТПР, що володіють j -им ресурсом на i -у добу (типові об'єкти ураження):

$$N_i^j = N_{i-1}^j + M_{i-1}^j - L_i^j, \text{ од.}, \quad (1)$$

де M_{i-1}^j - число відновлених (поповнених) об'єктів ТПР j -им ресурсом на i -у добу операції, од.;

L_i^j - збиток ТПР від засобів нападу противника по j -му ресурсу на i -у добу операції (типіві об'єкти ураження), од.

Число відновлених об'єктів по ресурсу та кількість техніки тилу після поточного і середнього ремонтів на i -у добу операції можуть бути змодельовані як випадкові величини з нормальним законом розподілу

$$M_i^j = I_{(□)}^j (B_{20\min} + (B_{20\max} - B_{20\min}) \eta(\xi(0); 0; 0,5)), \text{ од.}, \quad (2)$$

де $B_{20\min}, B_{20\max}$ - мінімальна і максимальна частки від втрат на i -у добу, які відновлюються після ремонту;

$\eta(\xi(0); 0; 0,5)$ - нормальний обернений розподіл рівномірно розподіленого випадкового числа, арифметичний середній розподіл рівний 0, стандартне відхилення рівне 0,5;

$\xi(0)$ - повертає рівномірно розподілене випадкове число яке більше або дорівнює 0, менше 1; нове випадкове число повертається кожного разу, коли робочий лист обчислюється;

З урахуванням часу евакуації, лікування і повернення до строю поранених і хворих M_i^{oc} приймається рівним нулю. Для матеріальних засобів M_i^{m3} , також було прийнято рівним нулю.

Якість застосування сил і засобів ТПР визначає не стільки раціональний розподіл сил і засобів по ділянках, скільки застосування варіантів (в основному без перевантажувального) просування військ і вантажів, не виключаючи перевантаження вантажів і збільшення темпу. Загальна структура імітаційної моделі у вигляді блоків і компонентів деталізується шляхом вибору керованих і некерованих перемінних, опису функціональних залежностей між ними, обмежень, цільової функції або функції критерію.

Число неуражених об'єктів ТПР, що володіють j -им ресурсом на i -у добу (типові об'єкти ураження):

$$N_i^j = N_{i0}^j + M_{i0}^j \cdot L_i^j, \text{ од.}, \quad (3)$$

де M_i^j – число відновлених (поповнених) об'єктів ТПР j -им ресурсом на i -у добу операції, од.;

L_i^j – збиток ТПР від засобів нападу противника за j -м ресурсом на i -у добу операції (типові об'єкти ураження), од.

Процеси відновлення елементів ТПР можна охарактеризувати як суму безлічі випадкових під процесів. Тому, відповідно до центральної граничної теореми теорії ймовірності, число відновлених об'єктів за ресурсом та техніка тилу після поточного і середнього ремонтів на i -у добу операції можуть бути змодельовані як випадкові величини з нормальним законом розподілу.

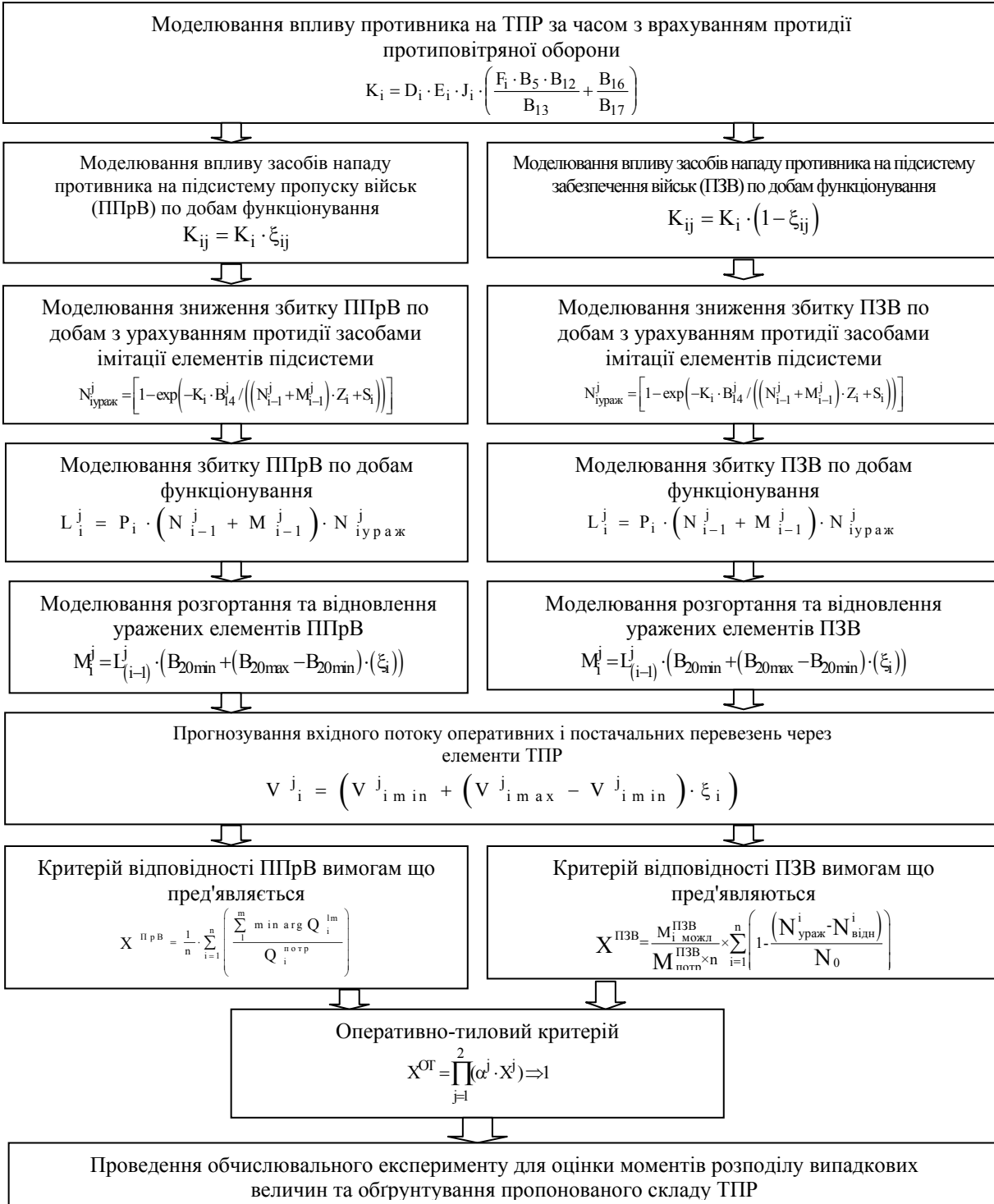


Рис. 1. Структура імітаційної моделі тимчасового перевантажувального району

$$M_i^j = L_{i\text{цп}}^j (B_{20\text{min}} + (B_{20\text{max}} - B_{20\text{min}}) \eta(\xi(); 0; 0,5)), \text{ од.} \quad (4)$$

де $B_{20\text{min}}, B_{20\text{max}}$ – мінімальна й максимальна частки від втрат на i -у добу, які відновлюються після ремонту;

$\eta(\xi(); 0; 0,5)$ – нормальний обернений розподіл рівномірно розподіленого випадкового числа, арифметичний середній розподіл рівний 0, стандартне відхилення рівне 0,5;

$\xi()$ – повертає рівномірно розподілене випадкове число яке більше або дорівнює 0, менше 1; нове випадкове число повертається кожного разу, коли робочий аркуш обчислюється.

Відновлення техніки тилу об'єктів ТПР після капітального ремонту моделювати не доцільно, оскільки середні терміни капітального ремонту перевищують тривалість операції.

З урахуванням часу евакуації, лікування і повернення до строю поранених і хворих M_i^{oc} приймається рівним нулю. Для матеріальних засобів M_i^{m3} , також було прийнято рівним нулю.

Математичне сподівання числа об'єктів ТПР, що уражаються по j -му ресурсу на i -у добу операції:

$$L_i^j = P_{\text{зруйн}} \times (N_{\text{цп}}^j + M_{\text{цп}}^j) \times N_{\text{ураж}}^j, \quad (5)$$

де $P_{\text{зруйн}}$ – ймовірність зруйнування об'єкту ТПР; яка характеризується ймовірністю виявлення об'єкту $P_{\text{вияв}}$, ймовірністю доставки засобів ураження $P_{\text{аін}}$, ймовірністю ураження $P_{\text{ураж}}$

Прогнозована кількість типових об'єктів ТПР, що уражаються ударами противника

$$N_{\text{ураж}}^j = \text{Exp} \left(K_i B_{14}^j / \left((N_{\text{цп}}^j + M_{\text{цп}}^j) Z_i + S_i \right) \right), \quad (6)$$

де K_i – потенціал засобів ураження противника на i -у добу операції;

B_{14}^j – частка j -го ресурсу, що підлягає ураженню при одноразовій дії противника на типовий об'єкт ТПР (при моделюванні приймався нормальний закон розподілу):

$$B_{14}^j = B_{14\text{min}}^j + (B_{14\text{max}}^j - B_{14\text{min}}^j) \eta(\xi(); 0; 0,5), \text{ од.} \quad (7)$$

Z_i – коефіцієнт зниження можливостей засобів розвідки противника за рахунок заходів приховання об'єктів ТПР на i -у добу;

S_i – кількість неуражених імітованих об'єктів ТПР на i -у добу:

$$S_i = S_{\text{цп}} \left(\frac{L_i S_{\text{цп}}}{S_{\text{цп}} + N_{\text{цп}}^j} \right) + U_i, \text{ од.}, \quad (8)$$

де U_i – кількість імітованих об'єктів ТПР, що створюються на i -у добу операції, (од.).

Основним параметром використання тих або інших засобів ураження прийнято вважати ймовірність руйнування об'єкту ТПР, яка характеризується ймовірністю виявлення об'єкту

$P_{\text{вияв}}$, ймовірністю доставляння засобів ураження

$P_{\text{дос}}$, ймовірністю ураження $P_{\text{ураж}}$ і визначається за формулою

$$P_{\text{зруйн}} = P_{\text{вияв}} \times P_{\text{дос}} \times P_{\text{ураж}} \quad (9)$$

Припустивши, що максимальний збиток об'єкту може бути завданий застосуванням зброї з мінімальною масою заряду бойової частини, але підвищеною точністю доставляння, за розрахунковий можна прийняти варіант ураження з максимальними значеннями ймовірності зруйнування об'єкту і ймовірності доставляння засобу ураження [2].

Загальний потенціал засобів ураження противника:

$$K_i = D_i E_i J_i \frac{F_i B_5 B_{12} + B_{16}}{B_{13} + B_{17}}, \text{ од.}, \quad (10)$$

де D_i – частка засобів нападу противника, що виділяється для ураження об'єктів тилу на i -у добу операції в d -й період операції;

E_i – частка засобів нападу противника, що виділяється для ураження об'єктів ТПР на i -у добу операції в d -й період операції;

J_i – частка попередженого системою протиповітряної оборони збитку об'єктам ТПР (при моделюванні приймається нормальний закон розподілу), яка визначається аналогічно B_{14} ;

F_i – частка справних засобів нападу противника на i -у добу операції з урахуванням втрат;

B_5 – кількість засобів авіації противника, що діє в визначеній смузі на початок операції (при моделюванні приймається рівномірний закон розподілу)

$$B_5 = B_{5\text{min}} + (B_{5\text{max}} - B_{5\text{min}}) \xi(), \quad (11)$$

де B_{12} – бойова напруга авіації противника, що діє в смузі АК (вильотів за добу);

B_{13} – кількість засобів авіації противника, що діє в смузі АК і використаної для ураження одного типового об'єкту ТПР, од.;

B_{16} – кількість крилатих ракет противника, використаних по об'єктах АК за операцію, од.;

B_{17} – кількість крилатих ракет противника, використаних для ураження одного типового об'єкту ТПР, од.;

$B_{12}, B_{13}, B_{16}, B_{17}$ – на кожну добу операції визначається аналогічно коефіцієнту B_5 (при моделюванні приймається рівномірний закон розподілу), од.

В процесі моделювання визнано доцільним користуватися середніми значеннями можливого наряду авіації і крилатих ракет (B_{13} і B_{17}), для ураження одного типового об'єкту ТПР (малорозмірного майданчикowego, точкового) для літаків 4 од., для крилатих ракет – 2 од.

Для випадкових процесів, про які відсутня інформація окрім діапазонів їх зміни, – таких, як частка засобів нападу противника, що виділяється для ураження об'єктів тилу на i -у добу операції в d -й період операції, при моделюванні приймався рівномірний закон розподілу:

$$D_i = (D_{d\min} + (D_{d\max} - D_{d\min})\xi(\cdot)). \quad (12)$$

Частка засобів нападу противника, що виділяється для ураження об'єктів ТПР на i -у добу операції в d -й період операції (при моделюванні приймався рівномірний закон розподілу):

$$E_i = (E_{d\min} + (E_{d\max} - E_{d\min})\xi(\cdot)). \quad (13)$$

Значення коефіцієнтів D_i і E_i , можуть бути розраховані з урахуванням складу, можливостей авіації противника та його поглядів на ведення операцій.

Досвід застосування та навчань військово-повітряних сил провідних країн світу свідчить про те, що для ізоляції району бойових дій і порушення роботи тилу може бути виділено до 25-30 % льотного ресурсу авіації, який розподіляється за періодами операції нерівномірно і залежить від завдань, що вирішуються військами противника [3].

Частка збитку об'єктам ТПР, яка попереджена системою протиповітряної оборони (при моделюванні приймався нормальний закон розподілу):

$$J_i = (J_{\min} + (J_{\max} - J_{\min})\eta(\xi(\cdot); 0, 0, 5)). \quad (14)$$

Частка справних засобів нападу противника на i -у добу операції з урахуванням втрат визначається як

$$F_i = \left[\frac{B_{4\min} + (B_{4\max} - B_{4\min})\xi(\cdot)}{\xi(\cdot; 0, 0, 5)} \right]^{(i-1)} \quad (15)$$

де B_4 – середньодобові втрати авіації противника, од.

Середньодобові втрати авіації противника, на підставі інформаційних матеріалів щодо навчань військово-повітряних сил провідних країн, приймаємо рівними $6+2\%$ [103].

За число неуражених об'єктів ТПР на i -у добу операції N_i при моделюванні можна прийняти мінімальне число неуражених об'єктів, що володіють j -м ресурсом (типові об'єкти ураження):

$$N_i^{\min j} = \min_j (N_{i\min}^j + M_{i\min}^j L_i^j), \text{ од.} \quad (16)$$

Мінімальний j -й ресурс можна визначити за допомогою функції МІН Microsoft Excel яка визначає мінімальне число неуражених об'єктів, що володіють j -м ресурсом і мають найменше значення в списку аргументів.

Зниження можливостей ТПР за рахунок дій диверсійно-розвідувальних груп визначається аналогічно коефіцієнту B_5 (при моделюванні приймався рівномірний закон розподілу).

Прогнозований обсяг оперативних і постачальних перевезень через елементи ТПР:

$$V_i^j = (V_{i\min}^j + (V_{i\max}^j - V_{i\min}^j)\xi_i), \quad (17)$$

де $V_{i\min}^j, V_{i\max}^j$ – мінімальний і максимальний обсяги перевезень на i -у добу за j -м ресурсом.

Відповідно до основних функцій, що виконуються, та вимог до критеріїв оцінки застосування сил і засобів ТПР імітаційна модель дозволяє оцінити їхню роботу за двома основними критеріями. Перший – характеризує середньодобову переважувальну здатність сил і засобів ТПР, другий, – дозволяє оцінити можливості сил і засобів ТПР щодо до забезпечення військ, що пропускаються, за розрахунковий період.

Оцінка інших функцій у даній роботі вноситься за межі дослідження.

Критерій відповідності підсистеми забезпечення військ вимогам, що пред'являються, визначається пропорційно середньодобовій частці тих об'єктів підсистеми, які збереглися та враховує резервування сил і засобів системи матеріального забезпечення ТПР на початок розрахункового періоду:

$$X^{\text{ПЗВ}} = \frac{M_{\text{іможл}}^{\text{ПЗВ}}}{M_{\text{потр}}^{\text{ПЗВ}} \times n} \times \prod_{i=1}^n \left(\frac{N_{\text{ураж}}^i + N_{\text{відп}}^i}{N_0} \right), \quad (18)$$

де $M_{\text{іможл}}^{\text{ПЗВ}}$ – можливості системи ПЗВ на i -у добу по матеріальному забезпеченню військ;

$M_{\text{потр}}^{\text{ПЗВ}}$ – вимоги до системи ПЗВ на i -у добу щодо матеріального забезпечення військ;

$N_{\text{ураж}}^i, N_{\text{відп}}^i, N_0$ – число об'єктів уражених на i -у добу, число об'єктів відновлених на i -у добу, число об'єктів на початок розрахункового періоду.

Критерій відповідності підсистеми пропуску військ вимогам, що пред'являються, визначається як відношення суми пропускних спроможностей паралельних маршрутів у ТПР до потрібної його пропускної спроможності. Пропускна спроможність кожного маршруту визначається елементом з мінімальною пропускною спроможністю:

$$X^{\text{ПрВ}} = \frac{1}{n} \times \prod_{i=1}^n \left(\frac{\min_{i=1}^m \arg Q_i^{\text{ім}}}{Q_i^{\text{потр}}} \right), \quad (19)$$

де $Q_i^{\text{ім}}$ – пропускна спроможність m -го елемента на i -му маршруті передачі військ та військових вантажів через ТПР на i -у добу;

$Q_i^{\text{потр}}$ – потрібна пропускна спроможність ТПР на i -у добу.

Згортку критеріїв пропонується здійснити мультиплікативним чином, оскільки невиконання одного із завдань приводить до невиконання завдання ТПР у цілому.

Узагальнений оперативно-тиловий критерій оцінки ефективності застосування сил і засобів ТПР буде виглядати:

$$X^{OT} = \prod_{j=1}^2 (a^j \times X^j)_{\Pi} \quad (20)$$

де α – коефіцієнт вагомості часткового критерію, який визначається з урахуванням обмеження:

$$\sum_{i=1}^2 a^j = 1. \quad (21)$$

Таким чином, оперативно-тиловий критерій у символічній формі можна представити як функцію безлічі параметрів:

$$X^{OT} = f(K_i; L_i^j; M_i^j; P_i; P_{зруйн}; J_i; Q_i^{lm}). \quad (22)$$

Оперативно-тиловий критерій є функцією від: кількості уражених і відновлених об'єктів; заходів приховання й імітації; імовірності зруйнування об'єктів; ефективності системи протиповітряної оборони;

можливостей елементів ТПР по пропуску військ і вантажів.

Висновки та перспективи подальших досліджень

Імітаційна модель ТПР ґрунтується на прогнозуванні (втрат) збитку об'єктів системи і темпів їх відновлення (поповнення) за кожен добу з урахуванням заходів протидії. Проведення обчислювального експерименту на основі даної моделі дозволить достовірно визначити показники застосування сил і засобів ТПР.

Розроблена модель дозволяє імітувати процес функціонування ТПР в умовах впливу противника та визначати найбільш раціональні варіанти передавання через бар'єрний рубіж військ та військових вантажів, що надає можливість удосконалити "Методику обґрунтування сил і засобів тимчасового перевантажувального району".

Література

1. Кивлюк В. С. Проблемні питання подолання бар'єрних рубежів з використанням тимчасового перевантажувального району / В. С. Кивлюк / Наука і оборона. – 2010. - № 3. – С. 26-30. 2. Основи імітаційного моделювання: навчальний посібник. – Київ.: НАОУ, 2006. – 40 с. 3. Основи моделювання

бойових дій військ: Підручник. – Київ.: НАОУ, 2005. – 484 с. 4. Шеннон Р. Имитационное моделирование систем – искусство и наука / Шеннон Р.; пер. с англ. Е. К. Масловского. – М.: "Мир", 1978. – 421 с. 5. Вентцель Е. О. Исследование операций, задачи, принципы, методология. – М.: Наука, 1988. – 208 с.

ИМИТАЦИОННАЯ МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ВРЕМЕННОГО ПЕРЕГРУЗОЧНОГО РАЙОНА

Владимир Семенович Кивлюк (канд. экон. наук, доцент)
Николай Ярославович Клонецк

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье рассматривается имитационная модель временного перегрузочного района которая позволяет оценить эффективность применения сил и средств временного перегрузочного района по соответствующим критериям. Разработка имитационной модели временного перегрузочного района определяется необходимостью исследования закономерностей динамики показателей временного перегрузочного района зависимостей его функционирования от начальных параметров и эффективности функционирования отдельных элементов временного перегрузочного района при стохастичности основных факторов, влияющих на его работу. Имитационная модель представлена в виде алгоритма функционирования системы временного перегрузочного района, состоит из совокупности процессов, математических моделей, которые представляются в виде блоков и описывают основные моменты деятельности временного перегрузочного района определяют его поведение во времени и непосредственно влияют на результаты работы. Разработанная модель позволяет имитировать процесс функционирования временного перегрузочного района в условиях воздействия противника и определять наиболее рациональные варианты передачи через барьерный рубеж войск и военных грузов, позволяет усовершенствовать "Методику обоснования сил и средств временного перегрузочного района".

Ключевые слова: временный перегрузочный район (ВПР) система; показатели; имитационное моделирование.

SIMULATION MODEL OF THE SYSTEM TEMPORARY OVERLOADING AREA

Volodymyr S. Kyvliuk (Candidate of Economic Sciences, Associate Professor)
Mykola Y. Klontsak

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

In the article the simulation model temporary overloading area, to evaluate efficiency capability of temporary overloading area by the relevant criteria. Development of the simulation model temporary overloading area is determined by investigating laws of Indexes dynamics of temporary overloading area,

dependence of its initial parameters and effectiveness of individual elements of the temporary overloading area at random main factors influenced on its performance. A simulation model presented as an algorithm of the system temporary overloading area, consisting of a set of processes, mathematical models offered in blocks and describes the main points of temporarily reloading area that determine its behavior in time and directly affect the results. The model allows simulating the process of functioning of interim reloading area under the influence of the enemy and determining the most rational options for transmission via Barrier line troops and military cargo, which enables improved method of grounding capability of interim reloading area.

Keywords: temporary transshipment region (TTR); system; indexes; simulation.

References

1. **Kyvlyuk V.S.** (2010), Problems of overcoming the barrier lines using temporary overloading area, Science and Defence. [*Problemni pytannia podolannia bariernykh rubezhiv z vykorystanniam tymchasovoho perevantazhualnoho raionu*], No. 3, pp. 26-30.
2. **Fundamentals of simulation modeling: a tutorial** (2006), [*Osnovy imitatsiinoho modeliuвання: navchalnyi posibnyk*], Kyiv, NAOU, 40 p.
3. **Basic simulation fighting troops: Textbook**, (2005), [*Osnovy modeliuвання boiovykh dii viisk: Pidruchnyk*], Kyiv: NAOU, 484 p.
4. **Shannon R.** (1978), Simulation Modeling Systems - the art and science. [*Imitatsionnoe modelirovanie sistem – iskusstvo i nauka*], Per. with English E.K. Maslovskoho, Moscow: "Mir", 421 p.
5. **Wentzel E.O.** (1988), Study operations, objectives, principles, methodology. [*Issledovanie operatsii, zadachi, printsipy, metodologiya*], Moscow: Nauka, 208 p.

Отримано: 03.08.2016 року.

Ігор Миколайович Козубцов (канд. техн. наук, с.н.с.)

Військовий інститут телекомунікацій та інформатизації, Київ, Україна

АНАЛІЗ НОРМАТИВНО-ПРАВОВОЇ СКЛАДОВОЇ ОБ'ЄКТНОГО КОМПОНЕНТА МЕТОДОЛОГІЧНОЇ КУЛЬТУРИ АД'ЮНКТІВ

В статті проаналізовано і згуртовано ключову нормативно-правову та законодавчу основу, на якій ґрунтується підготовка здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах). Окремо виділено підгрупу документів, на основі яких організовується підготовка зазначеної категорії саме для потреб Збройних Сил України. Перелічена нормативно-правова та законодавча основа становить об'єктну складову методологічної культури ад'юнктів та аспірантів. Автором в контексті об'єкту дослідження визначено приналежність ключової нормативно-правової бази, яка визначає єдиний порядок організації підготовки наукових та науково-педагогічних кадрів вищої кваліфікації в Україні та для потреб Збройних Сил України та виступає нормативно-правовою складовою об'єктного компонента методологічної культури ад'юнктів. Теоретичне значення дослідження полягає в розвитку теорії методологічної культури ад'юнктів.

Ключові слова: ад'юнкт; ад'юнктура; методологія; організація діяльності; методологічна компетентність; методологічна культура; науковий керівник; нормативно-правова основа; об'єктний компонент.

Вступ

Постановка проблеми і зв'язок її з важливими науковими завданнями. Правове регулювання атестації наукових кадрів вищої кваліфікації – це один із численних дозволивих адміністративно-правових режимів, які розповсюджують свою дію на виконання його суб'єктами (юридичними та фізичними особами) процедур забезпечення відповідності щодо правил, встановлених нормативно-законодавчими актами у цій сфері. Інакше кажучи, режим атестації наукових кадрів вищої кваліфікації є процедурою офіційного державного визнання кваліфікації здобувача наукового ступеня і, відповідно до цього, можливості виконання ним певних функцій, встановлених законодавством. В процесі підготовки та організації дисертаційного дослідження здобувач вченого ступеня поступово оволодіває всіма тонкощами щодо виконання всіх нормативних вимог, молодий вчений формує одну зі складових методологічної культури – нормативно-правову основу. Виходячи з цього, на нашу думку, важливою наукою та соціальною проблемою є забезпечення своєчасності набуття (формування світогляду) здобувачами вченого ступеня нормативно-правової основи методологічної культури як її об'єктного компонента.

Аналіз досліджень і публікацій. Теоретичних досліджень цього питання небагато, а термінологія відпрацьована недостатньо. Збільшилася кількість публікацій як із загальних, так і окремих питань наукового права [1], з'явилися нові дослідження та праці, в тому числі українських вчених [2; 3].

Увага вчених-правознавців до наукового права посилилась лише останніми роками.

Автори [4] звернули увагу на те, що Українське законодавство в науковій сфері має безліч

невизначеностей та протиріч. Це виражається в неадекватно великій кількості регулюючих норм і інститутів, значному адміністративному і податковому тиску, неприйнятно високій кількості зобов'язань, покладених на суб'єкти наукової, науково-технічної та інноваційної діяльності.

Формулювання мети статті. Мета статті полягає провести аналіз сучасної нормативно-правової складової об'єктного компонента методологічної культури ад'юнктів. За результату сформулювати висновки щодо сучасного стану.

Результат дослідження

Складність вирішення даного питання полягає в тому, що у педагогіці немає єдності в питанні при визначенні основних структурних і функціональних компонентів. При виділенні частин, підсистем дослідники часто керуються власним досвідом, своїми уявленнями про модельовану систему. Нами запропоновано власну структуру об'єктного компонента методологічної культури ад'юнктів (рис. 1).

Зміст нормативно-правової складової. Норми – це правила поведінки, очікування та стандарти, що регулюють взаємовідносини між ад'юнктам, вказуючи на правила поведінки за певних умов та ситуацій при організації професійної діяльності.

Норми визначають ад'юнктам методологічний порядок: організації професійної діяльності ад'юнктами в ад'юнктурі; взаємодії ад'юнкта з науковим керівником; організації ад'юнктами дисертаційного дослідження; логічного структурування розділів дисертаційної роботи (дисертації); підготовки ад'юнктами до друку наукових публікацій, їх мінімальну кількість; організації (проведення) участі ад'юнктів в наукових заходах та дотримання етичних норм поведінки. Завдяки нормативному компоненту у ад'юнкта утворюється певна система

загальносуспільних світоглядних уявлень, на основі яких він може організовувати свою професійну діяльність. Наявність нормативного компоненту робить можливість згуртування

множини ад'юнктів, як індивідуумів наукового суспільства, в єдиний науковий колектив, особливо при їх роботі в науковій школі.

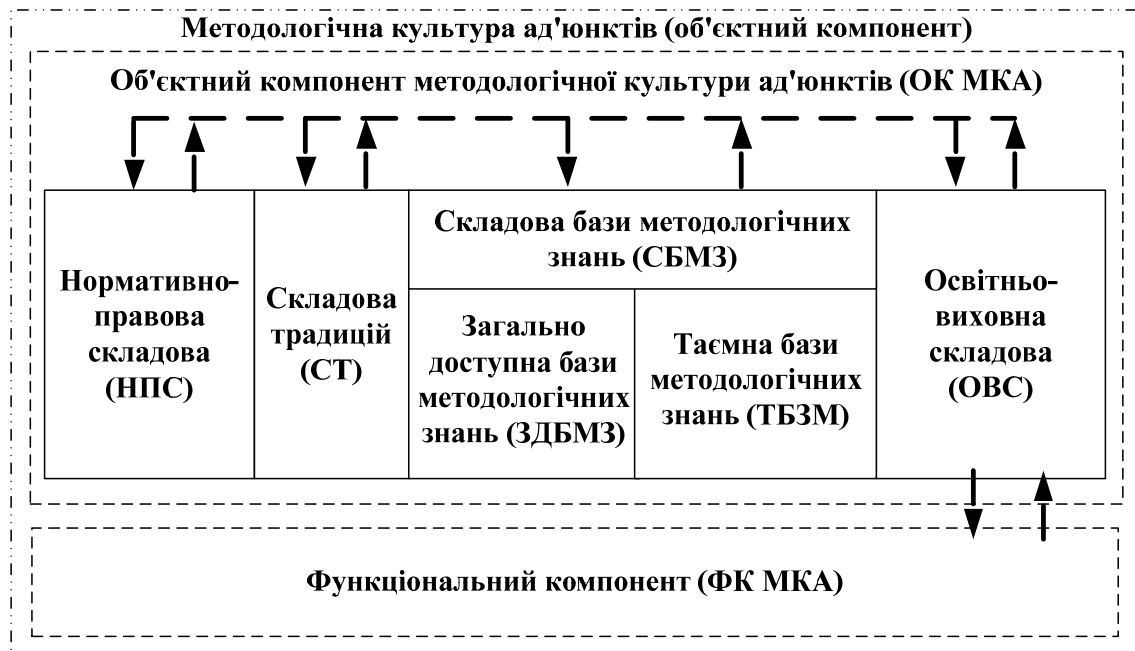


Рис 1. Структура об'єктного компонента методологічної культури ад'юнктів

Нормативно-правовий аспект практичної організації впровадження результатів дисертаційного дослідження

Автори дослідження проаналізували організаційно-методичні питання здійснення атестаційного процесу за період з 1992 по 2005 рр., що регулювалися нормативними актами ВАК

України, яких всього прийнято 620 [4, табл. 1.1]. Така чисельність нормативних актів ВАК, а згодом ДАК України представлено в табл. 1.

Ми частково доповнили цю таблицю нормативними актами за період з 2011 по 2016 рр. (див. табл. 2).

Таблиця 1.

Нормативні акти які прийнято ВАК України у 1997-2005 рр.

Нормативно-правова база атестації наукових та науково-педагогічних кадрів вищої кваліфікації

Тематика актів / рік	1997	1998	1999	2000	2001	2002	2003	2004	2005	Всього
Про підготовку науково-педагогічних і наукових кадрів			1							1
Про спеціалізовані ради	-	-	-	-	-	-	46	25	64	135
Про провідні установи	-	6	6	8	23	57	33	35	22	190
Про публікації	6	3	6	12	5	2	6	6	7	53
Про паспорти спеціальностей	6	27	18	10	22	19	9	14	9	134
Про перелік спеціальностей	1	1	3	2	3	1	3	2	1	17
Про норми оплати праці	2	1	-	-	1	1	1	3	2	11
Про форми документів	2	4	1	2	-	1	-	1	2	13
Про кандидатські іспити	-	-	3	-	-	-	-	-	1	4
Про основоположні документи	3	-	2	3	-	-	-	5	1	14
Про контроль ходу атестації	1	3	1	1	-	1	1	1	3	11
Про поліпшення якості робіт	-	5	1	-	-	-	1	2	-	10
Методичні	-	1	3	2	-	-	2	2	-	10
Інше	2	5	1	4	-	1	-	5	-	18
Всього	23	56	47	44	54	83	102	101	112	621

Як можна побачити значна чисельність нормативних актів носить формалізований характер та про покращення якості робіт без методичних рекомендацій - це утопія. Такої ж думки і автори монографії. Тематичний аналіз

свідчить про різке зростання кількості прийнятих нормативних документів на певних етапах розвитку атестаційного процесу - 1998, 2002, 2005 роки, що пояснюється, в першу чергу, зовнішніми вимогами активізації зусиль, а також розширенням

кола учасників. Значна частина нормативного поля визначає питання організації спеціалізованих вчених рад, затверджує переліки провідних установ та фахових видань. На перший погляд, велику частку займають постанови президії ВАК щодо переліку та паспортів спеціальностей (151), однак, перераховуючи загальну кількість на окремі галузі науки, приходимо до висновку про

мінімальну увагу щодо впорядкування цього сектора атестаційного процесу. Привертає увагу й занадто низька кількість постанов, прийнятих за результатами контрольних перевірок ходу атестації та спрямованих на покращення якості робіт, в середньому два на рік. Недостатньо, на нашу думку, є також кількість щорічно опрацьовуваних методичних матеріалів.

Таблиця 2.

Нормативні акти які прийнято ДАК України у 2011-2016 рр.

Тематика актів / рік	2011	2012	2013	2014	2015	2016	Всього
Порядок підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах)	-	-	-	-	-	1	1
Про спеціалізовані ради	2	-	-	1	3	1	7
Про організацію діяльності експертних рад з питань проведення експертизи дисертацій Міністерства освіти і науки України	-	-	-	1	-	-	1
Змін до Положення про експертну раду з питань проведення експертизи дисертаційних робіт Міністерства освіти і науки, молоді та спорту України	-	1	-	-	-	-	1
Про порядок присудження наукових ступенів і присвоєння вчених звань	1	2	-	-	-	1	4
Про призначення офіційних опонентів	-	-	1	-	-	-	1
Про провідні установи	-	1	-	-	-	-	1
Про публікації	-	1	1	-	-	-	2
Про перелік наукових фахових видань України	-	2	-	-	-	-	2
Про паспорти спеціальностей	1	-	-	-	-	-	1
Про перелік спеціальностей	1	-	-	-	-	-	1
Про теми дисертаційних робіт	-	-	1	-	-	-	1
Про оплату атестатів	-	-	-	-	2	-	2
Про видачу дублікатів дипломів доктора, кандидата наук та доктора філософії	-	-	-	3	1	-	4
Про основоположні документи	-	-	1	-	-	-	1
Методичні	-	2	1	-	-	-	3
Інше (Листи МОН)	-	-	3	3	7	-	13
Всього	5	9	8	8	13	3	46

При такому темпі наростання нормативних актів безумовно умовою забезпечення якісного рівня діяльності від ад'юнкта до спеціалізованої ради вбачається наявність курсів підвищення кваліфікації. Відслідкувати всі нововведення не є складно. Важливо методично врахувати зміни, доповнення, а інколи і потрібні методичні роз'яснення, оскільки в такому круговороті невиключно виникнення парадоксальних випадків.

Розглянемо в хронологічному порядку генезис категорії нормативно-правової бази з питань організації підготовки наукових та науково-педагогічних кадрів вищої кваліфікації в Україні.

До початку 90-х років ХХ століття законодавча база наукової діяльності в країні фактично була

відсутня. У процесі реформування економіки і соціально-політичної системи наука через об'єктивні й суб'єктивні причини фактично була виведена з головних пріоритетів держави. Внаслідок цього, хоча завдання створення законодавчої бази науки стояло досить гостро, розробка і ухвалення необхідних нормативно-правових актів були уповільнені.

Хронологія генезису категорії нормативно-правової бази з питань організації підготовки наукових та науково-педагогічних кадрів вищої кваліфікації в Україні подано в (табл. 3). Як можна побачити з таблиці тривалий час нормативно-правовою основою не змінювалася.

Таблиця 3.

Хронологія генезису категорії нормативно-правової бази з питань організації підготовки наукових та науково-педагогічних кадрів вищої кваліфікації в Україні та для потреб Збройних Сил України

Тип	Назва документа	набуття чинності	втрата чинності
Закон України	Про вищу освіту // Закон України від 17.01.2002 № 2984-III	17.01.2002	06.09.2014
Закон України	Про вищу освіту // Закон України від 01.07.2014 № 1556-VII	01.07.2014	-
Закон України	Про наукову і науково-технічну діяльність // Постанова ВР №1978-XII (1978-12) від 13.12.1991	13.12.1991	16.01.2016
Закон України	Про наукову і науково-технічну діяльність // Закон України від 26.11.2015 № 848-VIII	16.01.2016	-

Теоретичні основи створення і використання інформаційних технологій

Постанова Кабінет Міністрів України	Про затвердження Положення про підготовку науково-педагогічних і наукових кадрів // Положення від 01.03.1999 №309	01.03.1999	01.01.2019
Постанова Кабінет Міністрів України	Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах) // Перелік від 23.03.2016 №261	23.03.2016	–
Наказ Міністра оборони України	Положення про організацію наукової і науково-технічної діяльності у Збройних Силах України. Наказ Міністра оборони України від 13.01.2007 № 9.	13.01.2007	–
Наказ Міністерства оборони України та Міністерства освіти і науки України	Про затвердження Про затвердження Положення про підготовку науково-педагогічних і наукових кадрів у Збройних Силах // Наказ Міністерства оборони України та Міністерства освіти і науки України від 01.12.1993 №280/416	01.12.1993	18.07.2000
Наказ Міністерства оборони України та Міністерства освіти і науки України	Інструкція про організацію підготовки науково-педагогічних і наукових кадрів у ЗС України // Наказ Міністра оборони України / Наказ Міністерства оборони України та Міністерства освіти і науки України від 30.06.2000 №194/265	30.06.2000	–
Наказ Міністерства оборони України та Міністерства освіти і науки України	Зміни до Інструкції про організацію підготовки науково-педагогічних і наукових кадрів у Збройних Силах України, затвердженої наказом / Наказ Міністерства оборони України та Міністерства освіти і науки України від 30.06.2000 №194/265, зареєстрованої у Міністерстві юстиції України 18.07.2000 №433/4654 // Наказ від 14.11.2006 № 662/771	14.11.2006	–
Постанова Кабінет Міністрів України	Про затвердження Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника // Постанова Кабінет Міністрів України від 07.03.2007 №423	07.03.2007	30.08.2013
Постанова Кабінет Міністрів України	Про затвердження Порядку присудження наукових ступенів // Постанова Кабінет Міністрів України від 24.07.2013 № 567	24.07.2013	–
Наказ Вищої атестаційної комісії України	Перелік спеціальностей, за якими проводяться захист дисертацій на здобуття наукових ступенів кандидата наук і доктора наук, присудження наукових ступенів і присвоєння вчених звань // Наказ Вищої атестаційної комісії України від 23.06.2005 № 377	23.06.2005	17.10.2011
Наказ Міністерства освіти і науки, молоді та спорту України	Перелік наукових спеціальностей // Наказ Міністерства освіти і науки, молоді та спорту України від 14.09.2011 №1057	14.09.2011	–

В найближчій перспективі доречно переглянути обсяг навчального часу з дисциплін „Нормативно-правова основа (вищої освіти, наукової та науково-дослідницької діяльності)”. Діючий обсяг часу наведено в табл. 4. Як можна встановити з наявних даних відведеного обсягу

бюджету часу на вивчення ад’юнктами дисциплін „Нормативно-правова основа (вищої освіти та наукових науково-дослідницької діяльності)” є недостатнім для самостійного опанування, а тому пропонується збільшити час.

Таблиця 4.

Обсяг часу дисциплін “Нормативно-правова основа діяльності”

№ п/п	Найменування дисципліни	Всього годин навчальних занять	В тому числі за роками підготовки			Звітність
			1	2	3	
1.	Нормативно-правові основи вищої освіти	30	30	–	–	залік
2.	Нормативно-правові основи наукової та науково-дослідницької діяльності	30	30	–	–	залік

Річ в тому, що нормативні положення коригуються, виявляються ще більш наукового законодавства, які дуже часто суперечливими, розмитими і неузгодженими з

реальними потребами розвитку науково-технічної сфери, ніж правові норми, що діяли раніше. Саме наукове законодавство є незавершеним і внутрішньо суперечливим, що знижує його регулятивний потенціал, перешкоджає реформуванню науково-технічної сфери.

Висновки та перспективи подальших досліджень

Таким чином, можна сформулювати наступні висновки:

найпростішим і очевидним, але не раціональним напрямком рішення проблеми є запровадження постійно діючих курсів підвищення кваліфікації, що є необхідною умовою розвитку у наукових та науково-педагогічних кадрів вищої кваліфікації знань нормативно-правової складової об'єктного компонента методологічної культури, але як роз'яснювання тонкощів юриспруденції;

раціональним є якісно формувати і розвивати методологічну культуру ад'юнктів, а цьому сприяє своєчасне опанування знань нормативно-правової основи організації наукових досліджень;

доречно споживачу нормативно-правових актів в сфері науки і освіти надавати у вигляді системного, результуючого документа. Це не створюватиме імпліцитне бачення і індивідуальне розуміння споживача. В результаті формується у споживача спотворена внутрішня картина світу.

Література

1. Мельников И. И. Структура законодательства о науке как отрасли права / И. И. Мельников, Г. К. Сафаралиев, А. П. Бердашкевич. – М.: Изд. Гос. Думы, 2002. – 264 с. 2. Селіванов А. О. Наука і закон: Перший досвід системного аналізу законодавства у сфері науки і науково-технічної діяльності / А. О. Селіванов. – К.: Логос, 2003. – 262 с. 3. Інноваційне законодавство України: Повне зібрання норм.-прав. Актів у 3-х томах / За ред. Костецького В. В., Ришова В. Л. – К.: 2003. 4. Атестація наукових кадрів вищої кваліфікації в Україні: проблеми

Елемент наукової новизни. Автором в контексті об'єкту дослідження визначено приналежність ключової нормативно-правової бази, яка визначає єдиний порядок організації підготовки наукових та науково-педагогічних кадрів вищої кваліфікації в Україні та для потреб Збройних Сил України, що виступає нормативно-правовою складовою об'єктного компонента методологічної культури ад'юнктів.

Теоретичне значення дослідження полягає в розвитку теорії методологічної культури ад'юнктів.

Практичне значення дослідження полягає у вишукуванні структурно-логічної послідовності нормативно-правової бази об'єктного компонента методологічної культури ад'юнктів, розуміння якого сприяє зростанню соціально-економічного ефекту при підготовці здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах). Також покращення організації підготовки зазначеної категорії для потреб Збройних Сил України.

Найближчою перспективою подальшого дослідження полягає в проведенні аналізу сучасної традиційної складової об'єктного компонента методологічної культури ад'юнктів для доповнення аналізу національних особливостей систем підготовки і атестації вчених [5].

і рішення / В. І. Сергієнко, І. Б. Жилиєв, В. І. Торкатюк. – Харків: ХНАМГ, 2006. – 228 с. – ISBN 966-695-069-3.

5. Козубцов І. М. Національні особливості та перспективні принципи удосконалення систем підготовки і атестації вчених в контексті Болонського процесу / І. М. Козубцов // Вісник Глухівського національного педагогічного університету імені Олександра Довженка: зб. наук. праць. 2012. – Вип. 20. – С.50–54. – (Серія: Педагогічні науки; вип. 20). – ISBN 966-7763-85-4.

АНАЛИЗ НОРМАТИВНО-ПРАВОВОЙ СОСТАВЛЯЮЩЕЙ ОБЪЕКТНОЙ КОМПОНЕНТЫ МЕТОДОЛОГИЧЕСКОЙ КУЛЬТУРЫ АДЪЮНКТОВ

Игорь Николаевич Козубцов (канд. техн. наук, с.н.с.)

Военный институт телекоммуникаций и информатизации, Киев, Украина

В статье проанализированы и объединены в группу ключевая нормативно-правовая и законодательная база, на которой основывается подготовка соискателей высшего образования степени доктора философии и доктора наук в высших учебных заведениях (научных учреждениях). Отдельно выделены подгруппу документов, на основе которых организуется подготовка указанной категории именно для нужд Вооруженных Сил Украины. Перечисленная нормативно-правовая и законодательная база составляет объектную составляющую методологической культуры адъюнктов и аспирантов. Автором в контексте объекта исследования определены принадлежность ключевой нормативно-правовой базы, которая определяет единый порядок организации подготовки научных и научно-педагогических кадров высшей квалификации в Украине и для нужд Вооруженных Сил Украины и выступает нормативно-правовой составляющей объектного компонента методологической культуры адъюнктов. Теоретическое значение исследования заключается в развитии теории методологической культуры адъюнктов.

Ключевые слова: адъюнкт; адъюнктура; методология; организация деятельности; методологическая компетентность; методологическая культура; научный руководитель; нормативно-правовая основа; объектный компонент.

THE ANALYSIS OF REGULATORY CONSTITUENT OBJECTIVE COMPONENT OF ADJUNCTS
METHODOLOGICAL CULTURE

Ihor M. Kozubtsov (Candidate of Technical Sciences, Senior Research Fellow)

Military Institute of Telecommunications and Informatization, Kyiv, Ukraine

The article analyzes and cohesive key regulatory and legislative framework on which to base the preparation of candidates for higher education the degree of doctor of philosophy and doctor of science in higher educational institutions (scientific institutions). A separate subset of documents based on which training was provided to the specified categories specifically for the needs of the Armed Forces of Ukraine. Listed in the regulatory and legislative framework is the object component of methodological culture of adjuncts and graduate students. The author in the context of the object of study, determined the identity of the key normative-legal base, which defines a uniform procedure for the organization of training scientific and scientific-pedagogical personnel in Ukraine and for the needs of the Armed Forces of Ukraine and acts of legal-regulatory component object component of methodological culture of adjuncts. Theoretical value of research consists in the development of the theory of methodological culture of adjuncts.

Keywords: *adjunct; adjuncture; methodology; organization of activities; methodological competence; methodological culture; scientific director; regulatory framework; component object.*

References

- 1. Melnikov I.I., Safaraliev G.K., Berdashkevich A.P.** (2002), The structure of the law on science as a branch of law. [Struktura zakonodatelstva o nauke kak otrasli prava], Moscow: Izd. Gos. Dumyi, 264 p. **2. Selivanov A.O.** (2003), Science and law: first experience of system analysis of legislation in the field of science and scientific and technological activities. [Nauka i zakon: Pershyj dosvid systemnogho analizu zakonodavstva u sferi nauky i naukovotekhnichnoji dijalnosti], Kyiv: Loghos, 262 p. **3. Innovative legislation** of Ukraine: Complete norm. law. Acts 3 vols. [Innovacijne zakonodavstvo Ukrainy] (2003): Povne zibrannja norm.-prav. aktiv. U 3-kh tomakh, Za red. Kostecjkogho V.V., Ryzhova V.L., Kyiv. **4. Serghijenko V.I., Zhyljajev I.B., Torkatjuk V.I.** (2006). Certification of qualified scientists in Ukraine: Problems and solutions. [Atestacija naukovykh kadriv vyshhoji kvalifikaciji v Ukraini: problemy i rishennja], Kharkiv: KhNAMGh, 228 p., ISBN 966-695-069-3. **5. Kozubtsov I.N.** (2012), National characteristics and advanced principles of improving training and certification of scientists in the context of the Bologna Process. [Nacionaljni osoblyvosti ta perspektyvni pryncypy udoskonalennja system pidgotovky i atestaciji vchenykh v konteksti Bolonsjkogho procesu], Visnyk Ghlukhivskogho nacionaljnogho pedagoghichnogho universytetu imeni Oleksandra Dovzhenka: zb. nauk. Pracj, Vyp. 20, pp. 50-54, (Serija: Pedagoghichni nauky; vyp. 20), ISBN 966-7763-85-4.

Отримано: 25.05.2016 року.

Олександр Миколайович Косогов (канд. військ. наук, с.н.с.)
Анатолій Олександрович Сірик

Військова частина А1906

МОДЕЛЮВАННЯ ПРОЦЕСУ ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ЕКСПЕРТНИХ ВИСНОВКІВ

Запропонований метод моделювання процесу оцінювання інформаційної безпеки на основі експертних висновків, який може бути застосований для оцінювання комплексної безпеки різних систем. При цьому елементи, що характеризують систему, утворюють ієрархію, а фактори одного підрівня ієрархії полягають у відношеннях переваги (байдужості) один до одного. Як інтегрований критерій при оцінюванні безпеки використовується мультиплікативна згортка.

Зазначений метод може бути використаний для визначення показника рівня комплексної безпеки на базі агрегування значень з усіх рівнів ієрархії факторів на основі якісних даних про рівні факторів і їхніх відношень порядку на одному рівні ієрархії.

Ключові слова: інформаційна безпека; експертне оцінювання; рівні ієрархії; показник комплексної безпеки.

Вступ

Постановка проблеми. Проблеми забезпечення інформаційної безпеки у війсьній сфері, з огляду на появу нових та зростання рівня існуючих ризиків і загроз в інформаційному просторі України, набувають великої значущості і потребують відповідного наукового підґрунтя для їх вирішення. Одним з напрямів розв'язання цих проблем є постійне удосконалення науково-методичного забезпечення інформаційної безпеки, а саме визначення спрямованості загроз та оцінювання їх рівня, виявлення об'єктів інформаційного впливу та оцінювання ефективності заходів протидії.

Аналіз останніх досліджень і публікацій. Є низка публікацій, що присвячені проблемам інформаційної безпеки в інформаційних системах і мережах передачі та обробки інформації. Завдання створення, організації і дослідження процесів функціонування, удосконалення й розвитку систем забезпечення безпеки інформації тою чи іншою мірою висвітлені в працях вітчизняних і закордонних учених [1–4].

Однак дотепер повною мірою не вивчені та залишаються дискусійними методологічні, методичні й практичні аспекти дослідження проблем моделювання безпеки складних інформаційних систем.

Сучасні науково-практичні напрацювання в Україні, ряд основних міжнародних стандартів містять норми та вимоги, що спрямовані в основному на захист від несанкціонованого доступу. При цьому вони часто не забезпечують базового рівня безпеки, тому що дають змогу моделювати лише частину загроз. При цьому не існує загальноприйнятих стандартів або підходів, що дозволяють забезпечити підвищений або високий рівень захисту. Так само негативним фактором застосування сучасних стандартів є шаблонність пропонованого захисту та відсутність

варіантності.

Метою статті є викладення методики комплексного оцінювання рівня безпеки інформаційних систем, що ґрунтується на якісних шкалах і відношенні переваги між факторами в структурі ієрархії цих факторів.

Виклад основного матеріалу дослідження

Під рівнем інформаційної безпеки системи розуміється оцінка, яка отримана із сукупності показників і критеріїв, що характеризують стан системи на предмет захищеності критичних для неї елементів.

Рівень інформаційної безпеки системи можна характеризувати за такою матрицею:

$$B = \begin{pmatrix} K_1 & F_1 & V_1(T) & S_1 \\ K_2 & F_2 & V_2(T) & S_2 \\ \dots & \dots & \dots & \dots \\ K_n & F_n & V_n(T) & S_n \end{pmatrix},$$

де K_i – показник рівня безпеки за i -м критерієм;

F_i – тенденція зміни i -го критерію (зростає, убиває, незмінний);

$V_i(T)$ – швидкість зміни i -го критерію, що є функцією часу T (наприклад: низька, нижче середнього, середня, вище середнього, висока);

S_i – ступінь критичності негативних наслідків при реалізації загроз, яка погіршує значення i -го критерію.

Матрицю виду B в подальшому будемо називати матрицею безпеки (МБ).

Перший і четвертий стовпці МБ являють собою вектор часткових критеріїв безпеки і їх ваги та характеризують поточний стан комплексної інформаційної безпеки, даючи змогу оцінити ситуацію, що склалася на даний момент часу. Другий і третій стовпці матриці відображають динаміку розвитку процесів та дають змогу прогнозувати їх розвиток у подальшому.

У цьому випадку мультиплікативна згортка

інтегрального критерію комплексної безпеки являє собою величину

$$K = \prod_i K_i^{S_i}$$

Оцінки S_i можуть бути отримані експертним шляхом з використанням різних рангових методів, реалізація яких вимагає впорядкувати ці критерії [5-8].

Наприклад, можна використати метод нестрогого ранжування, відповідно до якого експертом нумерується всі критерії в порядку зниження рівня негативних наслідків, які пов'язані з цим критерієм безпеки. Критерії, які уже пройшли процес ранжування, послідовно нумеруються. Оцінка (ранг) критерію визначається за його номером [6].

Якщо на одному місці знаходяться декілька не розрізних між собою критеріїв, то оцінювання кожного з них приймається за середнє арифметичне їх нових номерів [7-8]. Однак, вважається за доцільне модифікувати такий метод оцінювання, прийнявши за ранг для кожного з не розрізних критеріїв номер усієї групи як цілого об'єкта за ступенем впорядкування.

У такий спосіб можуть бути оцінені як ступені впливу кожного параметра на часткові критерії безпеки K_i , так і ступені прийнятності наслідків реалізації загроз S_i .

Наприклад, будемо вважати, що експерт упорядкував критерії в такий спосіб:

$$K_5, (K_3, K_7, K_2), K_1, (K_6, K_8), K_9, K_4.$$

Критерії, які не розрізнені між собою, об'єднані в круглі дужки. Тоді оцінки для кожного із критеріїв, які обчислені відповідно до описаної вище процедури, дорівнюють:

$$S_5=1; S_3=S_7=S_2=2; S_1=3; S_6=S_8=4; S_9=5; S_4=6$$

Для цього застосуємо нормування за величиною, яка дорівнює сумі всіх оцінок:

$$S_{\text{норм}} = \sum_i S_i,$$

У нашому випадку $S_{\text{норм}}=29$. Таким чином, після лінійного перетворення в шкалу $[0;1]$ за нормою $S_{\text{норм}}$ отримаємо:

$$S_5 = \frac{1}{29}; S_3=S_7=S_2 = \frac{2}{29};$$

$$S_1 = \frac{3}{29}; S_6=S_8 = \frac{4}{29}; S_9 = \frac{5}{29}; S_4 = \frac{6}{29}.$$

Визначені запропонованим способом оцінки є узагальненням системи ваги Фішберна [9] у випадку змішаного розподілу переваг, коли порядок з перевагами в систему входять і відношення рівнозначності.

Отже, кожний рядок матриці безпеки (K_i, F_i, V_i, S_i) характеризує стан безпеки за i -м критерієм.

Часткові матриці, що складаються з рядків та визначають певний напрям забезпечення безпеки, у свою чергу, описують стан у відповідній області.

Показники рівня безпеки K_i тісно пов'язані з наслідками від можливої реалізації наявних у системі загроз та заходами, які спрямовані на попередження, запобігання, локалізацію й усунення таких наслідків.

Отриманий результат узгоджується з добре відомим у теорії прийняття рішень фактом [5,7,9]: система убуваючої переваги альтернатив найкраще відповідає системі ваг, що знижуються за правилом арифметичної прогресії.

Загрози, що впливають на безпеку системи, являють собою набір неупорядкованих факторів одного рівня ієрархії.

Вплив різних факторів на рівень комплексної безпеки може бути показаний у вигляді орієнтованого графа G , що має одну кореневу вершину та не містить петель і горизонтальних ребер в межах одного рівня ієрархії:

$$G = (\{F_i\}; \{D_{ij}\}),$$

де $\{F_i\}$ – множина факторів (вершин графа); $\{D_{ij}\}$ – множина дуг, що з'єднують i -ту і j -ту вершини; $F_0 = K$ – коренева вершина, що відповідає рівню комплексної безпеки в цілому (інтегральному критерію безпеки). При цьому дуги розташовані так чином, що початку дуги відповідає вершина нижнього рівня ієрархії (рангу), а кінцю дуги – вершина рангу, що є на одиницю меншим. Прикладом такого графа може служити чотирирівневий граф, в якому на нижньому, третьому рівні розташовані негативні фактори N_i , що впливають на безпеку системи, і Z_i – фактори, що демпфують та пов'язані із застосуванням превентивних заходів забезпечення безпеки, а також мають послабити вплив певних загроз (негативних факторів) [10]. На рівень вище розташовані загрози безпеки системи U_i . На рівнях з першого до передостаннього знаходяться часткові критерії безпеки K_i , а кореневій вершині нульового рівня відповідає комплексний критерій безпеки K .

Слід зазначити, що цей граф не є деревом, оскільки не виконується вимога відсутності простих циклів. Це обумовлено тим, що фактори, які перебувають на нижньому рівні ієрархії, можуть одночасно впливати на декілька факторів більш високого рівня. Наприклад, застосування превентивних заходів захисту від однієї загрози може одночасно з послабленням негативних наслідків цієї загрози підсилювати або зменшувати вплив тієї чи іншої загрози. Деякі негативні фактори можуть викликати зміни відразу декількох часткових критеріїв безпеки (іноді в протилежному напрямку).

Для подальшої побудови моделі комплексної безпеки системи на визначений граф необхідно накласти систему відношень переваг одних факторів над іншими за ступенем їхнього впливу на заданий елемент наступного рівня ієрархії:

$$E = \{F_i(e)F_j | e \in \{>, \approx\}\}, \quad (1)$$

де F_i, F_j – фактори одного рівня ієрархії;

$>$ – відношення переваги;

\approx – відношення байдужості.

Така система може бути отримана, наприклад, викладеним вище способом нестрогого ранжирування. Приклад накладення системи відношень переваги типу (1)

$E=\{N_1 > N_2; N_2 \in N_3 \approx N_4; N_4 \approx N_5\}$ на фрагмент графа зображений на рис.1.

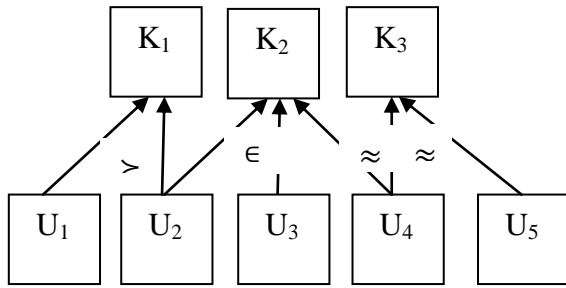


Рис. 1. Приклад системи відношень переваг на одному з рівнів ієрархії

При цьому залишається ввести для розгляду набір якісних оцінок рівнів кожного фактора в ієрархії:

$$L = \{\text{дуже низький рівень (ДН), низький рівень (Н), середній рівень (С), високий рівень (В), дуже високий рівень (ДВ)}\} \quad (2)$$

За математичну модель оцінювання комплексної безпеки системи (KBS) може бути прийнятий кортеж:

$$KBS = \langle G, L, E \rangle$$

Наступним кроком є визначення показника рівня комплексної безпеки на базі агрегування значень з усіх рівнів ієрархії факторів (на основі якісних даних про рівні факторів і порядок їхнього відношення на одному із цих рівнів).

Для оцінювання рівня комплексної безпеки з кількісного і якісного боку необхідно агрегувати дані, зібрані в межах ієрархії G. При цьому агрегування відбувається за напрямками дуг графа ієрархії.

Агрегуванню має підлягати не окреме значення обраної функції належності в структурі лінгвістичної змінної “Рівень фактора”, а вся функція належності в цілому. Для цього сформуємо лінгвістичну змінну “Рівень фактора” з терм-множиною значень L (2). Як сімейство функцій належності може бути стандартний п’ятирівневий 01-класифікатор, де функції належності – трапецієподібні нечіткі числа [9]:

$$ДН = \mu_1(x) = \begin{cases} 1, & 0 \leq x < 0,15 \\ 10(0,25-x), & 0,15 \leq x < 0,25 \\ 0, & 0,25 \leq x < 1 \end{cases} \quad (3)$$

$$Н = \mu_2(x) = \begin{cases} 0, & 0 \leq x < 0,15 \\ 10(x-0,15), & 0,15 \leq x < 0,25 \\ 1, & 0,25 \leq x < 0,35 \\ 10(0,45-x), & 0,35 \leq x < 0,45 \\ 0, & 0,45 \leq x < 1 \end{cases} \quad (4)$$

$$С = \mu_3(x) = \begin{cases} 0, & 0 \leq x < 0,35 \\ 10(x-0,35), & 0,35 \leq x < 0,45 \\ 1, & 0,45 \leq x < 0,55 \\ 10(0,65-x), & 0,55 \leq x < 0,65 \\ 0, & 0,65 \leq x < 1 \end{cases} \quad (5)$$

$$В = \mu_4(x) = \begin{cases} 0, & 0 \leq x < 0,55 \\ 10(x-0,55), & 0,55 \leq x < 0,65 \\ 1, & 0,65 \leq x < 0,75 \\ 10(0,85-x), & 0,75 \leq x < 0,85 \\ 0, & 0,85 \leq x < 1 \end{cases} \quad (6)$$

$$ДВ = \mu_5(x) = \begin{cases} 0, & 0 \leq x < 0,75 \\ 10(0,75-x), & 0,75 \leq x < 0,85 \\ 0, & 0,85 \leq x < 1 \end{cases} \quad (7)$$

де x – 01-носій (відрізок [0, 1] відповідної осі).

Стандартний класифікатор здійснює проекцію нечіткого лінгвістичного опису на 01-носій, при цьому робить це несуперечливим способом, симетрично розташовуючи вузли класифікації (0,1; 0,3; 0,5; 0,7; 0,9) [11].

У цих вузлах значення відповідної функції належності дорівнює одиниці, а всіх інших функцій – нулю. Непевність експерта в класифікації зменшується (збільшується) лінійно з віддаленням від вузла (з наближенням до вузла, відповідно). При цьому сума функцій належності в всіх точках носія дорівнює одиниці.

Зазначений класифікатор є різновидом так званої “сірої” шкали Поспелова [12], що являє собою полярну (опозиційну) шкалу, в якій перехід від властивості A⁺ до властивості A⁻ відбувається поступово.

Подібні шкали задовольняють умову взаємної компенсації між властивостями A⁺ і A⁻ (чим більшою мірою проявляється A⁺, тим менше проявляється A⁻, і навпаки).

Таким чином, здійснюється перехід від якісного опису рівня параметра до стандартного кількісного вигляду відповідної функції належності (нечітке трапецієподібне число) [13].

Якщо за кожним показником (F_{*1} ... F_{*n}) на обраному підрівні (*) ієрархії G відомі лінгвістичні оцінки L = (L_{*1} ... L_{*n}), а також визначена система ваг Фішберна P = (p_{*1} ... p_{*n}) на основі наведеної вище системи переваг E, то показник підрівня F* характеризується своєю лінгвістичною оцінкою, що обумовлена функцією належності на 01-носії x.

У таких випадках для агрегування зазвичай застосовується ОWA-оператор Ягера [14], причому вагами в згортці виступають згадані вище коефіцієнти Фішберна.

Однак, як було показано раніше, адитивна згортка та осереднення для оцінювання рівня безпеки системи неприйнятні, тому необхідно використати мультиплікативну згортку для обчислення інтегральних критеріїв:

$$\mu(x) = \prod_{i=1}^n \mu_{*j}^{p_j}(x), \quad (8)$$

де

$$\mu_{*j} = \begin{cases} (3), & \text{якщо } L_{*j} = (\text{ДН}) \\ (4), & \text{якщо } L_{*j} = (\text{Н}) \\ (5), & \text{якщо } L_{*j} = (\text{С}) \\ (6), & \text{якщо } L_{*j} = (\text{В}) \\ (7), & \text{якщо } L_{*j} = (\text{ДВ}) \end{cases} \quad (9)$$

Отриману функцію (8) необхідно лінгвістично

розпізнати, щоб зробити висновок про якісний рівень показника F^* . Для цього потрібно співвіднести отриману функцію $\mu_*(x)$ і функції $\mu_j(x)$ відповідно (3)-(7).

$$\text{Якщо } (\forall x \in [0, 1]) \sup \min (\mu_*(x), \mu_j(x)) = 0, \quad (10)$$

то рівень показника F^* однозначно не розпізнається як рівень, якому відповідає i -та "еталонна" функція належності. Повне розпізнавання настає, якщо виконується

$$(\forall x \in [0, 1]) \min (\mu_*(x), \mu_j(x)) = \mu_j(x) \quad (11)$$

У всіх проміжних випадках необхідно задатися мірою рівня розпізнавання, тобто ввести так званий індекс подібності (ІП) [15]. Для цього потрібно визначити поняття відстані між двома нечіткими числами A і B .

За таку величину може виступати лінійна (хемінгова):

$$\rho(A, B) = \int_0^1 |\mu_A(x) - \mu_B(x)| dx. \quad (12)$$

або квадратична (евклідова) відстань:

$$\rho(A, B) = \int_0^1 \sqrt{(\mu_A(x) - \mu_B(x))^2} dx. \quad (13)$$

Для визначення ІП необхідно обчислити відстань у точках, для яких виконується нерівність:

$$\mu_*(x) < \mu_j(x) \quad (14)$$

З метою підвищення інформативності перейдемо до відносної відстані:

$$\tilde{\rho} = \frac{\rho}{M} \quad (15)$$

де M – "потужність" еталонного нечіткого числа, яка дорівнює площині фігури, що описується її функцією належності. У нашому випадку це площа трапеції.

Для того щоб уникнути лінгвістичної невідповідності (чим вище ступінь близькості, тим більше повинен бути ІП) і з огляду на те, що $\rho(A, B) \leq 1$, за ІП можна прийняти величину

$$\text{ІП} = 1 - \rho(A, B) \quad (16)$$

Отже, ІП, змінюючись у діапазоні від 0 до 1, буде характеризувати близькість знайденої мультиплікативної згортки до тієї чи іншої еталонної функції належності виду (3)-(7).

Варто зауважити, що для збереження лінгвістичної відповідності при визначенні згорток значення деяких показників необхідно попередньо інвертувати.

Наприклад, при переході від рівня негативних факторів N_i і превентивних заходів безпеки Z_i на рівень загроз безпеки U_i перед знаходженням

згортки необхідно інвертувати значення показника Z_i , а при переході з рівня U_i до рівня часткових критеріїв безпеки K_i інвертувати значення U_i відповідно до табл. 1.

Таблиця 1

Інверсія лінгвістичних змінних

№ терм-множини	Рівень показника F	Інвертоване значення F
1.	ДН	ДВ
2.	Н	В
3.	С	С
4.	В	Н
5.	ДВ	ДН

Таким чином, розглянувши послідовно знизу вгору за всіма рівнями ієрархії G і застосовуючи співвідношення (1)-(16), можна шляхом комплексного агрегування даних не тільки зробити висновок про якісний рівень показника на кожному шаблі ієрархії (до $F_0 = K$), але й оцінити ступінь обґрунтованості певного судження за допомогою ІП.

Якщо крім якісних значень показників є кількісні дані, то найпростішим способом для їхнього спільного урахування при комплексному оцінюванні є узагальнення отриманих кількісних оцінок до якісного їхнього опису та подальший перехід до викладеної вище моделі оцінювання.

Висновки й перспективи подальших досліджень

Запропонований метод моделювання процесу оцінювання ІБ на основі експертних висновків може бути застосований для оцінювання комплексної безпеки різних систем. При цьому елементи, що характеризують систему, утворюють ієрархію, а фактори одного підрівня ієрархії полягають у відношенні переваги (байдужості) один до одного. Як інтегрований критерій при оцінюванні безпеки використовується мультиплікативна згортка.

Застосування модифікованого методу нестрогого ранжування дає змогу визначити ваги Фишберна для факторів одного рівня ієрархії та отримати узагальнення даних ваг на загальний випадок переваги (байдужості) факторів стосовно один до одного.

Отриманий опис може бути використаний для побудови показника рівня комплексної безпеки на базі агрегування значень з усіх рівнів ієрархії факторів на основі якісних даних про рівні факторів і їхніх відносин порядку на одному рівні ієрархії.

Література

1. Садердинов А. А. Информационная безопасность предприятия / А. А. Садерников, В. А. Трайнев, А. А. Федулов. – М.: Изд.-торг. корпорация "Дашков ДО" – 2005. – 336 с. 2. Курило А. П., Аудит информационной безопасности / А. П. Курило, С. Л. Зефилов, В. Б. Голованов. – М.: Изд. группа "Бдц-пресс" – 2006. – 304 с. 3. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К.: ТОВ "ТИД Дина Софт" – 2004. – 992 с. 4. Попов Г. А. Экономическая кибернетика / Г. А. Попов. – Астрахань: 3 "ЦНТЭП" – 2002. – 96 с.

5. Трухаев Р. И. Модели принятия решений в условиях неопределенности / Р. И. Трухаев. – М.: Наука – 1981. – 144 с. 6. Недосекин А. О. Вероятное распределение с нечеткими параметрами. Режим доступа: http://sedok.narod.ru/sc_group.html#book_2. 7. Литвак Б. М. Экспертная информация: методы получения и анализа / Б. М. Литвак. – М.: Радио и связь – 1982. – 92 с. 8. Фишберн П. Теория полезности для принятия решений / П. Фишберн. – К.: Наука, 1978. – 155 с. 9. Рыжов А. П. Элементы теории нечетких множеств и измерение нечеткостей / А. П. Рыжов. – М.: Диалог-

мгу – 1998. – 102 с. **10. Косо́гов О. М.** Модель динаміки зміни рівня інформаційної безпеки системи / О. М. Косо́гов. – К.: зб. наук. праць. ЦВСД НУО імені Івана Черняхівського. – 2015. – № 2(54) – С. 76–79. **11. Kaufmann A., Gupta M.** Introduction to Fuzzy Arithmetic: Theory and Applications. - Van Nostrand Reinhold, 1991. – 161 p. **12. Поспелов Д. С.** “Сірі” або “чорно-білі” шкали / Д. С. Поспелов. Прикладна ергономіка. “Рефлексивні процеси”. Спец. вип. – 1994. –

№ 1. – С. 15–21. **13. Недосекин А. О.** Нечеткое парное сравнение // Аудит и финансовый анализ. – 2003. – № 5. – С. 53. **14. Yager.** Families of OWA operators // Fuzzy Sets and Systems. – 1993. – 59. – pp. 53–59. **15. Проталинский О. М.** Применение методов искусственного интеллекта при автоматизации технологических процессов / О. М. Проталинский – Астрахань: 3 АГТУ – 2004. – 184 с.

МОДЕЛИРОВАНИЕ ПРОЦЕССА ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ЭКСПЕРТНЫХ ВЫВОДОВ

*Александр Николаевич Косо́гов (канд. воен. наук, с.н.с.)
Анатолий Александрович Сирьк*

Воинская часть А1906

Предложен метод моделирования процесса оценки информационной безопасности на основе экспертных выводов, который может быть применен для оценивания комплексной безопасности различных систем. При этом элементы, которые характеризуют систему, образуют иерархию, а факторы одного подуровня иерархии составляют в отношениих преимущества (безразличия) один к другому. В качестве интегрального критерия при оценке безопасности используется мультипликативная свертка.

Полученное описание может быть использовано для построения показателя уровня комплексной безопасности на базе агрегирования значений из всех уровней иерархии факторов на основе качественных данных о факторах и отношений их порядка на одном уровне иерархии.

Ключевые слова: информационная безопасность; экспертное оценивание; равные иерархии; показатель комплексной безопасности.

MODELLING BASED ON THE EXPERT JUDGEMENTS OF THE PROCESS OF INFORMATIONAL SAFETY EVALUATION

*Oleksandr M. Kosohov (Candidate of Military Sciences, Senior Research Fellow)
Anatoliy O. Siryk*

Military Unit A1906

The method of modeling information security evaluation process based on expert findings, which can be used for evaluation of various integrated security systems. The elements that characterize the system, constitute a hierarchy, and the factors for one sublevel of hierarchy being established in respect the benefits (indifference) to each other. As an integral criterion for safety assessment is used the multiplicative convolution.

This description can be used to construct a comprehensive index of safety level based on the aggregation of values from all levels of hierarchy factors based on the qualitative data on factors affecting and their relations order of the same level of hierarchy.

Keywords: information security; expert evaluation; equal hierarchy; integrated security measure.

References

1. Saderdinov A.A. Traynev V.A., Fedulov A.A. (2005), Information security of an enterprise. [Informatsionnaia bezopasnost predpriiatiia], textbook. Allowance, Moscow: Izd.-Torg. Corporation “Dashkov Co”, 336 p. **2. Kyrilov A.P.,** Zefirov S.L., Golovanov V.B. (2006), Information security Audit, [Audit informatsionnoi bezopasnosti], Moscow: Publishing House. Group “BDCpress”, 304 p. **3. Domarev V.V.** (2004), Methodology creating of system for informations defense, Security of information technologies, A systematic approach, [Bezpeka informatsiinykh tekhnolohii. Systemnyi pidkhid], Kyiv: “TID Dia Software”, 992 p. **4. Popov G.A.** (2002), In Economic Cybernetics, [Ekonomicheskaiia kibernetika], Astrakhan: Publishing house “CNCEP”, 96 p. **5. Troukhaev R.I.** (1981), Models of decision making under uncertainty. [Modeli priniatiia rishenii v usloviakh neopredelennosti] Moscow: Nauka, 144 p. **6. Nedosekin A.O.** Probabilistic distributions with fuzzy parameters. [Veroiatnoe raspredelenie s nechetkimi parametrami], http://sedok.narod.ru/sc_group.html#book_2. **7. Litvak B. G.** (1982), Expert information: methods for obtaining and analysis, [Ekspertnaia informatsiia: metody polucheniia i analiza], Moscow: Radio and communication, 92 p. **8. Fishburn P.** (1978), Theory for decision-making.

[Teoriia korysnosti dlia pryiniattia rishen], Moscow: Nauka, 155 p. **9. Ryjov A.** (1998) Elements of the theory of fuzzy sets and measure of fuzziness. [Elementy teorii nechetkikh mnozhestv i izmerenie nechetkosti], Moscow: Dialogue-MSU, 102 p. **10. Kosogov O.M.** (2015), Level change dynamics model of the information security of the system. [Model dynamiky zminy ravnii informatsiinoi bezpeky systemy], Kyiv: CMSR National University of Defense of Ukraine name by Ivan Chernyakhovski, No. 2 (54), pp. 76–79. **11. Kaufmann A., Gupta M.** (1991), Introduction to Fuzzy Arithmetic: Theory and Applications, Van Nostrand Reinhold, 161 p. **12. Pospelov D.S.** (1994), “Grey” and/or “black and white”. [“Siri” abo “chorno-bili” shkaly], Applied ergonomics. Spec. vol. The “Reflexine processes”, No. 1, pp. 15-21. **13. Nedosekin A. O.** (2003), Fuzzy pairwise comparisons, Audit and financial analysis. [Nechetkoe parnoe sravnenie], Audit i finansovyi analiz, No.5, p. 53. **14. Yager R.** (1993), Families of OWA operators, Fuzzy Sets and Systems. No. 59, pp. 53-59. **15. Protalinski O. M.** (2004), Application of artificial intelligence techniques in the automation technological processes. [Primenenie metodov iskusstvennogo intellekta pri avtomatizatsii tekhnologicheskikh protsessov], Astrakhan: publishing house of ASTU, 184 p.

Отримано: 13.08.2016 року.

Микола Богданович Кубявка

Любов Богданівна Кубявка (канд. техн. наук, доцент)

Київський національний університет імені Тараса Шевченка, Київ, Україна

КОНЦЕПТУАЛЬНА МОДЕЛЬ ВИЗНАЧЕННЯ НЕОБХІДНИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ НА ПРОТИВНИКА

Метою дослідження є створення науково-обґрунтованих методів управління інформаційними впливами, які можна було б застосувати в управлінні інформаційним супроводженням в процесах підготовки та проведення військових дій. Основна ідея цього дослідження – обґрунтувати та формально представити такі науково-методологічні інструменти управління впливами, які забезпечать значне покращення шляхів підготовки і проведення операцій з інформаційного впливу на противника, здійснення контрзаходів та будуть максимально інформативно зрозумілі, прості, результативні і мінімально затратні. Тому є необхідність розгляду питання управління інформацією не з позицій максимального інформування контрагентів впливу, а з позицій потрібної інформаційної дії на них. При цьому потрібно врахувати не тільки засоби отримання інформації, а й специфіку методів надання інформації, орієнтованих на інформаційну дію на противника. Враховуючи вище зазначене пропонується новий підхід до процесів визначення необхідного для ефективного управління інформованістю інформаційного впливу, що формує нове відношення (світогляд) у контрагента взаємодії. В його основі лежить застосування інструментів теорії несилової взаємодії, яка дає математичний інструментарій для визначення найбільш ефективних способів управління інформаційним супроводженням в процесах підготовки та проведення військових дій.

Ключові слова: управління інформаційним впливом; інформаційні операції; теорія несилової взаємодії.

Вступ

Відомо, що основою ефективного управління військами є інформація. А знання про інформацію, якою володіє противник, є засобом, що дозволяє підсилити нашу міць і знизити міць ворога або протистояти їй, а також захистити наші цінності, включаючи нашу інформацію.

Постановка проблеми. Проблема прийняття рішень командирами завжди пов'язана з якістю інформаційного забезпечення. Адже прийняття рішень в бойових обставинах відрізняється своєю динамічністю, змінами в залежності від обстановки, залежністю від часу. В цьому випадку більш потрібна своєчасна і, зрозуміло, достовірна інформація. Якщо інформація повна, своєчасна, достовірна то в успіх прийнятого рішення, а також його результату можна вірити. Але важливо не тільки отримати інформацію. Важливо яку інформацію отримують керівники, і в якому вигляді. І якщо вимоги повної, своєчасної та достовірної інформації є необхідною умовою ефективного управління, то вимоги “корисності” і “доступності” є достатньою умовою такого управління.

Аналіз останніх досліджень і публікацій.

Технології інформаційної ери зробили можливою теоретичну і практичну можливість - пряме маніпулювання інформацією противника. Інформація з'являється на основі подій навколишнього світу. Події повинні бути сприйняті якимось чином і проінтерпретовані, щоб стати інформацією. Тому інформація це результат двох речей - сприйнятих подій (даних) і команд,

необхідних для інтерпретації даних і зв'язування з ними значення. Відзначимо, що це визначення абсолютно не пов'язано з технологією. Тим не менш, що ми можемо робити з інформацією і як швидко ми можемо це робити, залежить від технології. А якість інформації – це показник труднощі ведення війни. Чим більше якісною інформацією володіє командир, тим більше в нього переваги в порівнянні з його ворогом.

Аналіз останніх досліджень і публікацій виявив, що конче необхідно розглянути питання управління інформацією не з позицій максимального інформування контрагентів впливу, а з позицій потрібної інформаційної дії на них. При цьому потрібно врахувати не тільки засоби отримання інформації, а й специфіку методів надання інформації, орієнтованих на інформаційну дію безпосередньо на контрагента взаємодії.

Мета статті. Враховуючи вище зазначене пропонується новий підхід до процесів визначення необхідного для ефективного управління інформованістю інформаційного впливу, що формує нове відношення (світогляд) у контрагента взаємодії. В його основі лежить застосування інструментів теорії несилової взаємодії [1] та моделей, методів і засобів візуалізації інформації [2], як найбільш впливовішого засобу донесення інформації до людських створінь.

У результаті аналізу джерел виділяються раніше невирішені частини загальної проблеми, яким присвячена стаття.

Виклад основного матеріалу дослідження

У повітряних силах багатьох держав аналіз результатів розвідки і прогнозу погоди є основою для розробки польотного завдання. Точна навігація збільшує ефективність виконання завдання. Всі разом вони є видами військових інформаційних функцій, які збільшують ефективність бойових операцій.

Військові інформаційні функції - це будь-які інформаційні функції, що забезпечують або поліпшують рішення військами своїх бойових завдань.

Беручи до уваги попередній досвід у впливах на супротивника, в проведенні спеціальних інформаційних операцій та інформаційних війн [3] пропонується науково-методологічний базис для розробки інструментів управління впливами, які можна було б застосувати в управлінні інформаційним супроводженням в процесах підготовки та проведення впливів на противника. Основна ідея цього базису – обґрунтувати та формально представити такі науково-методологічні інструменти (технології) управління впливами, які забезпечать значне покращення шляхів підготовки і проведення операцій з інформаційного впливу на противника, здійснення контрзаходів та будуть максимально інформативно зрозумілі, прості, результативні і мінімально затратні.

Для побудови ефективних інформаційних технологій управління інформаційними впливами, на думку автора, на самперед, необхідно провести таку підготовчу роботу:

вивчити об'єкт і ситуацію, в якій здійснюється вплив;

вибрати стратегію, тактику та засоби впливу;

визначити найбільш впливові на контрагента форм представлення інформації та розробити моделі і методи їх формування з допомогою всіх наявних засобів подання (доведення) інформації;

проаналізувати взаємозв'язок між інформацією, яка надається для впливу та інформованістю об'єкта на який здійснюється вплив;

розробити систему аналізу ефективності здійснюваного впливу та його корекції у разі недостатньої дії на контрагента впливу;

організувати протидію контрагенту впливу, якщо від нього здійснюються контрзаходи.

Вимоги до цих інструментів базуються на розумінні умов, в яких знаходяться об'єкти впливу, джерел та якості отримуваної інформації, а також способів формування різноманітних інформаційних представлень. Виходячи з цього, такими вимогами є:

1. Простота.
2. Багатогранність.
3. Алгоритмічна чіткість.
4. Можливість систематизації основних процесів управління інформацією.
5. Відкритість.

Ці вимоги в подальших дослідженнях будуть забезпечуватись:

1. Розробкою шаблонів та методів автоматичного визначення найбільш впливових шляхів представлення інформації (простота).

2. Застосуванням різних інструментів управління впливами, вибір яких буде залежати від інформаційних потреб щодо результатів впливу (багатогранність).

3. Формальними методами представлення інструментів управління впливами (алгоритмічна чіткість).

4. Розробкою стандартів інформаційної взаємодії, орієнтованої на перетворення представленої інформації в інформованість контрагентів впливу (можливість автоматизації основних процесів обробки інформації).

5. Можливістю доступу до засобів надання інформації з багатьох робочих місць (відкритість).

Наведені принципи створення системи відбору необхідних для здійснення впливу інструментів впливу в процесі формування інформаційних впливів на контрагента є концептуальною основою наукових досліджень, що проведені автором.

На думку провідних вчених сьогодення інструменти візуалізації [2] повинні найкращим чином забезпечувати “перетворення” бажання у контрагентів впливу та формування у них такого відношення до певної інформованості, яка дозволить досягти поставлених цілей. Нам же необхідно визначити, яка інформація дозволить сформулювати таке відношення та представити її у вигляді найбільш впливового інформаційного представлення. Але в зв'язку з існуванням трьох наведених вище досить складних задач інформаційного впливу (ідентифікації потрібного відношення до отриманої інформації у контрагентів впливу, визначення способів впливу на контрагентів впливу, наповнення інформаційного представлення потрібною інформацією) представимо методику впливу у вигляді структури (рис.1).

Виходячи з схеми (рис.1) в задачі створення інструментів управління інформованістю і впливами можна виділити дві основні частини: створення інструментів визначення інформованості контрагента впливу, а також створення інструментів інформаційної дії на нього. Об'єднує ці інструменти інформаційна технологія супроводження процесів впливу на контрагента впливу.

За науково-методологічний базис для вирішення першої частини проблематики пропонується взяти теорію несилової взаємодії [1], тому що вона в математичній формі досить чітко дозволяє визначити необхідні зміни в відношенні до категорій впливу (зміну відношення до дійсності) у контрагентів впливу. Для цього необхідно стандартизувати бачення різноманітних компонентів впливу, і особливо, їх взаємозв'язок з баченнями сторони, що впливає, того результату, який заданий цілями цього впливу. Інструменти

інформаційної дії на контрагентів впливу включатимуть в себе способи отримання необхідної інформації та наповнення цією інформацією форм впливу. Вирішення цих задач дозволить досягти мети роботи – ефективно управляти інформованістю (впливом) через засоби інформаційної дії.

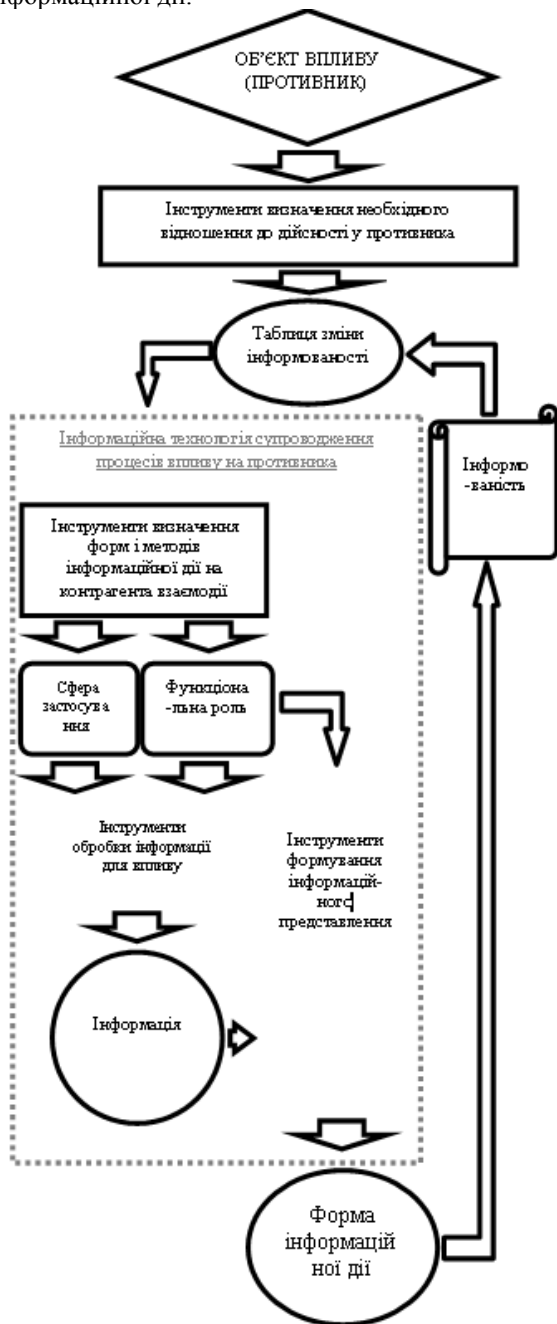


Рис.1 Схема зв'язку між інструментами інформаційної взаємодії у сфері

Її реалізація потребує визначити:

1. Як і яка інформованість (відношення до дійсності) позитивно вплине на результати інформаційного впливу;

Література

1. Тесля Ю. М. Введение в информатику Природы / Юрий Тесля / - Киев: Маклаут, 2010.- 256с. 2. Єгорченков О. В. Вплив інструментів візуалізації інформації на хід реалізації проектів / О. В. Єгорченков, Н. Ю. Єгорченкова,

2. Які інформаційні дії необхідні, щоб сформувані це відношення до дійсності.

Рішенням цих питань буде присвячена подальша робота автора.

Висновки й перспективи подальших досліджень

Як забезпечити ефективну інформаційну дію на широкі верстви населення, дію, яка по результатам буде прирівнюватися до виграшу в війні? Це питання має і практичне значення. Адже за період проведення антитерористичної операції (АТО) на населення сходу України постійно здійснюється цілеспрямований інформаційний вплив, який направлений на знищення суверенітету України. Як відновити позитивне відношення населення цього регіону до України, як їхньої Батьківщини, Європейської країни? Автори пропонують в якості науково-методичного базису такого потрібного інформаційного впливу використати теорію несилової взаємодії [1]. Теорія дає математичний інструментарій для визначення найбільш ефективних способів управління інформаційним супроводженням в процесах підготовки та проведення військових дій [4]. Для створення такого базису пропонується:

1. Представити в поняттях теорії несилової взаємодії атрибути "м'якої сили". Основним таким поняттям є поняття інтроформації. Під **інтроформацією** розуміється внутрішня організація взаємодіючих суб'єктів, яка формує їх відношення до дійсності та проявляється в їх діях. Щоб досягти необхідних дій контрагенту взаємодії необхідно спочатку змінити його відношення до дійсності. А це досягається зміною інтроформації. В свою чергу для зміни інтроформації необхідно щоб на контрагента здійснювались інформаційні дії дружніх контрагентів (з таким же або близьким відношенням до дійсності), направлені на потрібні зміни. Не дружніх, направлені на протилежні зміни.

Яка мета всього цього? Звичайно:

1. Контролювати інформаційний простір, щоб ми могли використовувати його, захищаючи при цьому наші військові інформаційні функції від ворожих дій (контрінформованість);
2. Використовувати контроль за інформацією для ведення інформаційних атак на ворога;
3. Підвищити загальну ефективність збройних сил за допомогою повсюдного використання військових інформаційних функцій.

Можна бути впевненим, що найближчими роками на цій базі буде досягнуто вагомих результатів у дослідженні спеціальних інформаційних операцій, передусім у напрямі захисту від них.

Н. О. Чорна // Управління розвитком складних систем. - 2014. - Вип. 19. - С. 27-33. 3. Тесля Ю. М., Кубявка Л. Б., Миколенко А. О., Кубявка М. Б. / Використання технологій інформаційного впливу під час підготовки та ведення

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ОПРЕДЕЛЕНИЯ НЕОБХОДИМО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ПРОТИВНИКА

Николай Богданович Кубявка

Любовь Богдановна Кубявка (канд. техн. наук, доцент)

Киевский национальный университет имени Тараса Шевченка, Киев, Украина

Целью исследования является создание научно-обоснованных методов управления информационными воздействиями, которые можно было бы применить в управлении информационным сопровождением в процессах подготовки и проведения военных действий. Основная идея этого исследования – обосновать и формально представить такие научно-методологические инструменты управления воздействиями, которые обеспечат значительное улучшение путей подготовки и проведения операций по информационному воздействию на противника, и осуществления контрмер, будут максимально информативно понятны, простые, результативные и минимально затратные. Поэтому есть необходимость рассмотрения вопроса управления информацией не с позиций максимального информирования контрагентов воздействия, а с позиций нужного информационного воздействия на них. При этом нужно учесть не только средства получения информации, но и специфику методов предоставления информации, ориентированных на информационное воздействие на противника. Учитывая выше сказанное, предлагается новый подход к процессам определения необходимого для эффективного управления информированностью информационного воздействия, что формирует новое отношение (мировоззрение) у контрагента взаимодействия. В его основе лежит применение инструментов теории несиловых взаимодействий, которые дают математический инструментарий для определения наиболее эффективных способов управления информационным сопровождением в процессах подготовки и проведения военных действий.

Ключевые слова: управление информационным влиянием; информационные операции; теория несиловых взаимодействий.

CONCEPTUAL MODEL FOR DEFINING THE NECESSARY INFORMATION IMPACT ON THE ENEMY

Mykola B. Kubiavka

Liubov B. Kubiavka (Candidate of Technical Sciences, Associate Professor)

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

The study aims to create evidence-based information management impacts that could be used in the management information support in the preparation and conduct of operations. The main idea of this research - to substantiate and formally submit such scientific and methodological tools of influence that will provide significant improvement through training and information operations impact on the enemy, the implementation of countermeasures will be most informative and clear, simple, effective and minimally costly. Therefore, there is need to consider the management information is not from the point of maximum exposure informing contractors and from the standpoint of information necessary action on them. It should take into account not only the means of obtaining information, but also the specific methods of information-oriented information to enemy action. Considering the above mentioned proposed a new approach to determining the processes necessary for the effective management of information influence awareness, shaping new attitude (ideology) in counterparty interaction. It is based on the theory of non-forcible use of tools of interaction that allows mathematical tools to identify the most effective ways to manage information support in the preparation and conduct of operations.

Keywords: management information actions; information operations; theory of non-coercive interaction.

References

1. Teslya Y. (2010), Introduction to Informatics Nature. [Vvedenie v informatiku Prirody], Kyiv: Maklout, 256p.
2. Yehorchenkov A., Yehorchenkova N., Chorna N. (2014) The impact of information visualization tools for the implementation of projects. [Vpliv instrumentiv vizualizacii informacii na hid realizacii proektiv], Managing the development of complex systems, No.19, pp. 27-33.
3. Teslya Y., Kubyavka L., Mikolenko A., Kubyavka M. (2014), Interactive discourse in the context of information security. [Vykorystannia tekhnolohii informatsiinoho vplyvu pid chas pidhotovky ta vedennia boiovykh dii], No. 2 (20), pp. 147-152.
4. Kubyavka M., Kubyavka L., Teslya Y. (2015), The possibilities of the theory of non-forcible influence in the military counter-intelligence. [Mozhlyvosti zastosuvannia teorii nesyloвого vplyvu v viiskovii kontrrozvidtsi], Scientific Journal "ScienceRise", No.2, 1(7), p. 18-22.

Отримано: 31.05.2016 року.

МАТЕМАТИЧНА МОДЕЛЬ СИСТЕМИ ФАЗОВОЇ АВТОПІДСТРОЙКИ ЧАСТОТИ З ЦИФРОВИМ ФАЗОВИМ ДЕТЕКТОРОМ З ПРИСТРОЄМ ФОРМУВАННЯ НЕУЗГОДЖЕНОСТІ ТА ГОТОВНОСТІ СИГНАЛІВ

Системи фазового автопідстроювання частоти (ФАПЧ) широко використовуються у сучасних системах мобільного, супутникового, та транкінгового зв'язку, а також в перспективних військових радіотехнічних комплексах різного призначення. Показники якості систем ФАПЧ, значною мірою визначають ефективність та якість зв'язку. У статті розглянуто функціональну схему системи фазового автопідстроювання частоти з цифровим фазовим детектором з пристроєм незгодженості та готовності сигналів. Отримано математичну модель об'єкту управління системи фазового автопідстроювання частоти, на основі якої розроблена структурна схема системи. Проведено аналіз та розглянута можливість побудови системи ФАПЧ з цифровим фазовим детектором з пристроєм незгодженості та готовності сигналів за допомогою методики складання різницевих рівнянь. Представлена модель проаналізована на наявність помилок та стійкості системи. Представлені результати дозволяють покращити динамічні характеристики систем фазового автопідстроювання частоти в схемах синхронізації засобів зв'язку.

Ключові слова: система фазового автопідстроювання частоти (ФАПЧ); математична модель.

Вступ

Постановка проблеми. Система фазового автопідстроювання частоти (ФАПЧ) є багатофункціональною системою, що використовується для частотної синхронізації, ущільнення і розподілу каналів в системах зв'язку, множення і перетворення частоти, яка підлаштовує фазу керованого генератора відповідно до значення фази опорного сигналу [1].

Останнім часом набуває все більшої актуальності використання у системах мобільного, супутникового, та транкінгового зв'язку, зокрема у військовій техніці, що використовувалися під час проведення АТО (повітряні сили, військово-морські сили) цифрових систем ФАПЧ, відомих виробників Analog Devices, Texas Instruments, Motorola, Gran-Jansen AS [9], в якості синтезаторів частот, ЦАП, в схемах відновлення несучої в передавачах і приймачах, в системах передачі та комутації з імпульсно-кодуючою модуляцією [3-5], а також для синхронізації в цифрових мережах.

Аналіз останніх досліджень і публікацій. Систем фазового автопідстроювання частоти ФАПЧ присвячена велика кількість робіт [1-6]. У роботах [2-5] розглянуті системи фазового автопідстроювання ФАПЧ, які є основним елементом систем синхронізації, і методом математичного моделювання в інтерактивній системі MATLAB досліджені процеси в системах ФАПЧ.

Система ФАПЧ визначає точність і швидкодію всієї системи синхронізації. Тому необхідно покращувати динамічні характеристики систем ФАПЧ, підвищувати основні показники якості цих систем - їх динамічну точність та швидкодію, ефективне і практичне підвищення яких є

неможливим без створення адекватної математичної моделі.

Метою роботи є створення математичної моделі системи ФАПЧ, яка дозволить покращити динамічні характеристики систем фазового автопідстроювання частоти в радіотехнічних засобах спеціального призначення.

Викладення основного матеріалу дослідження

Різницеві рівняння системи ФАПЧ

Розглянемо структурну схему класичної системи ФАПЧ, яка представлена на рис.1

Введемо наступні позначення $x(t)$ - сигнал опорного генератора системи ФАПЧ; $y(t)$ - вихідний сигнал перебудованого генератора системи ФАПЧ.

$$x(t) = A_{\text{опорн.г.}} \cos(\omega_{\text{опорн.г.}} t + \varphi_{\text{опорн.г.}}) \quad (1)$$

$$y(t) = A_{\text{пер.г.}} \cos(\omega_{\text{пер.г.}} t + \varphi_{\text{пер.г.}}) \quad (2)$$

де $A_{\text{опорн.г.}}$, $A_{\text{пер.г.}}$ - амплітуди коливань генераторів;

$\omega_{\text{пер.г.}}$, $\omega_{\text{опорн.г.}}$ - циклічні частоти цих коливань;

$\varphi_{\text{опорн.г.}}$, $\varphi_{\text{пер.г.}}$ - їх початкові фази.

При складанні математичної моделі рахуємо, що дільник частоти має фіксований коефіцієнт ділення - N_d . Сигнал з його виходу:

$$y_N(t) = A_{\text{діл.}} \cos\left(\frac{\omega_{\text{пер.г.}}}{N_d} t + \varphi_{\text{пер.г.}}\right) \quad (3)$$

Фазовий детектор (ФД) порівнює повні фази сигналу опорного генератора $x(t)$ і сигналу з виходу дільника частоти $y_N(t)$, $\varepsilon(t)$ - сигнал помилки фазового детектора. Фільтр нижніх частот (ФНЧ) перетворює сигнал помилки фазового детектора в керуючі напруги $U_{пер.г.}(t)$ перебудованого генератора.

Повну фазу коливань опорного генератора $\theta_{опор.г.}(t)$ і повну фазу коливань з виходу перебудованого генератора $\theta_{пер.г.}(t)$ визначимо співвідношенням:

$$\theta_{опор.г.}(t) = (\omega_{опор.г.} t + \varphi_{опор.г.}), \quad (4)$$

$$\theta_{пер.г.}(t) = \left(\frac{\omega_{пер.г.}}{N_d} t + \varphi_{пер.г.} \right). \quad (5)$$

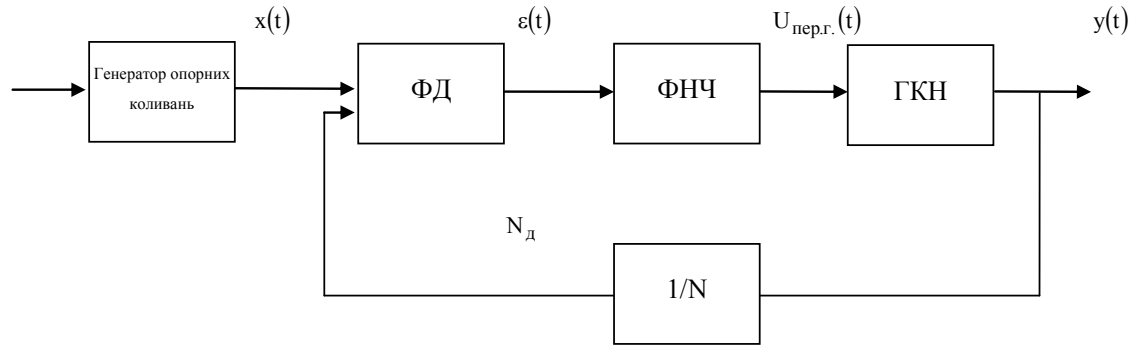


Рис. 1. Класична система ФАПЧ

На виході фазового детектора формується сигнал який визначається різницею фаз $\theta_{опор.г.}(t)$ і $\theta_{пер.г.}(t)$.

$$\varphi(t) = (\theta_{опор.г.}(t) - \theta_{пер.г.}(t)), \quad (6)$$

З врахуванням (4) і (5) отримаємо:

$$\varphi(t) = \left(\omega_{опор.г.} - \frac{\omega_{пер.г.}}{N_d} \right) t + \varphi_{поч.}, \quad (7)$$

$$\text{де } \varphi_{поч.} = (\varphi_{опор.г.} - \varphi_{пер.г.}). \quad (8)$$

Сигнал на виході фазового детектора представимо у вигляді:

$$\varepsilon(t) = F_{ФД}[\varphi(t)] \quad (9)$$

У виразі (9) $F_{ФД}[\varphi(t)]$ - передаточна функція фазового детектора. Якщо значення різниці повних фаз сигналу опорного генератора і сигналу перебудованого генератора знаходиться в діапазоні $[-2\pi, \dots, 2\pi]$, то передаточну функцію фазового детектору можна рахувати лінійною з коефіцієнтом передачі $K_{ФД}$.

З урахуванням (7-9) сигнал помилки $\varepsilon(t)$ запишемо у вигляді:

$$\varepsilon(t) = K_{ФД} \left[\left(\omega_{опор.г.} - \frac{\omega_{пер.г.}}{N_d} \right) t - \varphi_{поч.} \right]. \quad (10)$$

Коефіцієнт передачі фазового детектора визначається співвідношенням:

$$\frac{d\varphi}{dt} = \omega_{опор.г.} - \omega_{пер.г.} - K_{ФД} K_{ПГ} \int_0^t h_{ФНЧ}(t - \tau) \left[\left(\omega_{опор.г.} - \frac{\omega_{пер.г.}}{N_{д\ell}} \right) t - \varphi_{поч.} \right] dt. \quad (16)$$

В режимі синхронізму різниця повних фаз сигналу опорного генератора і сигналу перебудованого генератора повинна дорівнювати нулю:

$$\varphi(t) = 0. \quad (17)$$

Припустимо, що $h_{ФНЧ}(t)$ - імпульсна характеристика фільтру нижніх частот, тоді керуючу напругу перебудованого генератора запишемо як:

$$U_{пер.г.}(t) = \int_0^t h_{ФНЧ}(t - \tau) \varepsilon(t) dt. \quad (12)$$

Частота коливань перебудованого генератора визначається його коефіцієнтом передачі $K_{ПГ}$ і керуючою напругою $U_{пер.г.}(t)$:

$$\omega_{пер.г.}(t) = \omega_0 + K_{ПГ} U_{пер.г.}(t), \quad (13)$$

де ω_0 - частота перебудованого генератора. Коефіцієнт передачі перебудованого генератора $K_{ПГ}$ визначимо аналогічно коефіцієнту $K_{ФД}$:

$$K_{ПГ} = \frac{d\omega_{пер.г.}}{dU_{пер.г.}}. \quad (14)$$

Різницеве рівняння системи ФАПЧ має вигляд:

$$\frac{d\varphi}{dt} = \frac{d\theta_{опор.г.}(t)}{dt} - \frac{d\theta_{пер.г.}(t)}{dt}, \quad (15)$$

або з урахуванням (7)-(14):

Робота системи ФАПЧ рахується задовільною, якщо:

$$|\varphi| \leq \varphi_{доп.}, \quad (18)$$

де $\varphi_{доп.}$ - мале допустиме значення. При цій умові різницеве рівняння системи ФАПЧ має вигляд:

$$\omega_{\text{опорн.г.}} - \omega_{\text{пер.г.}} - K_{\text{ФД}} K_{\text{ПГ}} \int_0^t h_{\text{ФНЧ}}(t - \tau) \left(\left[\omega_{\text{опорн.г.}} \frac{\omega_{\text{пер.г.}}}{N_{\text{д}}} \right] t - \varphi_{\text{поч.}} \right) dt = 0. \quad (19)$$

Математична модель цифрової системи ФАПЧ з цифровим фазовим детектором з пристроєм неузгодженості та готовності сигналів.

Цифрова система ФАПЧ складається з цифрового фазового детектора з пристроєм неузгодженості та готовності сигналів, цифрового

фільтра, інтегратора, цифрового перебудованого генератора рис. 2.

Відмінність від класичної схеми полягає в застосуванні цифрового фазового детектора з пристроєм неузгодженості та готовності сигналів, який складається з дільника частоти, фазового компаратора та пристрою неузгодженості та готовності сигналів.

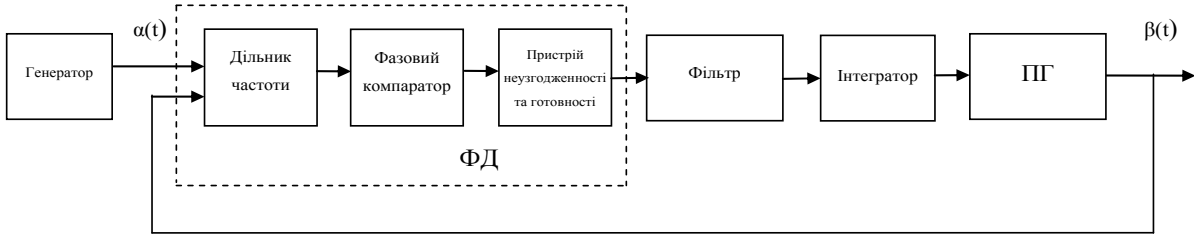


Рис. 2. Цифрова система ФАПЧ

Частота сигналу з виходу дільника частоти визначається співвідношенням

$$f[n] = \frac{1}{t_n - t_{n-1}}, \quad (20)$$

де t_n і t_{n-1} - моменти часу, які відповідають додатнім або від'ємним фронтам вихідного сигналу. В режимі синхронізму частота сигналу дільника частоти близька до частоти сигналу опорного генератора $f_{\text{опорн.г.}}$. Вважаючи, що

$$t_n = n f_{\text{опорн.г.}} + \Delta t_n \quad \text{і} \quad t_{n+1} = (n+1) f_{\text{опорн.г.}} + \Delta t_{n+1}, \text{ отримуємо}$$

$$f_{\text{д}}[n] = \frac{1}{f_{\text{опорн.г.}} + \Delta t_n - t_{n-1}}. \quad (21)$$

Знаючи частоту опорного генератора $f_{\text{опорн.г.}}[n]$, вираз для частоти сигналу дільника частоти можна представити у вигляді

$$f_{\text{д}}[n] = \frac{f_{\text{опорн.г.}}[n]}{N_{\text{д}}}. \quad (22)$$

Цифровий фазовий детектор відслідковує різницю фаз між додатними і від'ємними фронтами сигналів, отриманих на його вході. Тому, Δt_n і Δt_{n-1} потрібно розглядати як інтервали часу між додатними і від'ємними фронтами сигналів в моменти часу $(n) f_{\text{опорн.г.}}$ і $(n+1) f_{\text{опорн.г.}}$.

На вхід фазового компаратора цифрового фазового детектора приходять сигнали опорного генератора та перебудованого генератора з фазою $\omega_{\text{дл}}[n]$ і $\omega_{\text{опорн.г.}}[n]$

$$\omega_{\text{ФД}}[n] = \omega_{\text{опорн.г.}}[n] - \omega_{\text{пер.г.}}[n], \quad (23)$$

Із співвідношень (21-23) отримаємо

$$\omega_{\text{ФД}}[n] = 2\pi \frac{\Delta t_n}{T_{\text{опорн.г.}}}, \quad (24)$$

Пристрій неузгодженості та готовності сигналів вираховує фазову неузгодженість та формує цифровий код $N[n]$, пропорційний $\omega_{\text{ФД}}[n-1]$

$$N[n] = K_{\text{ФД}} \omega_{\text{ФД}}[n-1] \quad (25)$$

Коефіцієнт пропорційності $K_{\text{ФД}}$ (коефіцієнт передачі або підсилення фазового детектора) залежить від схематехнічної реалізації фазового детектора і властивостей фазового компаратора.

Цифровий код, який пропорційний фазовій помилці, поступає на цифровий фільтр (рекурсивний фільтр). Рівняння для такого фільтру має вигляд:

$$y(n) = -a_1 y(n-1) + a_0 y(n-2) + b_2 x(n) + b_1 x(n-1) + b_0 x(n-2). \quad (26)$$

Цифровий перебудований генератор являє собою генератор із змінним цифровим кодом, [7-10]. Фаза коливань $\omega_{\text{ПГ}}[n]$ генератора представлена, як сума значень фази коливань $\omega_{\text{ПГ}}[n+1]$ і додаткової величини $K_{\text{ПГ}} K_{\text{Ф}}[n]$

$$\omega_{\text{ПГ}}[n] = \omega_{\text{ПГ}}[n+1] + K_{\text{ПГ}} K_{\text{Ф}}[n], \quad (27)$$

Коефіцієнт $K_{\text{ПГ}}$ визначається виразом

$$K_{\text{ПГ}} = \frac{1}{\Delta T_{\text{ПГ}}}. \quad (28)$$

де $\Delta T_{\text{ПГ}}$ - затримка в кільцевому генераторі при зміні цифрового коду на одиницю молодшого розряду.

Враховуючи (23)-(28), отримаємо систему лінійних рівнянь цифрової системи ФАПЧ.

$$\begin{cases} \omega_{\PhiД} [n] = \omega_{\text{опорн.г}} [n] - \omega_{\text{діл.}} [n], \\ N_{\text{ПР}} [n] = K_{\PhiД} \omega_{\PhiД} [n - 1], \\ N_{\Phi} [n] = a_0 N_{\text{ПГ}} [n] + a_1 N_{\text{ПР}} [n - 1], \\ \omega_{\text{ПГ}} [n] = \omega_{\text{ПГ}} [n + 1] + K_{\text{ПГ}} K_{\Phi} [n], \\ \omega_{\text{д}} [n] = \frac{\Phi_{\text{ПГ}}}{N_{\text{д}}} \end{cases} \quad (29)$$

В режимі синхронізму $\omega_{\PhiД} [n] = 0$. В реальних цифрових системах ФАПЧ $\omega_{\PhiД} [n]$ повинна задовольняти умові:

$$\omega_{\PhiД} [n] \leq \omega_{\text{доп}}. \quad (30)$$

Передаточна характеристика цифрової системи ФАПЧ

Використовуючи параметри для опису класичної системи ФАПЧ можна записати передаточну функцію системи ФАПЧ з розімкнутою петлею зворотного зв'язку у вигляді

$$H(s) = \frac{K_{\text{ГКН}} K_{\PhiД} H_{\text{ФНЧ}}(s)}{N_s}, \quad (31)$$

де $H_{\text{ФНЧ}}(s)$ - передаточна функція фільтру. Тоді передаточна функція класичної системи ФАПЧ з замкнутою петлею зворотного зв'язку має вигляд

$$H_{\text{ФАПЧ}}(s) = \frac{H(s)}{1 + H(s)}, \quad (32)$$

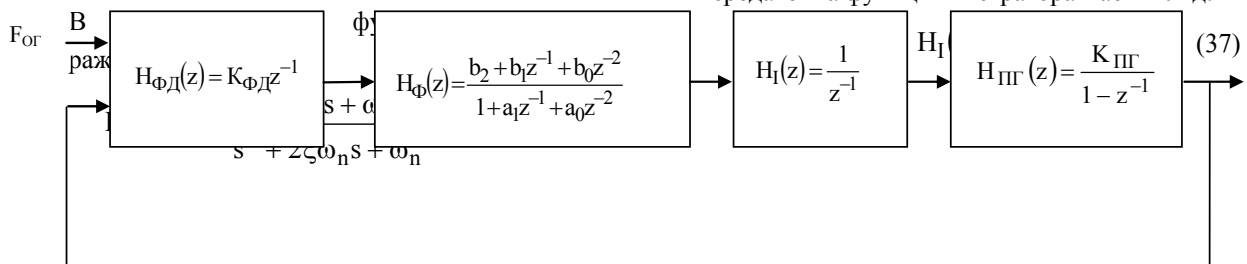


Рис.3. Модель цифрової системи ФАПЧ

Таким чином з урахуванням (34-37) цифрову систему ФАПЧ подано у вигляді моделі, та складено передаточну функцію системи ФАПЧ:

$$H_{\text{ФАПЧ}}(z) = \frac{z^{-1} - K_{\PhiД} K_i K_{\text{ПГ}} K_{\text{ФНЧ}}(z)}{(1 - z^{-1}) + z^{-1} K_{\PhiД} K_i K_{\text{ПГ}} K_{\text{ФНЧ}}(z)}. \quad (38)$$

Помилка слідкування цифрової ФАПЧ

При аналізі властивостей системи розглянемо передаточну характеристику типу

$$H_{\text{п}}(s) = 1 - H_{\text{ФАПЧ}}(s) \quad (39)$$

яка визначає відносну помилку встановлення фази вихідного сигналу системи ФАПЧ (помилку слідкування)

$$\frac{\Phi_{\text{вх}}(s) - \Phi_{\text{вих}}(s)}{\Phi_{\text{вх}}(s)}, \quad (40)$$

Помилка слідкування системи ФАПЧ визначається відношенням

$$\theta_{\text{пом}} = \frac{\Delta\Phi}{s} H_{\text{пом}}(s). \quad (41)$$

де ω_n власна частота, а ξ - коефіцієнт згасання системи ФАПЧ.

За аналогією з (31)-(33) отримаємо вираз для передаточної характеристики цифрової системи ФАПЧ. Запишемо передаточні функції всіх блоків, які входять в склад цифрової системи ФАПЧ (рис.3). Передаточна функція цифрового перебудованого генератора і фазового детектора мають вигляд:

$$H_{\text{ПГ}}(z) = \frac{K_{\text{ПГ}}}{1 - z^{-1}}, \quad (34)$$

$$H_{\PhiД}(z) = K_{\PhiД} z^{-1}. \quad (35)$$

Затримка на один такт означає, що в момент часу n фазового детектора буде результат порівняння фаз сигналу опорного генератора і сигналу перебудованого генератора в момент часу $n - 1$.

Відомо, що передаточна характеристика фазового детектора є лінійною, якщо різниця фаз сигналу опорного генератора і сигналу перебудованого генератора не перевищує 2π .

Передаточна функція фільтру має вигляд:

$$H_{\Phi}(z) = \frac{b_2 + b_1 z^{-1} + b_0 z^{-2}}{1 + a_1 z^{-1} + a_0 z^{-2}}. \quad (36)$$

Передаточна функція інтегратора має вигляд:

$$H_{\text{І}}(z) = \frac{1}{z^{-1}} \quad (37)$$

Знаючи відношення помилки системи ФАПЧ в s - області [1-3] знаходимо помилку слідкування для цифрової ФАПЧ.

Помилка слідкування цифрової системи ФАПЧ

$$\theta_{\text{пом.}}(z) = \Delta\Phi \left(\frac{z}{z-1} \right) H_{\text{пом.}}(z), \quad (42)$$

$$\theta_{\text{пом.}}(z) = \Delta\omega \left(\frac{T_d z}{z-1} \right) H_{\text{пом.}}(z). \quad (43)$$

Функція $H_{\text{п}}(z)$ має вигляд

$$H_{\text{пом.}} = \frac{\Phi_{\text{вх}}(z) - \Phi_{\text{вих}}(z)}{\Phi_{\text{вх}}(z)} = 1 - H_{\text{ФАПЧ}}(z), \quad (44)$$

Тоді помилка слідкування для цифрової системи ФАПЧ

$$H_{\text{пом.}}(z) = \frac{N_{\text{д}}(1 - z^{-1})}{N_{\text{д}}(1 - z^{-1}) + z^{-1} K_{\PhiД} K_{\text{ПГ}} K_i K_{\text{ФНЧ}}(z)}. \quad (45)$$

Для чисельної оцінки слідкування системи ФАПЧ використовуємо граничне відношення

$$\lim_{k \rightarrow \infty} (kT) = \lim_{z \rightarrow 1} H_{\text{пом.}}(z). \quad (46)$$

де k - число тактів системи

Аналіз стійкості системи ФАПЧ

Для визначення області стійкості цифрової системи ФАПЧ використовуємо критерій Гурвіца [1]

Замкнута дискретна система стійка коли всі корні характеристичного рівняння передаточної функції лежать в межах круга одиничного радіусу. Характеристичне рівняння функції системи ФАПЧ представимо у вигляді:

$$D(z) = A_0 z^{-3} + A_1 z^{-2} + A_2 z^{-1} + A_3.$$

де $A_0 = -b_2 K_{ФД} K_{ПГ} + a_2 N_d$,

$$A_1 = -b_1 K_{ФД} K_{ПГ} + a_1 N_d - a_2 N_d,$$

$$A_2 = K_{ФД} K_{ПГ} - N_d - a_2 N_d,$$

$$A_3 = N_d.$$

Корні характеристичного рівняння знаходимо аналітично:

$$z_1 = \frac{-A_2 + \sqrt{A_2^2 - A_1 A_3}}{2A_1},$$

$$z_2 = \frac{-A_2 - \sqrt{A_2^2 - A_1 A_3}}{2A_1}.$$

Література

1. Системы фазовой автоподстройки частоты / В. В. Шахгильдян, А. А. Ляховкин, В. Л. Под ред. В. В. Шахгильдяна. М.: Связь, 1972. с.1-220.
 2. Системы фазовой синхронизации с элементами дискретизации / Под ред. В. В. Шахгильдяна. – М.: Радио и связь. – 1989. 3. Черных И. В. Моделирование электротехнических устройств в MATLAB, SimPowerSystems и Simulink. – М.: ДМК Пресс, СПб: Питер, 2008. 288 с. 4. Линдсей В. Л. Системы синхронизации в связи и управлении / В. Л. Линдсей. – Москва : – Советское радио, 1978. – 599 с.
 5. Карякин В. Л. Синтез оптимальных по быстродействию импульсных систем синхронизации / В. Л. Карякин // Оптимизация систем передачи информации по каналам связи : сб. науч. тр.; учеб. инт. тов. связи. – Ленинград : ЛЭИС, 1986. – С. 107-112.
 6. Нетудыхата Л. И., Стеклов В. К. Системы фазовой автоматической подстройки в устройствах связи. – Київ: Техніка, 2003. – 368 с. 7. Chao-Ching Hung and Shen-Iuan Liu, “A 40-GHz Fast-Locked All-Digital Phase-Locked Loop Using a Modified Bang-Bang Algorithm” IEEE Transactions on Circuits and Systems-II, vol.58, no.6, pp.

Якщо виконується умова, коли корні характеристичного рівняння по модулю будуть менше одиниці, то система ФАПЧ стійка.

$$\left| \frac{-A_2}{2A_1} \right| < 1,$$

$$\left| \frac{A_2^2 - A_1 A_3}{4A_1^2} \right| < 1.$$

Висновки й перспективи подальших досліджень

Таким чином, враховуючи ідею створення цифрової системи фазової автопідстройки частоти з цифровим фазовим детектором з пристроєм неузгодженості та готовності сигналів:

1. Отримано математичну модель ФАПЧ, на основі якої розроблена структурна схема цифрової системи ФАПЧ.

2. Проведено аналіз та розглянута можливість побудови цифрової системи ФАПЧ з цифровим фазовим детектором з пристроєм неузгодженості та готовності сигналів за допомогою методики складання різницьових рівнянь.

Виведені співвідношення дозволяють проводити моделювання цифрових систем ФАПЧ.

321-325, June 2011. 8. Davide Tasca, Marco Zanuso, Giovanni Marzin, Salvatore Levantino, Carlo Samori and Andrea L. Lacaita, “A 2.9-4.0-GHz Fractional-N Digital PLL With Bang-Bang Phase Detector and 560-fsrms Integrated Jitter at 4.5-mW Power” IEEE Journal of Solid-State Circuits, vol.46, no.12, pp. 2745-2758, Dec 2011. 9. Голуб В. Система ФАПЧ и ее применения // интернет-портал Рынок микроэлектроники, URL: http://www.chipnews.ru/html.cgi/arihiv/00_04/stat_2.htm. 10. J.P. Hein and J.W. Scott, z-Domain Model for Discrete-Time PLL's I IEEE Transactions on Circuits and Systems, 1988, Vol.35., No.3, pp. 1393-1397. 11. Eric. Drucker, “Model PLL Dynamics and Phase - Noise Performance” // Microwaves & RF, 2000, No.5. pp. 10-16. 12. B.P. Lathi, “Modem Digital and Analog Communication System”, 3rd Edition / Oxford University Press, New York, 1998. 13. A. Demir, “Phase noise and timing jitter in oscillators with colored-noise sources” // IEEE Transaction on Circuits and Systems-I, 2002, Vol. 49., No. 12. 14. Стеклов В. К., Скляренко С. Н., Костик Б. Я. Системы фазовой автоподстройки с дифференциальными связями. – Київ: Техніка, 2003. –328 с.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ФАЗОВОЙ АУТОПОДСТРОЙКИ ЧАСТОТЫ С ЦИФРОВЫМ ФАЗОВЫМ ДЕТЕКТОРОМ С УСТРОЙСТВОМ ФОРМИРОВАТЕЛЯ СИГНАЛОВ РАССОГЛАСОВАНИЯ И ГОТОВНОСТИ

Евгений Вицентович Лебедь

Военный институт телекоммуникаций и информатизации, Киев, Украина

Системы фазовой автоподстройки частоты (ФАПЧ) широко используются в современных системах мобильной, спутниковой, и транкинговой связи, а также в перспективных военных радиотехнических комплексах разного назначения. Показатели качества систем ФАПЧ, в значительной степени определяют эффективность и качество связи. В статье рассмотрена функциональная схема системы фазовой автоподстройки частоты с цифровым фазовым детектором с устройством

формирователя сигналов рассогласования и готовности. Получена математическая модель объекта управления системы фазовой автоподстройки частоты на основе, которой разработана структурная схема системы. Проведен анализ и рассмотрена возможность построения системы ФАПЧ с цифровым фазовым детектором с устройством формирователя сигналов рассогласования и готовности с помощью методики составления разностных уравнений. Представленная модель проанализирована на наличие ошибок и устойчивости системы. Представленные результаты позволяют улучшить динамические характеристики систем фазовой автоподстройки частоты в схемах синхронизации средств связи.

Ключевые слова: система фазовой автоподстройки частоты (ФАПЧ); математическая модель.

MATHEMATICAL MODEL THE SYSTEM PHASE - LOCKED LOOP (PLL) WITH A DIGITAL PHASE DETECTOR WITH THE DEVICE RESHAPER OF SIGNALS DISAGREEMENT AND READINESS

Yevhen V. Lebid

Military Institute of Telecommunications and Informatization, Kyiv, Ukraine

The system phase - locked loop (PLL) are widely used in the modern systems mobile, satellite, and trunking communication, and also in the perspective military radiotechnical complexes of the different setting (Air Force, Navy military) indexes quality the systems PLL, largely determine efficiency and quality of connection. In the article the functional diagram the system PLL is considered with a digital phase detector with the device reshaper signals of inconsistency and readiness. The mathematical model object of management the system PLL is got which the flow diagram of the system is worked out on the basis. An analysis is conducted and possibility of construction the digital system PLL is considered with a digital phase detector with the device reshaper signals of inconsistency and readiness by means of methodology drafting of difference equations. The presented model is analysed in the presence of errors and stability the system. The presented results allow improving dynamic descriptions the systems PLL in the charts synchronization of communication means.

Keywords: PLL system; mathematical model.

References

1. **Shahgil'djan A.A.**, Ljahovkin V.L. (1972), A phase-locked loop [*Sistemy fazovoy avtopodstrojki chastoty*], Svjaz', Moscow, 220 p.
2. **Shahgil'djan A.A.** (1989), A phase-synchronized with sampling elements. [*Sistemy fazovoi sinkhronizacii s elementami diskretizacii*], Moscow: Radio i sviaz.
3. **Chernykh I.V.** (2008), Simulation of electrical devices in MATLAB. [Modelirovanie elektrotekhnicheskikh ustroystv v MATLAB], SimPowerSystems and Simulink, DMK Press, SPb: Piter, 288 p.
4. **Lindsei V.L.** (1978), Synchronization systems in communication and management. [*Sistemy sinkhronizacii v sviazi i upravlenii*], Moscow: Sovetskoe radio, 599 p.
5. **Kariakin V.L.** (1986), Synthesis-optimal pulse synchronization systems. [*Sintez optimalnykh po bystrodeistviuu impulsnykh sistem sinkhronizacii*], Optimizatsiia sistem peredachi informacii po kanalarnykh sviazi: sb. nauch. tr.; ucheb. in-tov. Sviaz, Leningrad: LEIS, pp. 107-112.
6. **Netudykhata L.L.**, Steklov V.K. (2003), The phase locked loop in communication devices. [*Sistemy fazovoi avtomaticheskoi podstroiki v ustroystvakh sviazi*], Kyiv: Tekhnika, 368 p.
7. **Chao-Ching Hung** and Shen-Iuan Liu, "A 40-GHz Fast-Locked All-Digital Phase-Locked Loop Using a Modified Bang-Bang Algorithm" IEEE Transactions on Circuits and Systems-II, vol.58, no.6, pp. 321-325, June 2011.
8. **Davide Tasca**, Marco Zanusso, Giovanni Marzin, Salvatore Levantino, Carlo Samori and Andrea L. Lacaita, "A 2.9-4.0-GHz Fractional-N Digital PLL With Bang-Bang Phase Detector and 560-fsrms Integrated Jitter at 4.5-mW Power" IEEE Journal of Solid-State Circuits, vol.46, no.12, pp. 2745-2758, Dec 2011.
9. **Golub V.** PLL and its application system. [*Sistema FAPCh i ee primeneniia*], Internet portal Market Microelectronics, URL: http://www.chipnews.ru/html.cgi/arhiv/00_04/stat_2.htm.
10. **J.P. Hein** and J.W. Scott (1988), z-Domain Model for Discrete-Time PLL's I IEEE Transactions on Circuits and Systems, , Vol.35., No.3, pp. 1393-1397.
11. **Eric. Drucker** (2000), "Model PLL Dynamics and Phase - Noise Performance", Microwaves & RF, No.5. pp. 10-16.
12. **Lathi B.P.** (1998), "Modem Digital and Analog Communication System", 3rd Edition, Oxford University Press, New York.
13. **A. Demir** (2002), "Phase noise and timing jitter in oscillators with colored-noise sources", IEEE Transaction on Circuits and Systems-I, Vol. 49, No.12.
14. **Steklov V.K.**, Skliarenko S.N., Kostik B.I. (2003), Phase Locked with differential constraints. [*Sistemy fazovoi avtopodstroiki s differentsialnymi sviaziami*], Kyiv: Tekhnika, 328 p.

Отримано: 05.08.2016 року.

*Олег Миколайович Маковецький
Ірина Робертівна Мальцева
Наталія Анатоліївна Паламарчук
Юлія Олександрівна Черниш
Олександр Вікторович Шемендюк*

Військовий інститут телекомунікацій та інформатизації, Київ, Україна

ПІДХОДИ ДО УДОСКОНАЛЕННЯ МЕТОДИКИ ОЦІНКИ ЕФЕКТИВНОСТІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

В статті розглядається обґрунтування і вибір варіантів побудови, оптимізації і оперативного управління функціонуванням систем захисту інформації в автоматизованих системах, а також питання оцінки ефективності системи захисту інформації. Розглянуто та вивчено узагальнену модель системи, яка дає можливість чіткого описання та класифікації ресурсів, що захищаються, та загроз, що виникають перед цими ресурсами та безпосередньо самих механізмів захисту.

Запропоновано удосконалення методики оцінки ефективності систем захисту інформації на різних етапах (класифікація ресурсів, що захищаються та визначення їх цінності; ідентифікація, класифікація та оцінка загроз; визначення механізмів захисту, повноти їх реалізації та міри послаблення загрози; визначення оцінки ефективності системи захисту, підготовка експертного висновку) з повним перекриттям загроз на основі врахування важливості ресурсів, що захищаються, де для кожного інформаційного ресурсу встановлюється відповідний рівень конфіденційності, цілісності, доступності і спостережності. Наведено оцінку ризиків для інформації в частині втрат, які може понести організація в різних варіантах реалізації механізмів захисту. Враховано важливість кожного ресурсу, що дозволяє зробити висновок про оптимальність використання коштів на систему захисту. Приведено можливість втрат без виконання певних вимог і відвернені втрат при їх виконанні.

***Ключові слова:** загрози інформації; система захисту інформації; оцінка ефективності комплексних систем захисту інформації; конфіденційність; цілісність; доступність; спостережність.*

Вступ

Постановка проблеми. Комплексна методика оцінки системи захисту інформації (СЗІ), в тому числі і комплексної системи захисту інформації (КСЗІ) необхідна для цілеспрямованого підвищення ефективності роботи і якості процесу її проектування. Крім того, існує певна залежність між мірами захисту і цінністю інформації, що захищається, тобто ефективність системи захисту, а отже і затрати на її побудову та утримання знаходяться в прямій залежності від значимості ресурсу, причому, залежність може бути не постійною.

Аналіз останніх досліджень і публікацій. Складними питаннями під час оцінки ефективності КСЗІ є:

- загалом, в реальних умовах, експерт має справу з неповною і нечіткою інформацією;
- розглядається не лише кількісний, а і якісний опис показників;
- набір факторів, як правило, досить великий, що викликає необхідність аналізу експертом великої кількості ситуацій;
- експерту завжди важко сформулювати свої знання у вигляді чітких правил і алгоритмів, легше поставити оцінку ніж описати як він до неї дійшов;
- система оцінки ефективності повинна пов'язуватись зі значимістю ресурсу, тобто ефективні міри захисту повинні бути не лише достатніми, але й не повинні бути надлишковими.

Крім того, провівши аналіз існуючих методик

оцінки ефективності СЗІ [2] слід зазначити, що на даному етапі не існує повноцінної методики, яка б враховувала:

- важливість ресурсів, що захищаються;
- інтенсивність та рівень (складність) загроз, що впливають на систему;
- зниження інтенсивності та рівня загрози системою захисту;
- сумарний рівень загрози, що впливає на систему з використанням системи захисту;
- можливість використання методики як в системах, що проектуються, так і в готових функціонуючих системах;
- можливість локалізації слабких місць системи, а також дослідження зміни рівня захисту від зміни певних показників системи.

Метою статті є оцінка обґрунтування і вибір найкращих варіантів побудови, оптимізації і оперативного управління функціонуванням СЗІ для забезпечення оптимального захисту ресурсів організації при прийнятних затратах.

Побудова методики оцінки комплексної системи захисту інформації (в тому числі оцінки захищеності АС) перш за все потребує вивчення узагальненої моделі такої системи, яка б давала можливість чітко описати та класифікувати ресурси, що захищаються, та загрози, що виникають перед цими ресурсами та безпосередньо самі механізми захисту.

Найбільший інтерес для нас представляє "загальна модель системи захисту інформації з повним перекриттям" представлена на рис. 1 [3].

Тут кожній окремій загрозі t_i з області загроз T протиставляються механізми захисту КСЗІ m_k , відповідно, що стоять на шляху до атакованого ресурсу v_j . Проходження через механізми захисту m_k системи захисту, знижує рівень цієї загрози, в результаті чого загроза стає або взагалі мізерною, або зниженою до такого рівня, на якому вже не здатна нанести суттєвої шкоди.

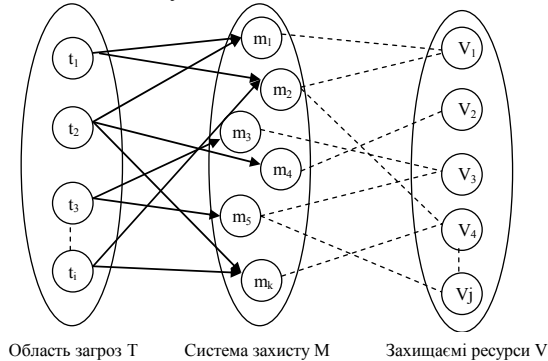


Рис. 1. Загальна типова модель процесу захисту інформації з повним перекриттям загроз

Виклад основного матеріалу дослідження

Методика оцінки ефективності функціонування системи ЗІ з повним перекриттям загроз передбачає наступні етапи:

1. Класифікація ресурсів, що захищаються та визначення їх цінності.
2. Ідентифікація, класифікація та оцінка загроз.
3. Визначення механізмів захисту, повноти їх реалізації та міри послаблення загрози.
4. Визначення оцінки ефективності системи захисту, підготовка експертного висновку.

Застосування критерію ризику, на сьогоднішній день є одним з найбільш розповсюджених критеріїв для оцінки систем захисту [1, 2]:

$$R(p) = \sum_{i=1}^w C_i p_i (1 - q_i)$$

де C_i – цінність ресурсу (наслідки втрати інформації) в разі здійснення загрози i -го виду;

p_i – ймовірність появи i -ої загрози;

q_i – ймовірність відбиття i -ої загрози;

w – кількість загроз, що діють на систему.

Перший етап. Класифікація ресурсів визначається, як правило, в документі під назвою

“Політика інформаційної безпеки”. Для кожного інформаційного ресурсу встановлюється відповідний рівень конфіденційності, цілісності, доступності і спостережності по багатобальній калі, наприклад, п’ятибальній. Рівень конфіденційності визначається ступенем важливості ресурсу і наслідками розголошення відповідної інформації, рівень цілісності ресурсу – ступенем пошкодження, фінансових втрат і можливістю відновлення, рівень доступності ресурсу – значенням максимального часу, на протязі якого недоступність ресурсу не впливає негативно на діяльність організації, рівень спостережності – ступенем повноти, якості і контролю використання ресурсу з боку авторизованих користувачів.

Середньоарифметичне значення рівнів конфіденційності, цілісності, доступності і спостережності кожного ресурсу визначає важливість цього ресурсу (1).

$$V_i = \frac{K_i + C_i + D_i + S_i}{4} \tag{1}$$

де K_i – конфіденційність i -го ресурсу;

C_i – цілісність i -го ресурсу;

D_i – доступність i -го ресурсу;

S_i – спостережність i -го ресурсу.

Другий етап. Ідентифікація оцінки загроз і вразливостей полягає в послідовному виконанні наступних кроків:

1) Визначення загроз для ресурсів організації;

2) Визначення рівня реалізації загроз без використання механізмів захисту.

При цьому спочатку необхідно визначити потенційні загрози для кожного ресурсу, враховуючи місцезнаходження джерела загроз, природу його походження та характер прояву загрози. В цьому нам може допомогти модель загроз інформації, що обробляється в автоматизованій системі. Слід відмітити, що можуть використовуватись різні методи, в основу яких покладені експертні оцінки, статистичні дані і фактори, що впливають на рівні загроз і т.ін.

В табл. 1. приведені 7 рівнів реалізації загрози в залежності від їх можливої частоти (інтенсивності).

Таблиця 1

Рівні загрози			
Характеристика загрози	Бальна оцінка	Ймовірнісна оцінка	Частота загрози
зневажливо мала	1	0-0,05	Практично неможлива
дуже низька	2	0,05-0,2	2-3 рази на 5 років
низька	3	0,2-0,4	1 раз на рік
середня	4	0,4- 0,6	1 раз на півроку або рідше
висока	5	0,6- 0,8	1 раз на місяць або рідше
дуже висока	6	0,8- 0,95	декілька разів на місяць
найвища	7	0,95-1	декілька разів на день

Подібний підхід можна використати для визначення рівнів загрози виходячи зі ступеня їх складності. Або ж використавши комплексний показник, наприклад в табл. 2. представлені бальні

оцінки рівня загроз в залежності від п'яти рівнів частоти їх виникнення: раз на кілька років, раз на рік, кілька раз на рік, раз на місяць, раз на добу або частіше.

Таблиця 2

Оцінка рівня загрози

Рівень складності загрози	Частота виникнення загрози				
	Раз на кілька років або рідше	Раз на рік	Кілька раз на рік	Раз на місяць	Раз на добу або частіше
1	1	1	1	1-2	2-3
2	1	1	2	2-3	3-4
3	1	1-2	3	3-4	4-5
4	1-2	2-3	4	4-5	5-6
5	2-3	3-4	5	5-6	6-7
6	3-4	4-5	6	6-7	7
7	4-5	5-6	7	7	7

Якщо частота виникнення загрози на середньому рівні, то рівень реалізації загрози залишається початковим, тобто бальна оцінка загрози не змінюється. У випадку, коли загроза виникає частіше (рідше), оцінка збільшується (зменшується) на 1-2 бали.

Третій етап. Визначення механізмів захисту, що протидіють загрозі та входять до складу СЗІ. А також рівень, з яким механізми захисту зменшують загрозу, що діє на систему.

Для оцінки даного параметра механізмів захисту пропонується розглянути методику оцінки якості системи захисту інформації на основі матриці знань. Проведений аналіз існуючих способів і методів ЗІ дозволяє виділити основні показники блока НАПРЯМКИ (H_j) в процесі створення й оцінки системи захисту інформації, наприклад [2]:

H_1 – захист об'єктів корпоративних систем;

H_2 – захист процесів, процедур і програм обробки інформації;

H_3 – захист каналів зв'язку;

H_4 – придушення побічних електромагнітних випромінювань;

H_5 – керування системою захисту.

Кожний з показників блока “НАПРЯМКИ” повинен бути структурований у залежності від заданої глибини деталізації СЗІ.

Саме показники блока “НАПРЯМКИ” пропонується розглядати як механізми захисту, що протидіють загрозам. В разі, якщо загроза при дії на ресурс проходить через декілька механізмів захисту, то за остаточний рівень загрози слід приймати загрозу на виході механізму захисту, що найменше зменшує її дію.

Кожен з даних показників блока “НАПРЯМКИ” оцінюється за рядом показників “ОСНОВИ” на всіх “ЕТАПАХ” функціонування системи захисту.

Проведений аналіз основних підходів до створення СЗІ дозволяє виділити наступну групу показників блока ОСНОВИ (O_i):

O_1 – нормативно-правова і наукова база;

O_2 – структура і задачі органів;

O_3 – організаційні заходи і методи (політика безпеки);

O_4 – програмно-технічні способи і засоби.

Значення кожного з перерахованих показників блоку “ОСНОВИ” повинне бути деталізоване для конкретної інформаційної системи.

У даний час при побудові СЗІ розглядають різні етапи життєвого циклу системи. Усі вони досить ефективні і дозволяють вирішувати поставлені задачі. На основі проведеного аналізу пропонується розгляд відповідних показників блока ЕТАПИ (M_k) створення СЗІ, що підлягають оцінці. До них зазвичай відносять [2]:

M_1 – визначення інформації, що підлягає захисту;

M_2 – виявлення повного переліку потенційно-можливих загроз і каналів витоку інформації;

M_3 – проведення оцінки уразливості і ризиків інформації при наявній множині загроз і каналів витоку;

M_4 – визначення вимог до системи захисту;

M_5 – здійснення вибору засобів ЗІ і їхніх характеристик;

M_6 – впровадження й організація використання обраних заходів, способів і засобів захисту;

M_7 – здійснення контролю цілісності і керування системою захисту та інше.

Етапи, в разі такої необхідності, можуть бути розбиті на більш детальні пункти.

Структура моделі оцінки СЗІ полягає в логічному об'єднанні показників блоків “ОСНОВИ”, “НАПРЯМКИ” і “ЕТАПИ” у МАТРИЦЮ ОЦІНОК, що складається з K елементів (рис 2).

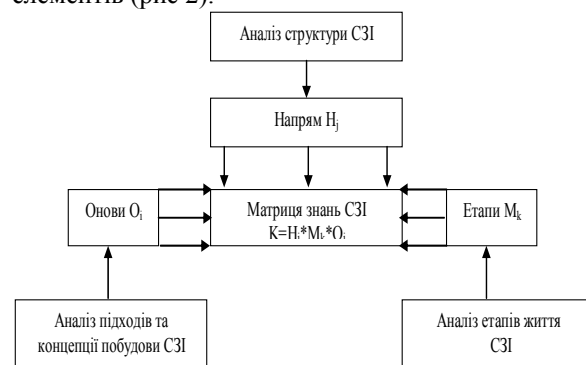


Рис. 2. Взаємозв'язок елементів матриці знань СЗІ

У загальному випадку кількість елементів “матриці” може бути визначена виразом:

$$K = O_i \cdot H_j \cdot M_k$$

На основі проведеного вище аналізу в типовому варіанті (за умови, що $O_i = 4, H_j = 5, M_k = 7$) загальна кількість елементів “матриці” складає:

$$K = 4 \cdot 5 \cdot 7 = 140$$

Показник рівня захисту СЗІ пропонується визначати методом експертних оцінок, використовуючи положення теорії нечіткої логіки і нечітких тверджень [2].

Оцінки можуть формуватися по різних групах елементів матриці, у залежності від цілей перевірки [4].

У нашому випадку доцільно розділити дану матрицю за показниками НАПРЯМКИ тобто оцінити ступінь зниження загрози кожним з механізмів захисту.

Отримавши оцінку ступеня зниження загрози механізмом захисту ми можемо визначити остаточний рівень загрози

$$D_k = Z_k - [\max(Z) * H_i] \quad (2)$$

де D_k – остаточний рівень загрози після проходження механізму захисту;

Z_k – рівень k-ї загрози до проходження через механізми захисту;

$\max(Z)$ – максимальний рівень загрози згідно обраної шкали оцінки;

H_i – рівень зниження загрози i-м механізмом захисту.

Четвертий етап. Визначення рівня ризику для ресурсів системи з урахуванням механізмів захисту та висновку про ефективність системи захисту.

Остаточний рівень ризиків визначається як добуток важливості ресурсу і рівня реалізації загрози (табл.3).

$$R_{nk} = V_n * D_k \quad (3)$$

де, R_{nk} – остаточний рівень ризику, що створюється k-ю загрозою для деякого ресурсу n після проходження механізмів захисту;

V_n – рівень важливості певного ресурсу n;

Таблиця 3

Рівні ризику

Важливість ресурсу	Рівень реалізації загрози						
	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21
4	4	8	12	16	20	24	28
5	5	10	15	20	25	30	35

Якщо значення ризику знаходяться в межах 1-4, при цьому припускається, що потенційні втрати мінімальні (до 10 %), вплив на діяльність організації практично відсутній, рівень ризику низький і задовольняє умовам нормального функціонування;

Якщо значення ризику знаходяться в межах 5-8, при цьому припускається, що потенційні втрати становлять до 20%, є невеликий негативний вплив на діяльність організації. Постає питання про необхідність проведення дій по керуванню даним ризиком.

В разі якщо значення ризику знаходяться в межах 9-35, існують серйозні негативні наслідки для організації, необхідно терміново почати відповідні дії по керуванню даним ризиком, удосконаленню системи захисту, зміни умов її функціонування.

Як логічне завершення оцінки ефективності виступає “Експертний висновок”. Зрозуміло, що він може бути оформлений в різноманітних варіаціях в залежності від того, яку інформацію хоче отримати для себе замовник. Окрім загальної оцінки, яка може виставлятися у будь якій зручній для експерта або замовника шкалі, та в разі негативних результатів висновку про необхідність доопрацювання системи захисту, вище розглянута

Література

1. **Богданов В. В.** Застосування критерію ризику для оцінки захищеності автоматизованої системи. – К.: Збірник доповідей та тез доповідей, V-та науково-технічна конференція ВІПІ НТУУ “КПІ”, 2010. с. 70-72.

методика дозволяє також, враховуючи важливість кожного ресурсу, зробити висновок про оптимальність використання коштів на систему захисту, не допускаючи не лише їх недостатності, а й надлишковості. Часто керівники відділу захисту інформації зустрічають непорозуміння з боку керівництва щодо виділення коштів на систему захисту.

Висновки й перспективи подальших досліджень

Вище описана методика дозволяє оцінити ризик для інформації без використання СЗІ, та відповідно втрати, які понесе організація в різних варіантах реалізації механізмів захисту, а отже і наглядно показати можливі втрати без виконання певних вимог і відверненні втрати при їх виконанні, тобто враховує, якою ціною досягається захист даної інформації. Крім того, використання матриці знань дозволяє обґрунтувати необхідність виділення коштів перед керівництвом на систему захисту, локалізувати місця в системі захисту, де вимоги виконані недостатньо, а де з надлишком, що дає можливість оптимально перерозподілити затрати на систему захисту між її елементами, а також розробити конкретний план заходів по усуненню недоліків СЗІ.

2. **Домарев В. В.** Безопасность информационных технологий. К.: 2002. с. 352. 3. **Романов О. І., Лівенцев С. П., Павлов І. М.** Математична модель захисту інформації в автоматизованих мережах

спеціального призначення. К.: Збірник наукових праць ВІТІ НТУУ “КПІ” № 5, 2004. с. 23–31. 4. Гайдук О. С. Методологія вибору раціонального варіанту системи захисту інформації на основі експертних оцінок. – Л.: Збірник тез доповідей підсумкової науково-практичної

конференції Всеукраїнського конкурсу студентських наукових робіт з природничих, технічних та гуманітарних наук у 2011/2012 навчальному році, галузь знань “Інформаційна безпека” 2012 с. 32.

ПОДХОДЫ К СОВЕРШЕНСТВОВАНИЮ МЕТОДИКИ ОЦЕНКИ ЭФФЕКТИВНОСТИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

*Олег Николаевич Маковецкий
Ирина Робертовна Мальцева
Наталья Анатольевна Паламарчук
Юлия Александровна Черныш
Александр Витальевич Шемендюк*

Военный институт телекоммуникаций и информатизации, Киев, Украина

В статье рассматривается обоснование и выбор вариантов построения, оптимизации и оперативного управления функционированием систем защиты информации в автоматизированных системах, а также вопросы оценки эффективности системы защиты информации. Рассмотрены и изучены обобщенную модель системы, которая дает возможность четкого описания и классификации ресурсов, защищаемых и угроз, возникающих перед этими ресурсами и непосредственно самих механизмов защиты.

Предложено усовершенствование методики оценки эффективности систем защиты информации на различных этапах (классификация ресурсов, защищаемых и определения их ценности; идентификация, классификация и оценка угроз, определение механизмов защиты, полноты их реализации и степени ослабления угрозы, определение оценки эффективности системы защиты, подготовка экспертного заключения) с полным перекрытием угроз, на основе учета важности защищаемым ресурсам, где для каждого информационного ресурса устанавливается соответствующий уровень конфиденциальности, целостности, доступности и наблюдаемости. Приведена оценка рисков для информации в части потерь, которые может понести организация в различных вариантах реализации механизмов защиты. Учтена важность каждого ресурса, что позволяет сделать вывод об оптимальности использования средств на систему защиты. Приведены возможности потерь без выполнения определенных требований и предотвращены потери при их выполнении.

Ключевые слова: угрозы информации; система защиты информации; оценка эффективности комплексных систем защиты информации; конфиденциальность; целостность; доступность; наблюдаемость.

APPROACH TO IMPROVING EFFICIENCY EVALUATION METHOD OF THE COMPLEX INFORMATION SECURITY

*Oleh M. Makovetskyi
Iryna R. Maltseva
Nataliia A. Palamarchuk
Yuliia O. Chernysh
Oleksandr V. Shemendiuk*

Military Institute of Telecommunications and Information, Kyiv, Ukraine

The article presents justification and list of choices of formation, optimization and operational management on information security systems in automated systems and performance evaluation of information security system. It was reviewed and examined the general system model that enables to clearly describe and classify protected resources and emerging threats.

It was recommended the information security systems methodology improvements on different stages (resources classification; identification, classification and assessment of threats; definition of security mechanism, the fullness of its accomplishments and solution to weakness a threat; definition the evaluation of security system, preparing of expert conclusion) with full threats overlapping based on consideration of the importance of the protected resources taking into account that for every information resource should be set up appropriate level of confidentiality, sustainability, availability and observability. It was introduced the risk assessment for information concerning costs incurred using different variant of security mechanisms. It was taking into account the importance of each resource that enables to infer about appropriation of financial resources on security system. It was introduced the possibility of losses that arise without fulfilling certain conditions and avoided losses.

Keywords: information security threat; information security system; performance evaluation of information security system; confidentiality; sustainability; availability; observability.

References

1. **Bogdanov V.V.** (2010) The application of risk criteria for assessing the security of the automated system. [Zastosuvannya kryteriyu rizyku dlya otsinki zahishchenosti avtomatizovanoi sistemi], Kyiv, Collection of papers and abstracts, V-scientific and technical conference Viti NTU “KPI”, pp 70-72. 2. **Domarev V.** (2002) Safety of information technology. [Bezopasnost informatsionnyh tehnologiy] Kyiv, p. 352. 3. **Romanov A.I., Liventsev S.P., Pavlov I.** (2004) Mathematical model of information

security in automated networks for special purposes. [Matematichna model zahistu informatsiyi v avtomatizovanih mrezhah spetsialnogo pryznachennya] Kyiv, Proceedings of Viti “KPI” number 5, pp. 23-31. 4. **Haiduk A.C.** (2012) Methodology rational choice version information protection system based on peer reviews. [Metodologiya viboru ratsionalnogo variantu sistemi zahistu informatsiyi na osnovi ekspertnih otsinok], Lviv, The collection of abstracts 2011/2012 academic year, p. 32.

Отримано: 03.08.2016 року.

Рустам Камілович Мурасов (канд. техн. наук)
Ярослав В'ячеславович Мельник

Національний університет оборони України імені Івана Черняхівського, Київ, Україна

ЗАВЧАСНЕ ПОПЕРЕДЖЕННЯ ПРО DDoS АТАКУ НА БАЗІ МЕТОДІВ ПРОГНОЗУВАННЯ

У статті на основі системного аналізу розглядаються сучасні способи DDoS-атак, наведена статистика щодо зростання кібернетичних атак по роках та збитки від них. Для своєчасної та ефективної протидії DDoS-атак, запропоновано здійснювати прогнозування DDoS-атак, розглядаючи їх як випадковий, нестационарний, скалярний процес. Дана методика не накладає обмежень на випадковий процес, забезпечує оптимальну точність прогнозу. Також дана методика застосовує кореляційні зв'язки проміж складовими, що відображається на достовірності прогнозу. Особливо ефективно прогнозування буде здійснюватись при різкій зміні стану випадкового процесу. Також не накладається обмеження на дисперсію випадкового процесу, що значно розширює можливості прогнозування.

Ключові слова: DDoS-атаки; прогнозування; випадковий процес.

Вступ

Роль Інтернету в сучасному суспільстві набуває вагомого значення. Спілкування, інформування, банківські послуги, медіаінформування, управління, сайти державних установ, Інтернет-магазини – все це напряму залежить від здатності функціонування системи Інтернету. Для організації роботи вказаних об'єктів вкладаються великі кошти та зусилля.

Зрозуміло що всі вищевказані об'єкти є цілком для атаки зловмисників чи противника. Одним з видів Інтернет атак є DDoS-атака (Distributed Denial Of Service Attack).

Постановка проблеми. Особливістю даної атаки є те що зловмисники не ставлять за мету проникнення до захищеної комп'ютерної мережі чи викрадення/знищення даних. Метою даної атаки є паралізувати роботу веб-вузлу що атакується (Рис.1).

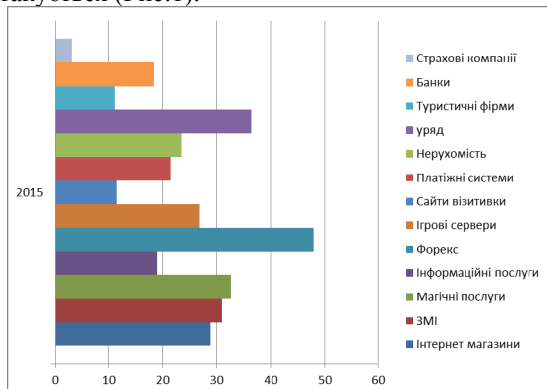


Рис. 1. Кількість DDoS атак по сферам.

Аналіз останніх досліджень і публікацій.

Перші згадки про DDoS-атаки відносяться до 1996 року. Але вперше, як про серйозну проблему було піднято питання у 1999 році коли було атаковано сайти таких великих корпорацій як: Amazon, Yahoo, CNN, eBay, E-Trade і інші менш відомі корпорації. Через рік атака повторилася, сайти були атаковані по DDoS технології при

повному безсиллі мережевих адміністраторів. З того часу подібні атаки вже не рідкість (Рис.2).

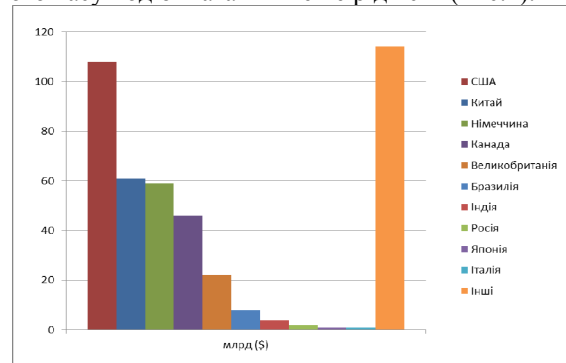


Рис. 2. Орієнтовні збитки від кібератак за 2015 рік.

Метою статті є розгляд DDOS атаки, методи та способи її здійснення та шляхи вирішення протидії DDOS атаки.

Виклад основного матеріалу дослідження

Схема DDoS-атаки виглядає наступним чином (Рис.3). На обраний в якості жертви сервер здійснюється велика кількість хибних запитів з великої кількості комп'ютерів розташованих в різні місця світу. Сервер витрачає час та ресурси на обробку цих запитів і стає практично недоступним для звичайних користувачів. Складність ситуації полягає ще в тому, що користувачі комп'ютерів з яких посилаються запити, можуть і не підозрювати про те що, їх машина використовується хакерами, так-як на неї встановлено спеціальні програми.

Класично схема будується як трьохрівнева структура. Ієрархічно така структура виглядає так.

Управляюча консоль – комп'ютер з якого зловмисник подає сигнал про початок атаки.

Головні комп'ютери – комп'ютери, котрі отримують сигнал з управляючої консолі та передають його комп'ютерам-зомбі. На одну

управляючу консоль може приходиться до кількох сотень головних комп'ютерів.

Агенти – безпосередньо заражені комп'ютери – зомбі, які атакують своїми запитами вузол-мішень.

Головною проблемою є проста організація даної атаки, її розподіленість і те що ресурси зловмисників майже не обмежені.

Іншою проблемою є те, що зловмисникам не потрібно володіти спеціальними знаннями та програмами, все це знаходиться у вільному доступу мережі Інтернет. Це пов'язано з тим що, спеціальне програмне забезпечення DDoS створювалось для тестування роботи мереж і їх здатності до роботи в період навантажень та стійкості до зовнішніх навантажень. Найбільш ефективним є використання ICMP-пакетів (Internet control messaging protocol), пакетів які мають помилкову структуру. На обробку даного пакета необхідно більше ресурсів - після визначення про помилку пакет відправляється назад до відправника, таким чином навантаження мережі досягає максимального рівня.

З моменту появи перших програмних засобів було розроблено більш сучасне програмне забезпечення і на даний час існує такі DDoS атаки:

1. UDP flood – здійснюється відправка на адрес системи-цілі множені пакетів UDP (User Datagram Protocol). Даний метод використовувався в перших атаках і на даний час вважається найменш небезпечним. Програми які використовують цей тип атаки легко виявляються, так як при обміні головного контролера і агентів використовуються незашифровані протоколи TCP і UDP.

2. TCP flood - відправлення на адрес мішені множені TCP-пакетов, що також призводить до “зв'язування” мережевих ресурсів.

3. TCP SYN flood – відправлення великої кількості запитів на ініціалізацію TCP- з'єднань з вузлом – мішенню, що в результаті вимагає витратити усі власні ресурси на відстеження частково відкритих з'єднань.

4. Smurf-атака – пінг - запити ICMP (Internet Control Message Protocol) на адресу направленої ширококомовної по адресу розсилки з використанням в пакетах запиту фальшивої адреси, адрес джерела в результаті є мішенню що атакована.

5. ICMP flood - атака, така сама, як Smurf але без використання розсилки.

Найбільш небезпечними є програми, що використовують одночасно декілька видів атак що було описано. Вони отримали назву TFN і TFN2K і вимагають високого рівня підготовки.

Однією з останніх і досконалих програм для DDoS-атак є Stacheldracht (колючий дріт), яка дозволяє організовувати різноманітні типи атак і лавини широкоешательних пінг – запитів з шифруванням обміну даними проміж контролерами і агентами.

На даний час для протидії DDoS-атакам пропонується вирішити два типи задач:

1. Діагностувати DDoS-атаку на ранніх стадіях. Чим раніше буде діагностовано DDoS-атаку, тим раніше може втрутитися в процес мережевий адміністратор і тим раніше будуть проводитися анти DDoS заходи. Крім того, при виявленні DDoS-атаки можливо, не чекаючи дій адміністратора, автоматично запустити заходи по протидії: задіяти резервні канали, увімкнути мережеві фільтри і т.д.

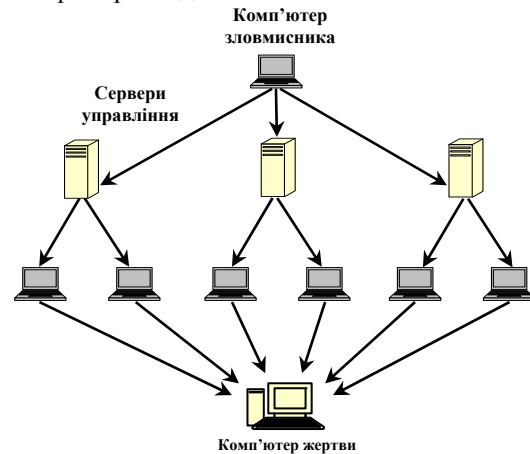


Рис. 3. Схема DDoS атаки.

2. Друга задача пов'язана з розподіленням мережевого трафіку на шкідливий та звичайний. Проаналізувавши трафік та виділивши шкідливий трафік створюються правила для між мережевого екрану та ACL, або передати ці данні на вищестоящий мережевий маршрутизатор.

Перша задача є достатньо новою. Основним методом боротьби на даний час є виконання другої задачі. Але зловмисники удосконалюють способи і методи атак даного типу. Сучасні атаки відрізняються складністю і наявністю підготовчого етапу. Під час підготовчого етапу, зловмисник намагається виявити слабкі місця для атаки. Це можуть бути деякі скрипти, котрі здійснюють запити до бази даних, тим чином використовують ресурси системи, відслідковуючи час на відповідь запиту. Для виявлення подібних місць для атаки здійснюється серія міні DDoS-атак. Знайшовши слабке місце зловмисник може паралізувати сервер використовуючи бот-мережу меншого розміру. Якщо завчасно виявити DDoS-атаку мережевий адміністратор буде мати час на оптимізацію скриптів, побудови системи фільтрів та інше.

Для виявлення DDoS-атак за першим типом атаки визначимо такі методи що базуються на статистичному аналізі. Це кількісний аналіз, аналіз середньоквадратичних відхилень, кластерний аналіз, методи прогнозування випадкових процесів.

Основними параметрами за якими здійснюється аналіз атаки можуть бути:

- кількість запитів за визначений період;
- швидкість надходження запитів;
- кількість запитів з визначеного джерела чи мережі;

- кількість запитів до визначеного джерела (для web - серверу це визначений скрипт);
- час проміж запитами;
- інші параметри мережевої активності.

Крім того можемо розглядати DDoS-атаку як векторний випадковий процес з корельованими або некорельованими складовими. Де за складові можемо обрати джерело атаки, час запиту, частоту запитів, кількість запитів і т.д. – в залежності від наявності даних для аналізу.

Розглянемо математичну формалізацію DDoS-атаки.

Окрему DDoS-атаку розглянемо як скалярний випадковий процес без післядії. Даніми випадкового процесу будуть кількість запитів за проміжок часу.

$$\bar{X} = \{x(1), x(2), \dots, x(1)\}.$$

Найбільш універсальним з точки зору відсутності обмежень на клас випадкових процесів і зручним для обчислення є метод екстраполяції, що базується на канонічному розкладенні Пуґачова. Дане розкладення в дискретному ряді точок t_i , $i = \overline{1, I}$ випадкового процесу що досліджується $\bar{X}(t)$ має вигляд

$$X_h = m_h(i) + \sum_{\lambda=1}^h \sum_{v=1}^i V_v^{(\lambda)} \phi_{hv}^{(\lambda)}(i), h = \overline{1, H}, \quad (1)$$

де $\phi_{hv}^{(\lambda)}(i)$ - невідповідні координатні функції, що визначаються як

$$\phi_{hv}^{(\lambda)}(i) = \frac{1}{D_v^{(\lambda)}} M[X_h(i) V_v^{(\lambda)}], \phi_{hv}^{(\lambda)}(i) = 0 \text{ при } i > v \text{ або}$$

$$\lambda > h; \quad (2)$$

Література

1. **Кудрицкий В. Д.** Прогнозирующий контроль радиоэлектронных устройств / В.Д. Кудрицкий – К.:Техника, 1982. – 166 с. 2. **CyberArk**, Security for the Heart of Enterprise <http://www.cyberark.com/> (26.06.2015). 3. **Butler B.** Interop network squares off against controlled 70G bit/sec DDoS attack. [http://www.networkworld.com/article/2166091/data-](http://www.networkworld.com/article/2166091/data-center/interop-network-squares-off-against-controlled-70g-bit-sec-ddosattack.html)

$$\phi_{hv}^{(\lambda)}(i) = 1 \text{ при } h = \lambda \text{ і } v = i;$$

$V_v^{(\lambda)}$ - випадкові коефіцієнти, що мають наступні властивості:

$$M[V_v^{(\lambda)}] = 0, M[V_v^{(\lambda)} V_\mu^{(\zeta)}] = 0 \text{ при невиконанні жодної умови } v = \mu \text{ і } \lambda = \zeta; M[V_v^{(\lambda)}]^2 = D_v^{(\lambda)}.$$

Як слідує з (2), єдиним обмеженням що накладається на процес апаратом канонічних розкладень є конечність дисперсій відповідних коефіцієнтів, що звичайно задовольняється для реальних фізичних процесів і не є суттєвим.

Показано, що канонічне розкладення (1) точно описує функцію що розкладеться в точках дискретизації t_i , $i = \overline{1, I}$ і забезпечує мінімум середнього квадрату помилки наближення в проміжках проміж ними.

Таким чином, враховуючи переваги метода екстраполяції, що базується на канонічному розкладі випадкового процесу (відсутність на клас процесів що прогнозується, простота обчислення), даний підхід може бути прийнятим за основу в подальших дослідженнях.

Висновки й перспективи подальших досліджень

Вирішення даної задачі дозволить завчасно спрогнозувати та виявити DDoS-атаки та вжити необхідні заходи по протидії та захисту інформаційної та комп'ютерної мережі.

ЗАБЛАГОВРЕМЕННОЕ ПРЕДУПРЕЖДЕНИЯ ОБ DDoS АТАКЕ НА БАЗЕ МЕТОДОВ ПРОГНОЗИРОВАНИЯ

*Рустам Камилович Мурасов (канд. техн. наук)
Ярослав Вячеславович Мельник*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье на основе системного анализа рассматриваются современные способы DDoS-атак, представлена статистика про увеличение количества кибернетических атак по годам и убытки нанесённые данными атаками. Рассмотрены варианты DDoS-атак и показаны современные программные комплексы, которые применяются. В статье для наглядности приведена классическая схема DDoS-атаки. Для своевременного и эффективного противодействия DDoS-атакам, предложено осуществлять прогнозирование DDoS-атак, рассматривая их как случайный, нестационарный, скалярный процесс. Данная методика не накладывает ограничений на случайный процесс, обеспечивает оптимальную точность прогноза. Так же данная методика применяет корреляционные связи между составными элементами, которые отображаются на достоверном прогнозе. Особенно эффективно прогнозирование будет осуществляться при резком изменении состояния случайного процесса. Также не накладывает ограничений на дисперсию случайного процесса, что значительно расширяет возможности прогнозирования.

Ключевые слова: DDoS-атаки; прогнозирование; случайный процесс.

EARLY WARNING INFORMATION ON DDOS ATTACKS BASED ON THE PREDICTION METHODS

Rustam K. Murasov (Candidate of Technical Sciences)

Yaroslav V. Melnyk

National Defense University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine

The article is based on the analysis considering modern methods of DDoS-attacks, presented statistics on the increase of cyber-attacks and losses them. To counteraction DDoS-attacks is proposed to forecast DDoS-attacks, considering them as random, transient, scalar process. This technique does not impose restrictions on the random process ensures optimum accuracy of the forecast. Also, this method uses the correlation between the components displayed on the reliability prediction. Especially prediction will effectively be carried out with a sharp change in the state of a random process. Also, there are no constraints on the variance of a random process, which significantly expands the possibilities of forecasting.

Keywords: DDoS-attacks; forecasting; random process.

References

- 1. Kudritskiy V.D.** (1982), Predictive control of electronic devices. [*Prognozirujushhij kontrol' radioelektronnyh ustrojstv*], Kyiv: Technic, 166 p.
- 2. CyberArk**, Security for the Heart of Enterprise. <http://www.cyberark.com/> (26.06.2015).
- 3. Butler B.** Interop network squares off against controlled 70G bit/sec DDoS attack. <http://www.networkworld.com/article/2166091/data-center/interop-network-squares-off-against-controlled-70g-bit-sec-ddosattack.html> (26.06.2015).
- 4. Wang J., Phan R. C.-W., Whitley J. N., Parish D. J.** (2011), Advanced DDoS Attacks Traffic Simulation with a Test Center Platform, International Journal for Information Security Research (IJISR), Vol. 1(4).

Отримано: 06.08.2016 року.

¹Леонід Анатолійович Маслюк (канд. техн. наук, с.н.с.)¹Петро Іванович Стужук (канд. військ. наук, доцент)¹Олександр Олександрович Челобітченко (канд. техн. наук, с.н.с.)²Олександр Миколайович Правдивець¹Національний університет оборони України імені Івана Черняхівського, Київ, Україна²Генеральний штаб Збройних Сил України, Київ, Україна

ПРОБЛЕМИ ТА РЕКОМЕНДАЦІЇ ЗІ СТВОРЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ВІЙСЬКАМИ (СИЛАМИ) ДЛЯ ЗБРОЙНИХ СИЛ

Під час створення автоматизованих систем управління військами (силами) для збройних сил виникає низка проблем. У статті проведений аналіз цих проблем та на підставі власного досвіду створення навчальної автоматизованої системи управління військами (АСУВ) автори пропонують практичні рекомендації для їх усунення. Визначені основні принципи створення АСУВ: системності, розвитку (відкритості), сумісності, стандартизації (уніфікації), ефективності, першого керівника, нових завдань. Запропоновано функціональну структуру АСУВ визначати на основі єдності оперативного-стратегічних, системотехнічних та організаційних аспектів процесу управління військами (силами). Показано, що в основу формування складу функціональних підсистем та інформаційно-розрахункових задач (моделей) навчальної АСУВ був покладений об'єктно-функціональний метод. Наявність геоінформаційної підсистеми є необхідною умовою існування сучасної АСУВ. Також показано, що незважаючи на функціональну єдність органів військового управління, структури АСУВ різних рівнів та різних об'єктів автоматизації не ідентичні між собою.

Ключові слова: автоматизовані системи управління військами; об'єктно-функціональний метод; структура автоматизованих систем управління військами.

Вступ

Останні десятиріччя ХХ та початку ХХІ століття характеризуються переходом збройних сил передових у військовому відношенні країн світу до автоматизованого управління військами (силами) і зброєю. Армії майже усіх провідних держав мають на озброєнні автоматизовані системи управління військами (силами). Автоматизоване управління військами і зброєю у часі, близькому до реального, та єдине інформаційне середовище прийняття управлінських рішень на застосування військ (сил) та зброї стали вирішальним чинником досягнення успіху в бою (операції) [2].

Постановка проблеми. Як свідчить практика, проблема створення АСУВ, крім фінансових, організаційних і навіть політичних аспектів, полягає у відсутності ґрунтовних методологічних засад і рекомендацій [4].

Вже на передпроектних стадіях створення АСУВ замовник у тактико-технічному завданні (ТТЗ) визначає певний обрис системи. Як правило, цьому передують дослідження об'єктів автоматизації, під час яких встановлюють функції, які підлягають автоматизації, а також структура дослідного зразка майбутньої АСУВ [5]. Структура системи визначається достатньо суб'єктивно, у кращому випадку з урахуванням вітчизняного та світового досвіду, але без урахування особливостей і реалій функціонування системи управління збройних сил (ЗС). Тому раціональність такої структури є сумнівною, що змушує у подальшому постійно вносити зміни до

ТТЗ. Проблема поглиблюється тим фактором, що на передпроектних стадіях створення АСУВ невідомі у повному обсязі інформаційні технології, які будуть застосовані для створення дослідного зразка системи. А оскільки структура АСУВ (склад, зв'язки) та розподіл автоматизованих і неавтоматизованих функцій між підсистемами корінним чином залежить від вибраних технологій оброблення інформації, то їх визначення є об'єктивно проблематичним навіть на стадії розроблення технічного проекту [1].

Аналіз останніх досліджень і публікацій.

Проблеми створення АСУВ, основні завдання та можливі напрями широко проаналізовані у спеціальній літературі, періодичних виданнях. Порядок створення організаційних АСУ детально висвітлений у міжнародних і державних стандартах та відомчих документах [2–4]. Разом з тим методи визначення раціональної структури АСУВ достатньо мірою не розроблені. Світова та вітчизняна наука і практика не запропонували нічого кращого, ніж ітераційні методи створення АСУ (каскадний, спіральний та ін.), що змушує постійно уточнювати початкову модель структури дослідного зразка в міру просування в його створенні.

Співробітники Національного університету оборони України імені Івана Черняхівського упродовж останніх років займалися створенням навчальної АСУВ для ЗС, використовуючи при цьому результати власних досліджень та практичних розробок.

Метою статті є висвітлення результатів

досліджень, проведених в університеті, та надання практичних рекомендацій стосовно визначення раціональної структури та створення АСУВ для ЗС.

Виклад основного матеріалу дослідження

Створення АСУВ завжди було і залишається складною науково-технічною проблемою. Складність її вирішення значною мірою може бути послаблена за рахунок дотримання принципів та використання доцільних методів створення системи, у тому числі щодо структури дослідного разка АСУВ [1, 4].

Для вибору методів обґрунтування структури дослідного зразка АСУВ надзвичайно важливо установити, що вони не суперечать основним принципам її створення. Для АСУ організаційного типу, як правило, виділяють такі основні принципи її створення: системності; розвитку (відкритості); сумісності; стандартизації (уніфікації); ефективності; першого керівника; нових завдань [1, 6, 7].

Принцип системності полягає у тому, що під час декомпозиції АСУВ мають бути установлені склад структурних елементів та зв'язки між ними, які забезпечують її цілісність, сумісність та інтегрованість як в середині системи, так і з іншими АСУ. Принцип системності слід застосовувати під час розроблення усіх видів забезпечення АСУВ. Так, у програмному забезпеченні необхідно використовувати єдину структурну побудову, програмну сумісність, стандартизацію прикладних програм (застосувань), у технічному забезпеченні – взаємозв'язок і сумісність усіх технічних засобів АСУ, в інформаційному – єдність інформаційної бази, системи класифікації і кодування інформації, використання уніфікованої системи документації тощо.

Принцип розвитку полягає у тому, що АСУВ необхідно створювати з урахуванням можливості її поповнення та оновлення функцій і складу без порушення її функціонування.

Принцип стандартизації полягає у тому, що під час створення АСУВ мають бути раціонально застосовані типові, уніфіковані й стандартизовані елементи проектних рішень і базові пакети прикладних програм (застосувань). Дотримання

цього принципу особливо важливо у разі створення АСУВ високого рівня управління, для яких трудомісткість робіт становить декілька тисяч людино-років. Рівень типізації може бути різним, – від рівня підсистем до окремих інформаційно-розрахункових задач (ІРЗ) або інформаційних задач (ІЗ).

Принцип ефективності полягає у досягненні раціонального співвідношення витрат на створення АСУВ і цільовому ефекті, якого досягають у результаті автоматизації управління військами (силами).

Принцип першого керівника передбачає безпосередню участь першого керівника органу військового управління (ОВУ), який глибше розуміється на сутності і важливості втілення АСУВ, перебудові організаційної структури управління в умовах застосування системи, перерозподілі функцій і завдань колективу, їх навчання, формуванні нового становлення персоналу до своїх обов'язків і стилю роботи з використанням АСУВ. Академік Глушков В. М. відмічав цей принцип як визначальний у побудові АСУ.

Принцип нових завдань передбачає пошук таких можливих нових завдань управління військами (силами), вирішення яких забезпечить високу ефективність застосування АСУВ. Цей принцип вимагає аналізу управлінських завдань і виявлення втрат, які виникають в об'єктах управління. Висока ефективність АСУВ, що створюється, значною мірою забезпечується введенням принципово нових задач, як правило, оптимізаційних, які раніше ОВУ не вирішував.

Структура АСУВ організаційно та функціонально має відповідати існуючій або перспективній структурі системи управління військами (силами), змісту роботи структурних підрозділів та посадових осіб ОВУ, а також повинна автоматизувати функції посадових осіб зі складу тимчасових функціональних структур, що створюються або підпорядковуються ОВУ для вирішення окремих завдань управління. Згідно з державними стандартами АСУВ поділяють на дві частини: функціональну (1+k) та забезпечення (1+z), які характеризують різні властивості системи (рис. 1).

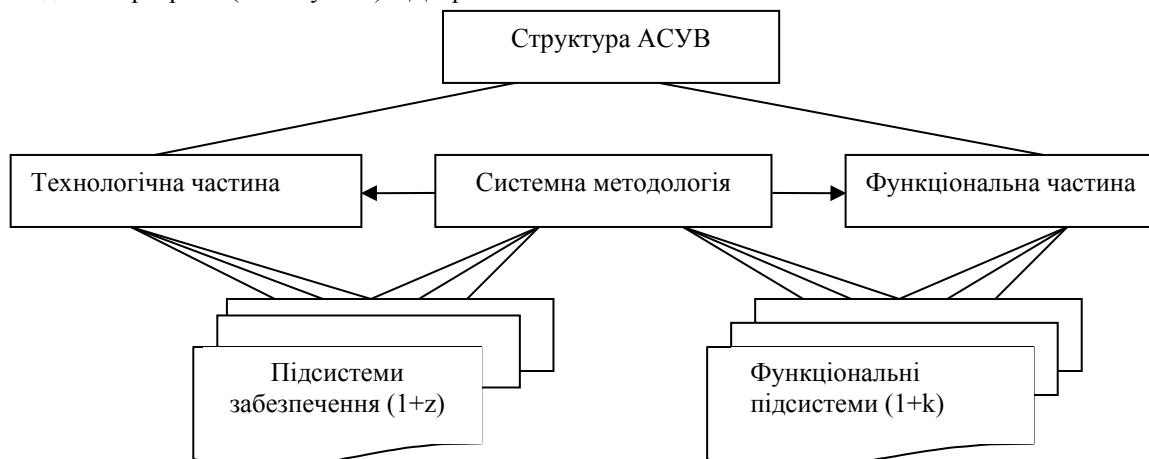


Рис. 1. Структура побудови підсистем АСУВ

Функціональна частина АСУВ відображає стан цілей і керуючих впливів, пов'язаних з певними функціями управління і зв'язками між ними. Частина забезпечення системи включає об'єднані телекомунікаційними мережами комплекс забезпечувальних (технологічних) підсистем. Дослідження показують, що такий рівень деталізації складових АСУВ є недостатнім для практичного розроблення її раціональної структури.

В основу формування складу функціональних підсистем навчальної АСУВ покладено об'єктно-

функціональний метод [7]. Сутність методу полягає у виділенні горизонтальних функцій управління, які підлягають автоматизації на кожному рівні ієрархії органів управління, з одночасною автоматизацією вертикальних функцій управління військами (силами) (рис. 2). Для цього виконують декомпозицію загальних функцій управління військами (силами) з деталізацією до функцій, виконання яких покладається на певні структурні підрозділи ОВУ та їх посадових осіб, розміщених на автоматизованих робочих місцях (АРМ).

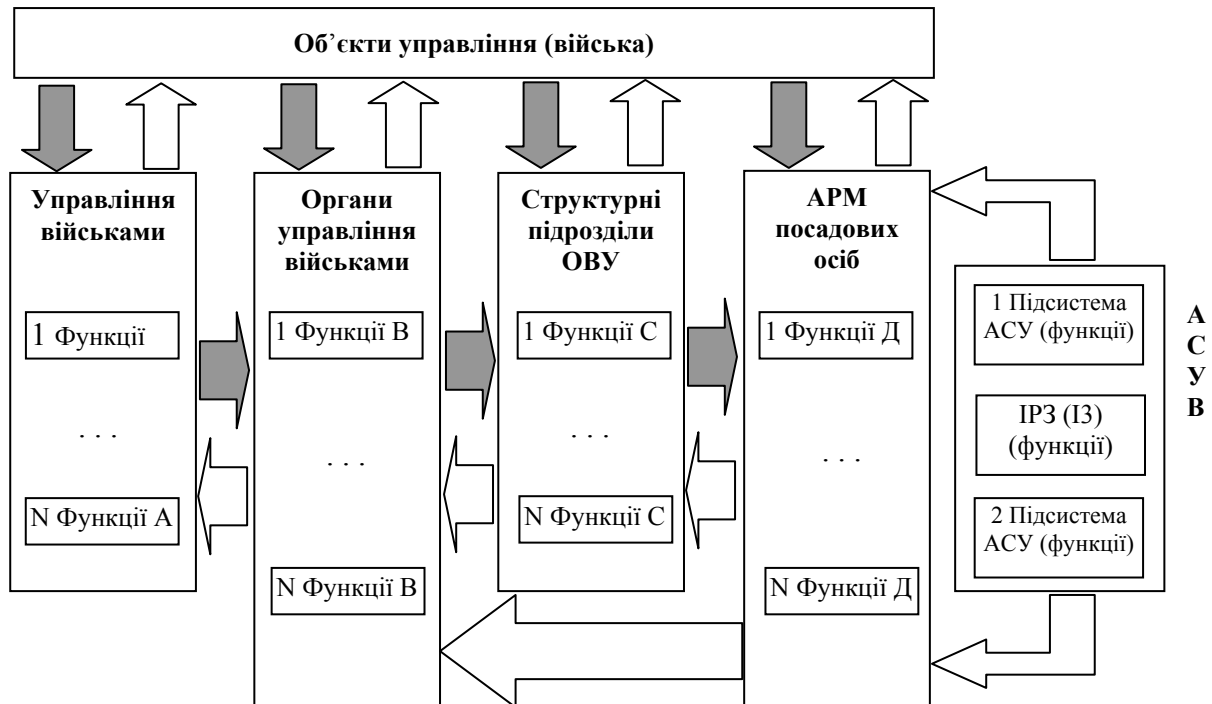


Рис. 2. Сутність об'єктно-функціонального методу визначення складу підсистем та інформаційно-розрахункових задач (моделей)

У подальшому здійснюється об'єктно-функціональний синтез автоматизованих функцій у рамках функціональних і забезпечувальних (технологічних) підсистем та інформаційно-розрахункових задач (ІРЗ) (моделей), а також вибір інформаційних технологій, за допомогою яких можна здійснити автоматизацію спорідненої множини функцій. Загальні функції, які постійно виконують більшість посадових осіб ОВУ, автоматизуються функціональними підсистемами, часткові функції, які виконують періодично, – автоматизуються за рахунок використання ІРЗ (моделей) та окремих програмних засобів [5, 6].

Функціональна структура АСУВ визначається на основі єдності оперативно-стратегічних, системотехнічних та організаційних аспектів процесу управління військами (силами). Для цього функціональна структура має насамперед задовольняти такі критерії:

забезпечувати максимальну автономність стосовно автоматизації функцій (одна відокремлена функція управління реалізується однією функціональною підсистемою, декілька близьких за змістом функцій доцільно об'єднувати та реалізовувати в рамках однієї функціональної підсистеми);

враховувати особливості математичних методів і моделей, спеціального програмного забезпечення (декілька функцій, які можна реалізувати з

використанням єдиного математичного апарату та спеціального програмного забезпечення, об'єднуються в рамках однієї функціональної системи на базі одного програмного комплексу);

врахувати функціональні особливості ОВУ за характером вирішуваних завдань та інформації, яку використовують для їх вирішення.

Як правило, визначення підсистем АСУВ тільки на основі автоматизації однотипних функцій є неповним, оскільки наявні інформаційні технології не забезпечують їх вирішення у рамках однієї із них, а інтеграція у рамках одного програмного виробу часто неможлива, оскільки суперечить вимогам щодо завершеності та незалежності функціонування підсистем. Так, текстуальні електронні документи створюються засобами електронного документування, а графічні документи на електронних картах – засобами відображення оперативної обстановки. Хоча функціонально це один бойовий (оперативний) документ, наприклад, План вогневого ураження противника.

В інших випадках можливе об'єднання різних автоматизованих функцій у рамках однієї підсистеми, наприклад, інформаційно-довідкова підсистема може як надавати вихідні дані, так і зберігати результати розрахунків розв'язання ІРЗ та моделей за допомогою інформаційно-розрахункової підсистеми.

Для визначення раціонального складу АСУВ за функціонально-об'єктним методом необхідно або розробити детальну інформаційну (математичну) модель АСУВ, або покласти в основу системи, що створюється, реальну систему. Перший спосіб складний і не гарантує позитивного кінцевого результату. Його застосовують, якщо не існує відповідних аналогів АСУ. За реальний базовий прототип для створення АСУВ оперативно-тактичного рівня (управління ОК – бригада) пропонується прийняти навчальну АСУВ.

Проведений аналіз функцій управління військами (силами) показав [5], що найпоширенішою функцією ОВУ є обмін інформацією, а найбільш відомою інформаційною технологією її реалізації є електронна пошта. Тому в основу підсистеми обміну інформацією АСУВ можна покласти основні технологічні рішення електронної пошти, з розширенням її прикладної функціональної складової та з урахуванням особливостей обміну інформації в середині та між ОВУ ЗС. У підсистемі також мають реалізуватися вимоги керівних документів щодо організації обміну інформацією у ЗС у цілому. Крім того, з урахуванням обмежених можливостей військових телекомунікаційних мереж у підсистемі має використовуватися раціональна дисципліна формування черг електронних відправлень на основі їх пріоритетності. На думку авторів, такою є дисципліна формування черг електронних відправлень на основі їх відносної пріоритетності. Тобто черга формується на основі заданої пріоритетності (терміновості), а чергове відправлення здійснюється після завершення попереднього. Така дисципліна реалізована у підсистемі інформаційного обміну (ПІО) навчальної АСУВ. Випробування підсистеми з використанням реальних військових телекомунікаційних мереж підтвердили високу її

ефективність – електронний бойовий документ, що включав текстову і графічну на електронній карті складові, передавався із ОВУ тактичного рівня до ОВУ оперативного рівня за 5–7 секунд.

Запропоновані вище підходи і методи визначення складу підсистем АСУВ дали змогу зменшити кількість підсистем, які забезпечують обмін інформацією. Так, наприклад, у навчальній АСУВ, на відміну від абсолютної більшості відомих проектів, функції командно-сигнальної підсистеми реалізовані у підсистемі інформаційного обміну, оскільки вона забезпечує обмін інформацією будь-якого формату як у середині одного ОВУ, так і між різними ОВУ фактично у реальному часі.

У складі більшості АСУ військового призначення є підсистема відеоконференцв'язку (ВКЗ), яка призначена для забезпечення аудіо- та відеозв'язком посадових осіб органу управління, що дає змогу ставити завдання, проводити службові наради у формі відеоконференцій. Дослідження показали, що дана підсистема не є найкращим вирішенням бойового управління військами. Можливості з її застосування обмежуються військовими телекомунікаційними мережами. Співвідношення між витратами на її створення та ефективністю застосування для обміну інформацією між ОВУ є нижчими, чим у підсистемі інформаційного обміну. Тому ВКЗ доцільно використовувати у середині великих ОВУ, наприклад, управління оперативних командувань (ОК).

Підсистеми електронного документообігу (ПЕДО) органів управління АСУВ ЗС різних рівнів повинні мати можливість гарантованого обміну електронними документами (ЕД). Типова схема передачі вихідних ЕД через підсистему електронного документообігу АСУВ показана на рис. 3.

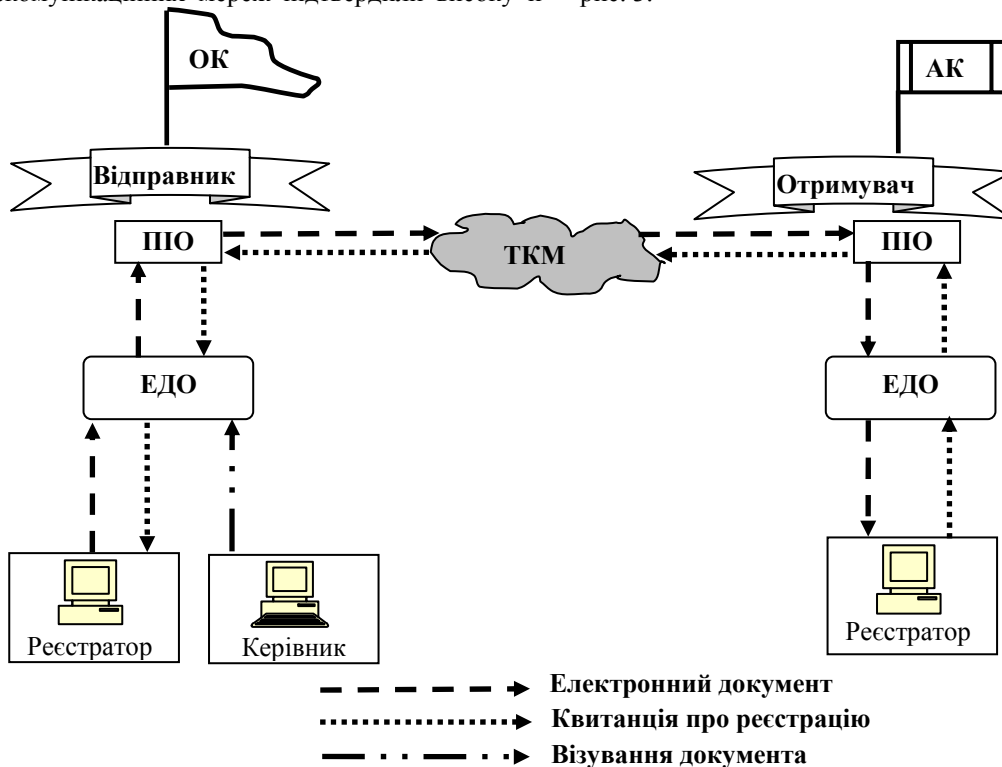


Рис. 3. Типова схема передачі вихідних електронних документів

Документообіг у системі управління військами (силами) припускає складні багатокрокові алгоритми проходження оперативних (бойових) документів під час їх розроблення, погодження та затвердження. Тому застосування в ОВУ для управління військами неадаптованих підсистем аналогічного призначення неможливе.

Протиріччя між зростаючими обсягами потоків геодезичної інформації (ГІ) та можливостями їх оброблення і використання, потребують розроблення нових програмних та технічних засобів з використанням сучасних ГІС-технологій, серед яких важливе місце займають геоінформаційні системи військового призначення, які є невід'ємною складовою сучасних АСУВ [2, 3, 8].

Геоінформаційна підсистема (ГПС) АСУВ – це система збору, зберігання, аналізу й графічної візуалізації просторових даних і пов'язаної з ними інформації про об'єкти, розташовані на місцевості, в якій поєднується робота з просторовими і тематичними базами даних (БД), що забезпечує виконання функцій моделювання, розрахунків і створення тематичних карт з метою інформаційного забезпечення, прийняття рішень, керування, контролю тощо.

Дослідження показали, що основу ГПС мають становити: програмне забезпечення ArcGis; спеціальне прикладне програмне забезпечення, що урахує специфічні потреби ОВУ; база цифрових топогеодезичних даних (електронні карти (ЕК), цифрові фотоплани, цифрові просторові моделі місцевості тощо); технічну основу – обчислювальна техніка з достатніми можливостями стосовно оброблення і зберігання ГІ, пристрої оперативного друку і тиражування невеликих за обсягами тиражів документів з інформацією про місцевість.

Структура ГПС навчальної АСУВ показана на рис. 4.

Традиційно на ГПС покладають також завдання відображення оперативно-тактичної обстановки (ОТО) на ЕК. Але наразі жодна із відомих ГПС не задовольняє у повному обсязі вимоги щодо відображення і ведення ОТО. Тому в АСУВ потрібна додаткова підсистема для відображення на ЕК місцевості положення сил та засобів сторін, їх стану та дій, підтримки унікальності обстановки в органі управління, ведення оперативним складом робочих ЕК, формування карти операції (бою) тощо.

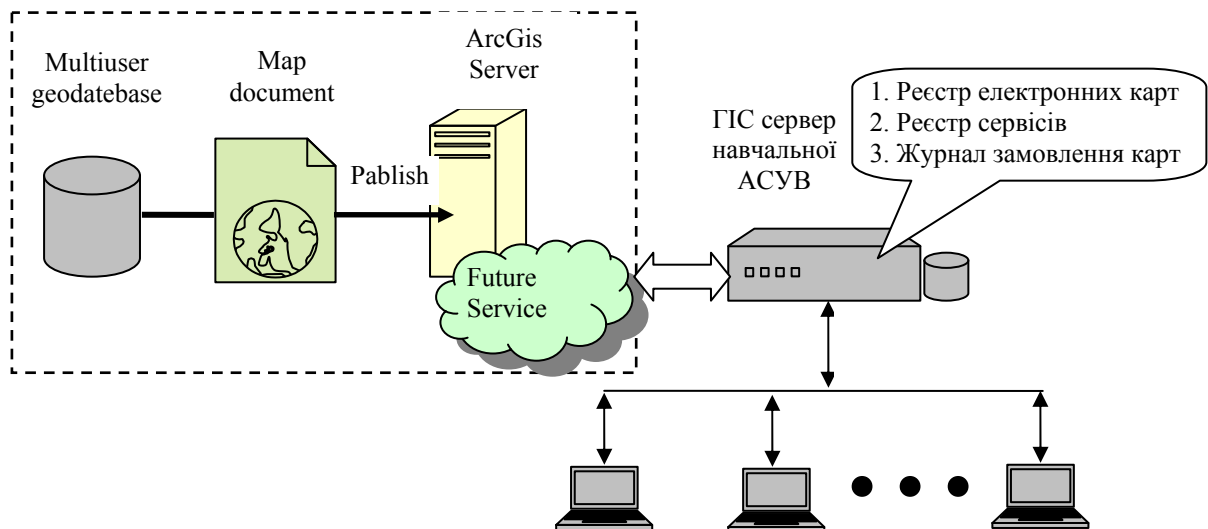


Рис. 4. Структура ГПС навчальної АСУВ

В навчальній АСУВ функції оброблення геодезичних даних та ведення ОТО технологічно розділені через геоінформаційну підсистему та підсистему ведення і відображення положення, стану та дій військ (ПСД), що дало змогу використовувати більш ефективні технології оброблення інформації, а головне, задовольнити потреби ОВУ в автоматизації функцій управління.

Підсистема забезпечує таке: формування бібліотек умовних знаків; нанесення ОТО на електронну карту місцевості; ведення робочої карти офіцера; ведення карти операції (бою); передачу і отримання ОТО тощо. Як показує досвід проведення навчань зі слухачами університету, підсистема виявилася також надзвичайно корисною для колективного

вироблення замислу операції (бою), організації взаємодії та проведення брифінгів з демонстрацією ОТО на електронній карті місцевості.

Інформаційно-аналітична складова (ІАС) – найбільш різноманітна сфера діяльності ОВУ. За обсягом трудовитрат ІАС становить близько 80% усіх заходів із оперативного планування [9]. Для оброблення різноманітної управлінської інформації та проведення різних оперативно-тактичних розрахунків у навчальній АСУВ розроблена інформаційно-розрахункова підсистема (ІРП), яка забезпечує інформаційно-аналітичну діяльність ОВУ. Структура підсистеми показана на рис. 5.

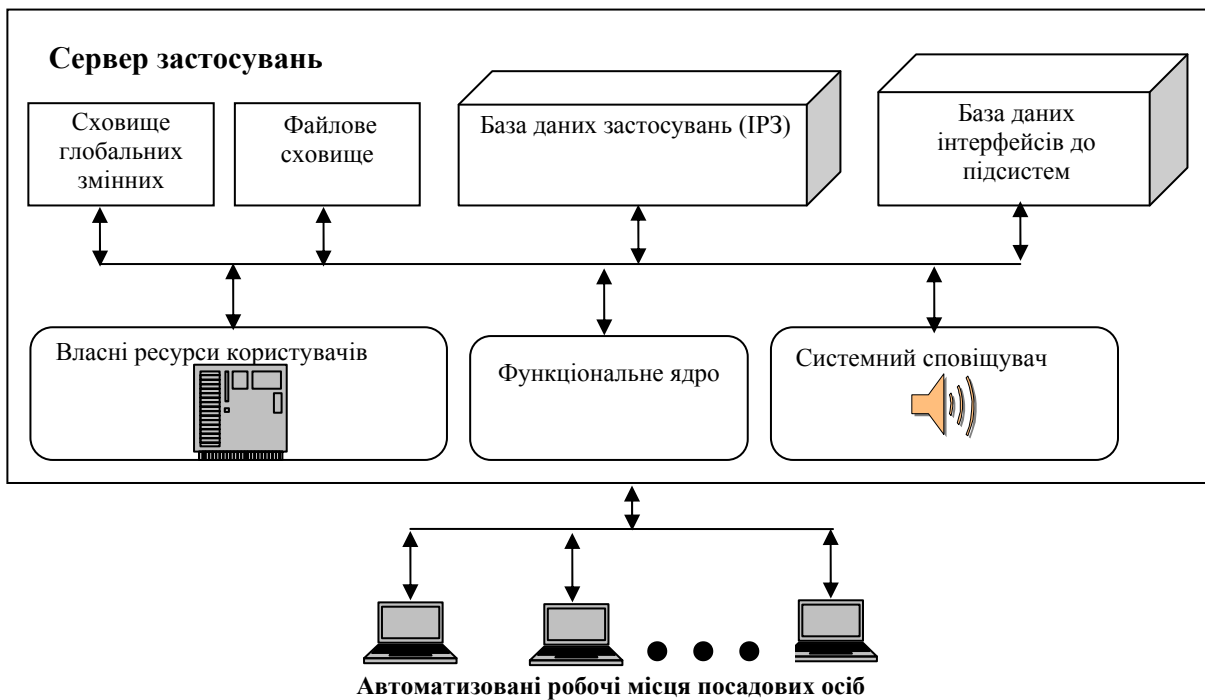


Рис. 5. Структура інформаційно-розрахункової підсистеми АСУВ

Переважно більшість управлінських функцій посадових осіб ОВУ необхідно виконувати з підтримкою відповідних ІРЗ, ІЗ та моделей. Інформаційно-розрахункова підсистема може включати велику їх кількість (від декількох десятків до декількох сотень) залежно від потреб користувачів в обробленні інформації та проведенні оперативно-тактичних розрахунків. При цьому функції, що автоматизуються, мають розглядатися з точки зору потреб кінцевих користувачів, а не зручності програмної реалізації. Але, з іншого боку, необхідно забезпечити мінімальну надлишковість задач та моделей, особливо таких, які одноразово використовують посадові особи на різних часових зрізах процесу підготовки та ведення операції [9].

Окремі ІРЗ (ІЗ) та моделі АСУВ можуть оперувати різними масивами вихідної та результуючої інформації, різними ступенями її деталізації, але за використовуваними методами та алгоритмами розв'язання, та їх все ж треба поєднувати у функціональні комплекси, коли результати розв'язання однієї задачі є вхідними даними для декількох інших.

Аналіз результатів виконання ДКР зі створення АСУВ показує, що наразі не існує єдиної методології визначення раціонального переліку й комплексів ІРЗ (ІЗ) та моделей, здатних моделювати та аналізувати різні види знань, що надходять з різнорідних джерел для вирішення складних слабкоструктурованих і неструктурованих завдань управління військами (силами) [9].

Разом з тим аналіз характеру предметної галузі управління військами (силами) дає змогу сформулювати особливості визначення раціонального переліку ІРЗ (ІЗ) і моделей та

формування їх комплексів для АСУВ: розподілений характер розв'язання задач, адаптивність представлення знань та пошуку рішень, велика різноманітність методів та алгоритмів оброблення інформації, використання сучасних інформаційних технологій, ієрархічність структури бази даних і бази знань, відкритість модульної структури тощо.

Завдяки застосуванню об'єктно-функціонального методу розподілу функцій інформаційно-розрахункові (інформаційні) моделі та задачі використовують базові можливості усіх складових підсистем АСУВ, що виключає непотрібне дублювання СПЗ та забезпечує розширений інтерфейс користувачам АРМ (рис. 6).

Об'єктно-функціональний підхід до формування переліку ІРЗ (ІЗ) та моделей дає змогу, з одного боку, визначити раціональний склад ІРП як функціональної складової частини АСУВ, а з іншого боку, – раціональну сукупність самостійних формальних ІРЗ, моделей, програмних комплексів, що реалізують в інтерактивному режимі функції інформаційно-аналітичного забезпечення командувача та решти посадових осіб під час підготовки та прийняття формалізованих і неформалізованих управлінських рішень на їх АРМ.

При такому підході до визначення переліку ІРЗ (моделей) забезпечується повне охоплення функцій і завдань, які вирішують посадові особи ОВУ у будь-яких умовах його функціонування. Крім цього забезпечується певний рівень структуризації складу комплексів ІРЗ та моделей і відсутність надлишковості у зв'язку з їх чіткою прив'язкою до функцій управління.

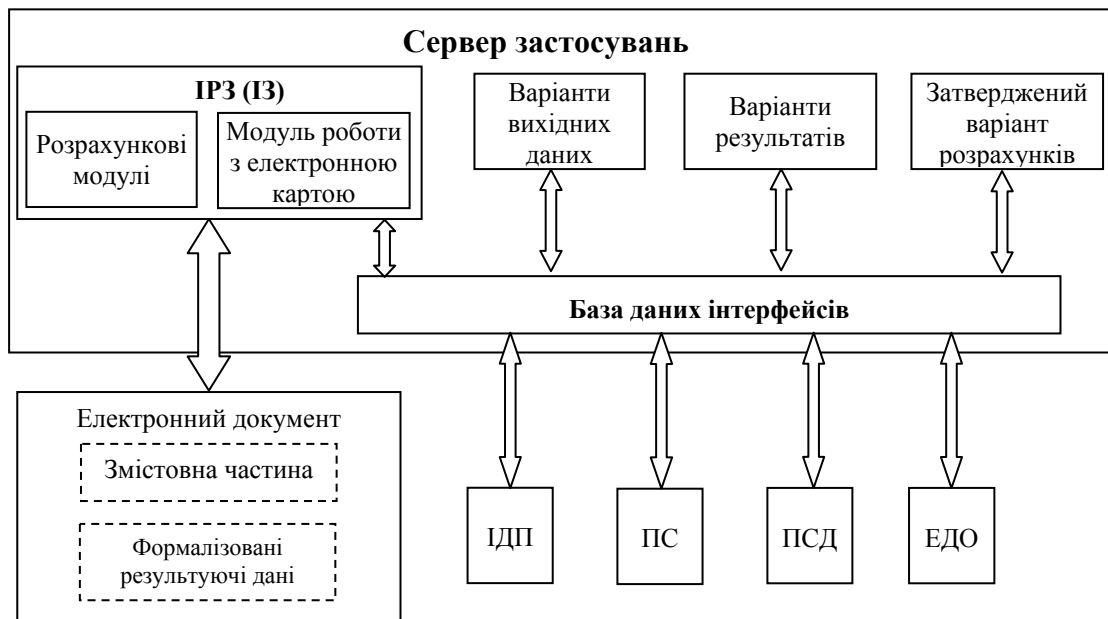


Рис. 6. Базова структура інформаційно-розрахункової задачі

Дослідження показали, що для формування необхідного інформаційного ресурсу АСУВ має бути створена інформаційно-довідкова підсистема (ІДП), яка забезпечує необхідну довідкову інформацію для розв'язання ІРЗ та моделей. Підсистема має забезпечувати: створення і ведення електронних довідників за обраною тематикою; пошук і надання користувачам необхідної довідкової інформації; надання довідкових даних для проведення оперативно-тактичних

розрахунків; ефективний пошук і зручне подання інформації.

Інформація про інформаційні об'єкти, наприклад, про ОБТ, може надаватись у формалізованому і неформалізованому вигляді, як показано на рис. 7. Архітектура ІДП може бути фасетно-ієрархічною і будується за схемою: тематичний довідник – спеціалізований довідник – клас – об'єкт – атрибут – значення атрибута – посилання.

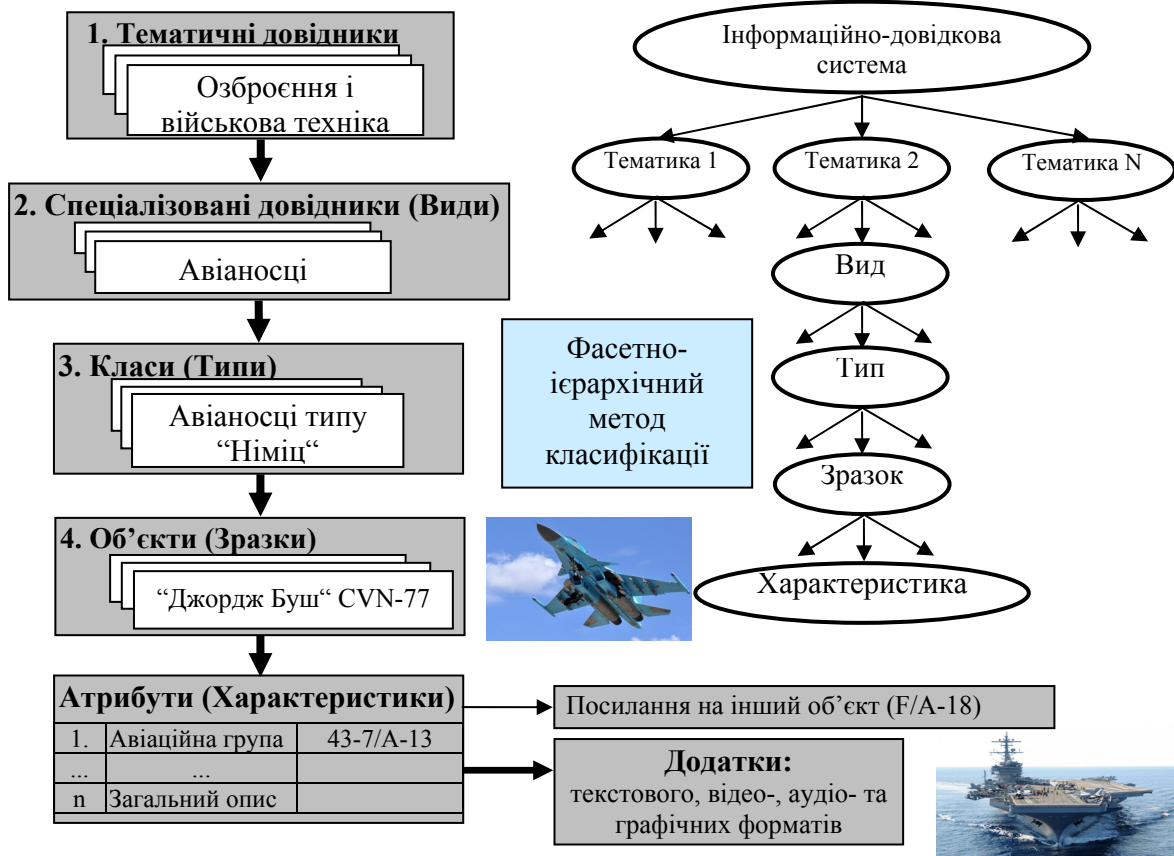


Рис. 7. Архітектура інформаційно-довідкової підсистеми

Всі інформаційні об'єкти стосовно управління військами (силами), які можуть бути описані даною ієрархією, можуть бути також представлені в ІДП. Кожен довідник з інформацією є унікальним, створюється під потреби певного ОВУ, але може тиражуватись також в інші органи управління.

Тематичні довідники об'єднані у фасети, а інші її елементи є ієрархією спеціалізованих довідників, класів, об'єктів і атрибутів, значень, посилань.

Однією з основних умов ефективного функціонування АСУВ є наявність підсистеми, що забезпечує організацію спільної автоматизованої роботи підрозділів (центрів, груп) органів управління, встановлення раціональних зв'язків між джерелами і приймачами інформації та шляхів її циркуляції.

Підсистема організації роботи штабу має забезпечувати планування роботи органу управління, ставити завдання оперативному складу та контролювати їх виконання, проводити організаційні розрахунки, в тому числі і розрахунок часу, графіки роботи та календарні плани тощо.

Надзвичайно важливою функцією ОВУ, яку належить автоматизувати, є висвітлення поточної ОТО. Основним призначенням підсистеми висвітлення обстановки є збір, оброблення, збереження та надання інформації про противника, свої війська та фізико-географічні умови в районі операції (бойових дій).

Складність створення такої підсистеми полягає не тільки і не стільки у великій кількості джерел, обсягу та різноманітності інформації, але насамперед, у великій різноманітності методів і способів її оброблення і формального відображення. Їх реалізація у рамках однієї підсистеми є складним науково-технічним завданням. Зарубіжний досвід створення таких систем свідчить про необхідність її декомпозиції. Наприклад, створення окремих підсистем збору, оброблення, збереження і обміну інформації окремо про противника, свої війська, район бойових дій тощо.

Управління функціонуванням АСУВ – це виконання важливих функцій контролю, планування, виділення, впровадження, координування та моніторингу ресурсів власне самої системи. Відповідно до змісту управління функціонуванням АСУВ підсистема управління функціонуванням (ПУФ) призначена для

забезпечення організаційного та програмно-технічного управління роботою функціональних підсистем для їх комплексного, сумісного, стійкого та безперервного функціонування згідно з визначеним регламентом, підтримки єдиного часу, моніторингу, контролю за функціонуванням і управлінням комплексу засобів автоматизації (КЗА), балансування обчислювального навантаження тощо.

Комплексні системи захисту інформації КЗА об'єктів автоматизації АСУВ створюють з урахуванням забезпечення режиму секретності під час проектування, розроблення, виготовлення, випробування, сертифікації, експлуатації, ремонту, списання та ліквідації системи.

Незважаючи на функціональну єдність ОВУ, структури АСУВ різних рівнів та різних об'єктів автоматизації не однакові. Будучи прив'язаними до існуючих структур органів управління, що базуються на ручному обробленні інформації, для низки випадків структури АСУВ об'єднують функціональні підсистеми і підсистеми забезпечення під однією ознакою і розглядаються як однорідні. У результаті створюється положення, при якому одну й ту ж вихідну інформацію, що характеризує ті чи інші процеси управління, збирають різні служби для подальшого оброблення. При цьому одні розв'язувані системою завдання дублюються в різних підсистемах, а інші – узагалі не є предметом розгляду. Неоднорідність підсистем АСУВ передбачає певне раціональне дублювання деяких типів завдань. Тому доцільно групувати їх за однорідними ознаками, при цьому не тільки не повторюються елементи одних підсистем в інших, але і залишається широкий маневр формування комплексів завдань автоматизованого управління, не міняючи самої структури і методики їх розв'язання та взаємозв'язок між підсистемами за рахунок вхідної і результуючої інформації.

На нашу думку, склад КЗА ОВУ оперативного і тактичного рівнів має бути типовим і включати такі підсистеми навчальної АСУВ (рис. 8): інформаційного обміну; відеоконференцзв'язку; електронного документообігу; організації роботи штабу; інформаційно-довідкову; геоінформаційну; ведення і відображення положення, стану та дій військ; інформаційно-розрахункову; висвітлення обстановки; управління функціонуванням; комплексну систему захисту інформації від несанкціонованого доступу.

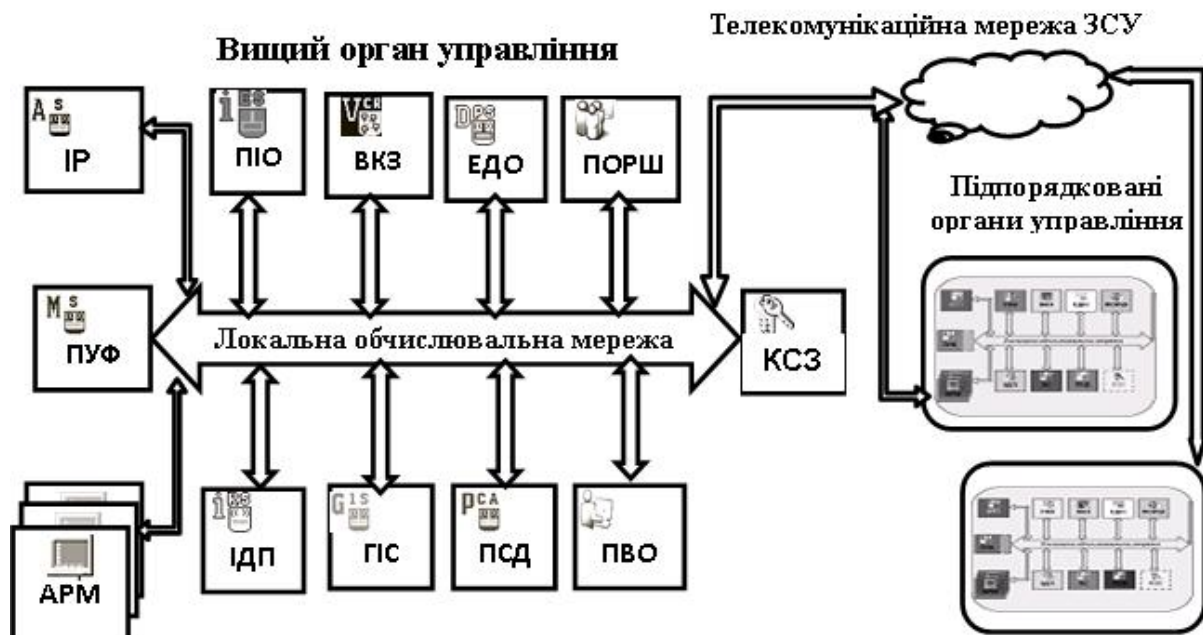


Рис. 8. Орієнтовний склад підсистем АСУВ оперативного і тактичного рівнів

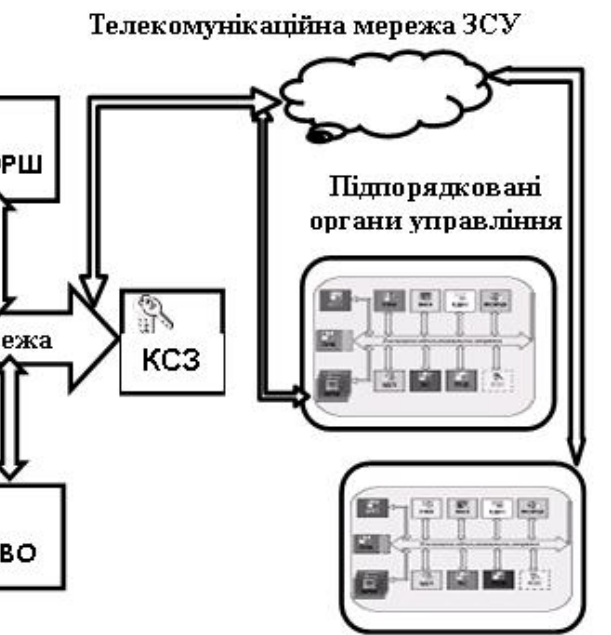
Наведений склад підсистем не є вичерпаним, але надає достатню базову основу для автоматизованого управління військами (силами). Можна з високою ймовірністю припустити, що з використанням навчальної АСУВ більшість функцій управління військами (силами) оперативно-тактичного рівня будуть вирішуватися автоматизовано. А оскільки система з точки зору технології створення є відкритою, то у разі потреби є можливість розширення функціональних можливостей як через створення нових складових підсистем, так і розширення складу ІРЗ і моделей.

Комплекси засобів автоматизації ОВУ повинні містити підсистеми АСУВ, які автоматизують діяльність ОВУ в загальній системі управління військами (силами). КЗА повинні розгортатися та функціонувати за призначенням на усіх пунктах управління (ПУ) ЗС до окремої частини (підрозділу) включно.

Комплекси засобів автоматизації ОВУ мають бути типовими за своїм складом, базовими за виконанням загальних функцій і спеціалізованими щодо реалізації специфічних функцій управління та включати комплекс підсистем, що можуть функціонувати як автономно, так і забезпечувати сумісне (інтероперабельне) функціонування на основі кооперування в потрібний проміжок часу для вирішення поточних завдань автоматизованого управління військами (силами).

Елементи КЗА на ПУ ОВУ можуть бути розподілені по-різному, але головною умовою їх функціонування є об'єднання в локальну обчислювальну мережу [1, 6].

Різні КЗА мають урахувувати специфіку функцій, які виконують посадові особи ОВУ. Для цього створюють спеціалізовані АРМ посадових осіб, які налаштовуються на конкретного користувача (персональні АРМ).



Досвід проведення КШН з використанням навчальної АСУВ свідчить про доцільність спеціалізації АРМ відповідно до потреб конкретних посадових осіб та структурних підрозділів ОВУ, але без фізичного закріплення до певної робочої станції. Автоматизоване робоче місце посадової особи має формуватися автоматично на комп'ютері після її реєстрації в АСУВ.

Висновки й перспективи подальших досліджень

Загальна мінімальна кількість фізичних АРМ для кожного структурного підрозділу (кожного КЗА) ОВУ залежить від його ієрархічного рівня в системі управління, обсягу і специфіки завдань, які виконують посадові особи, і має становити до 50–60 % від кількості оперативного складу. Більш конкретно їх кількість визначається на етапі розроблення робочо-конструкторської документації на створення АСУВ та може уточнюватися в процесі дослідної експлуатації конкретного КЗА ОВУ.

Аналіз стану робіт зі створення АСУВ різного рівня і функціонального призначення для потреб ЗС [2–4] викриває ряд загальних науково-технічних проблем і недоліків, а саме:

недотримання методології (послідовності і принципів) створення АСУВ, у тому числі щодо визначення раціональної структури;

застарілість державних та галузевих стандартів щодо створення АСУ та відсутність конкретних рекомендацій стосовно створення АСУВ;

відсутність ґрунтовних вихідних даних для створення АСУВ як результат непроведення НДР за відповідною тематикою, та неефективний науковий супровід ДКР.

Використання об'єктно-функціонального методу як частини системної методології створення АСУВ дає змогу виділити основні

складові системи з більшою деталізацією та можливістю практичної реалізації – включно до визначення раціонального складу, розподілу функцій, які автоматизуються, між окремими підсистемами, окремими програмними застосуваннями та ІРЗ і моделями. Застосування методу на передпроектних і проектних стадіях створення АСУВ може суттєво зменшити кількість ітерацій та обсяг як проектних робіт, так і розроблення спеціального програмного забезпечення.

Можливі шляхи вирішення науково-технічних проблем створення АСУВ для ЗС:

Література

1. **Азаренко Е. В.** Проектирование АСУ на компьютерных сетях : монография / Е. В. Азаренко, Б. М. Герасимов, Б. П. Шохин. – Севастополь : Гос. Океанариум, 2007. – 272 с.; ил. 2. **Вознюк Ю. С.** Світові тенденції, проблеми та перспективи створення АСУВ для ЗС України / Ю. С. Вознюк, П. М. Грицай, П. І. Стужук // 36. наук. пр. ЦВСД НУОУ. – 2012. – № 1 (45). – С. 68–76. 3. **Дружинін С. В.** Сучасний стан автоматизації управління в ЗС України / С. В. Дружинін, О. К. Климович, О. Г. Саєнко // Системи озброєння і військова техніка. – 2010. – № 1 (21). – С. 60–62. 4. **Морозов А. О.** Основні проблеми інформатизації ЗС України на сучасному етапі / А. О. Морозов, Г. Є. Кузьменко, А. Д. Яровий // Наука і оборона. – 2004. – № 3. – С. 16–22. 5. **Науменко Е. М.** Формирование рационального варианта технической реализации АСУ

розроблення і розвиток методології та державних і галузевих стандартів створення АСУВ;

подальше розроблення теорії управління військами (силами) як основи вихідних даних для створення АСУВ;

використання об'єктно-функціонального методу визначення структури дослідного зразка АСУВ на передпроектних і проектних стадіях його створення;

прийняття навчальної АСУВ за базу для створення АСУВ оперативного-тактичного рівня для ЗСУ.

на предпроектных стадиях / Е. М. Науменко, Ю. Я. Самохвалов // УС и М, 2005. – №5. – С. 62–67. 6. **Нестеренко О. В.** Основи побудови автоматизованих інформаційно-аналітичних систем органів державної влади : монографія / О. В. Нестеренко. – К. : Наук. думка, 2006. – 628 с. 7. **Петухов Г. Б.** Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем / Г. Б. Перухов, В. И. Якунин. – М. : АСТ, 2006. – 504 с. 8. **Попов М. О.** Геоинформационные системы та технології в завданнях оборони й національної безпеки / М. О. Попов, Є. С. Серединин // Перспективні технології в оборонній сфері. – К. – С. 49–56. 9. **Основи** моделювання бойових дій військ: підручник / А. В. Атрохов, І. Е. Вернер, В. І. Гавалко та ін. за заг. ред. Пермякова О. Ю. – К. : НУОУ, – 2005.– 476 с.

ПРОБЛЕМЫ И РЕКОМЕНДАЦИИ ПО СОЗДАНИЮ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ВОЙСКАМИ (СИЛАМИ) ДЛЯ ВООРУЖЕННЫХ СИЛ

¹Леонид Анатолиевич Маслюк (канд. техн. наук, с.н.с.)

¹Петр Иванович Стужук (канд. воен. наук, доцент)

¹Александр Александрович Челобитченко (канд. техн. наук, с.н.с.)

²Александр Николаевич Правдивец

¹Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

²Генеральный штаб Вооруженных Сил Украины, Киев, Украина

Во время создания автоматизированных систем управления войсками (силами) (АСУВ) для вооруженных сил возникает ряд проблем. В статье проведен анализ этих проблем и на основе собственного опыта по созданию учебной АСУВ авторами предложены практические рекомендации по их преодолению. Определены основные принципы создания АСУВ: системности, развития (открытости), совмещенности, стандартизации (унификации), эффективности, первого руководителя, новых задач. Предложено функциональную структуру АСУВ определять на основании единства оперативно-стратегических, системотехнических и организационных аспектов процесса управления войсками (силами). Показано, что в основу формирования состава функциональных подсистем и информационно-расчетных задач (моделей) учебной АСУВ был положен объектно-функциональный метод. Наличие геоинформационной подсистемы есть необходимым условием существования современной АСУВ. Также показано, что, невзирая на функциональное единство органов военного управления, структуры АСУВ разных уровней и разных объектов автоматизации не идентичны между собой.

Ключевые слова: автоматизированные системы управления войсками; объектно-функциональный метод; структура автоматизированных систем управления войсками.

PROBLEMS AND RECOMMENDATIONS FOR THE CREATION AUTOMATED CONTROL SYSTEMS TROOPS (FORCES) FOR ARMED FORCES

¹Leonid A. Masliuk (Candidate of Technical Sciences, Senior Research Fellow)

¹Petro I. Stuzhuk (Candidate of Military Sciences, Associate Professor)

¹Oleksandr O. Chelobitchenko (Candidate of Technical Sciences, Senior Research Fellow)

²Oleksandr M. Pravdyvets

¹*National Defence University of Ukraine named after Ivan Cherniakhovskiy, Kyiv, Ukraine*

²*General Staff of the Armed Forces of Ukraine, Kyiv, Ukraine*

The article analyses the problems concerning establishment of automatic command and control systems for armed forces as well as suggests practical recommendations how to overcome them.

A set of problems arises during the establishment of automatic troops (forces) command and control systems of the Armed Forces. The analysis of these problems has been carried out on the basis of personal experience of training automatic troops (forces) command and control system establishment. In the article the authors proposed the practical recommendations to eliminate these problems. The main principles of automatic troops (forces) command and control system establishment are the following: consistency, development (openness), interoperability, standardization (unification), effectiveness, the first leader, new tasks. The functioning structure of automatic troops (forces) command and control system has been proposed to be defined on the basis of unity of operational and strategic, system and technical and organizational aspects of troops (forces) command and control. The objective and functional method was presented as a basis for a composition of functional subsystems and informational and calculation tasks (models) of training automatic troops (forces) command and control system. Geoinformation subsystem is a necessary condition for a modern automatic troops (forces) command and control system. It is shown that despite the functional unity of the military command and control bodies, automatic troops (forces) command and control system structures of various levels and objects of automatization are not identical.

Keywords: *automatic command and control systems; object and functional method; automatic command and control system structure.*

References

- 1. Azarenko E.V.,** Gerasimov B.M., Shokhin B.P. (2007) Design automation on computer networks. [*Proektirovanie ASU na komp'iuternykh setiakh : monografiia*], Sevastopol: Gos. Okeanarium, 272 p.
- 2. Vozniuk Yu.S.,** Hrytsai P.M., P.I. Stuzhuk (2012), Global trends, challenges and prospects for the creation ASU Armed Forces of Ukraine. [*Svitovi tendentsii, problemy ta perspektyvy stvorennia ASUV dlia ZS Ukrainy*], Zb. nauk. pr. TsVSD NUOU, No. 1 (45), pp. 68-76.
- 3. Druzhynin S.V.,** Klymowych O.K., Saienko O.H. (2010), The current state of automation in the management Armed Forces of Ukraine. [*Suchasnyi stan avtomatyzatsii upravlinnia v ZS Ukrainy*], Systemy ozbroiennia i viiskova tekhnika, No.1 (21). pp. 60-62.
- 4. Morozov A.O.,** Kuzmenko H.Ye., Yarovy A.D. (2004), The main problem of Ukraine Armed Forces of information at this stage. [*Osnovni problemy informatyzatsii ZS Ukrainy na suchasnomu etapi*], Nauka i oborona, No.3, pp. 16-22.
- 5. Naumenko E.M.** Samokhvalov I.I. (2005), Formation of a rational variant of technical implementation of ACS in the preliminary stages. [*Formirovanie ratsional'nogo varianta tekhnicheskoi realizatsii ASU na predproektnykh stadiakh*], US i M, No.5, pp. 62-67.
- 6. Nesterenko O.V.** (2006), Fundamentals of automated information systems of public authorities. [*Osnovy pobudovy avtomatyzovanykh informatsiino-analitychnykh system orhaniv derzhavnoi vlady: monografiia*], Kyiv: Nauk. dumka, 628 p.
- 7. Petukhov G.B.,** Iakunin V.I. (2006), Methodological basis of the external design of targeted processes and dedicated systems. [*Metodologicheskie osnovy vneshnego proektirovaniia tselenapravlenykh protsessov i tselestremlennykh sistem*], Moscow: AST, 504 p.
- 8. Popov M.O.,** Seredynyn Y.S., Geographic information systems and technologies in the tasks of defense and national security. [*Heoinformatsiini systemy ta tekhnologii v zavdanniakh oborony y natsionalnoi bezpeky*], Perspektyvni tekhnologii v oboronni sferi, Kyiv, pp. 49-56.
- 9. Atrokhov A.V.,** Verner I.E., Havalko V.I. (2005), Based simulation of fighting forces, tutorial. [*Osnovy modeliuвання boiovykh dii viisk: pidruchnyk*], ta in. za zah. red. Permiakova O.Yu., Kyiv: NUOU, 476 p.

Отримано: 13.05.2016 року.

МЕТОДИКА АВТОМАТИЗОВАНОГО РОЗРАХУНКУ ПАРАМЕТРІВ ЧАСТОТНОЇ МАНІПУЛЯЦІЇ В УМОВАХ АПРІОРНОЇ НЕВИЗНАЧЕНОСТІ

У статті запропоновано методику автоматизованого розрахунку несучої частоти, ширини спектра, символної швидкості, кількості на номіналів піднесучих радіосигналів із частотною маніпуляцією в умовах відсутності апріорної інформації про параметри сигналу та комунікаційного каналу. Методика ґрунтується на аналізі спектральних, ймовірнісних та циклостаціонарних характеристик миттєвих значень параметрів сигналу. Приводяться залежності відносної похибки визначення вказаних параметрів від відношення сигнал/шум.

Ключові слова: методика; автоматизація; частотна маніпуляція; радіосигнал; параметр; вимірювання; невизначеність.

Вступ

Постановка проблеми. Одним із основних завдань, що вирішуються у системах радіомоніторингу та радіоконтролю, є визначення параметрів радіосигналів [1, 2]. Реалізація даного завдання є необхідною передумовою для якісного виконання наступних етапів радіоконтролю: пеленгування, ідентифікації, демодуляції, декодування тощо. Збільшення кількості видів сигнально-кодових конструкцій, що використовуються в радіосигналах сучасних телекомунікаційних систем, та розширення діапазону можливих значень модуляційних параметрів обумовлюють необхідність розвитку існуючих методів аналізу радіосигналів і автоматизації процесів обробки з метою підвищення продуктивності праці оператора та зниження впливу людського чинника на результати вимірювань [1].

У сучасних цифрових телекомунікаційних системах широко застосовуються радіосигнали з багатопозиційною частотною маніпуляцією (ЧМн), яким властива висока енергетична ефективність, перешкодостійкість та які не потребують складних алгоритмів обробки на приймальній стороні [3]. Основними параметрами таких радіосигналів, що підлягають визначенню, є несуча частота, ширина спектра, частота рознесення піднесучих, символна швидкість та кратність маніпуляції [1,2]. При цьому, для забезпечення більш ефективного використання обчислювальних ресурсів системи радіоконтролю параметри повинні визначатися комплексно, оскільки їх розрахунок передбачає виконання ряду ідентичних операцій [4]. Автоматизований процес обробки має передбачати вибір оператором необхідної ділянки радіосигналу, що підлягає аналізу, запуск процедур автоматичного визначення параметрів та отримання результатів. Таким чином, актуальним науковим і практичним завданням є удосконалення існуючих методів та

розробка методики автоматизованого визначення параметрів ЧМн радіосигналів в умовах відсутності апріорної інформації.

Аналіз останніх досліджень і публікацій. Для визначення параметрів ЧМн радіосигналів в умовах апріорно параметричної невизначеності запропоновано ряд алгоритмів, які використовують характеристики амплітудно-частотного спектру (АЧС) [5], параметри функції миттєвої частоти [5,7], гістограму миттєвої частоти [6], характеристики переходу радіосигналу через "нуль" [7] та циклостаціонарні властивості цифрових видів модуляції [8-10]. Перші три підходи досить просто реалізуються, однак точність визначення ними параметрів сильно залежить від відношення сигнал/шум (ВСШ), характеристик фільтрів, що використовуються для зменшення флуктуацій в АЧС та миттєвій частоті, а також обраних порогів прийняття рішення. Підходи, що ґрунтуються на циклостаціонарних властивостях ЧМн радіосигналу мають меншу похибку визначення параметрів при низьких значеннях ВСШ, але їх розрахункова складність досить висока, а кількість параметрів, що визначаються обмежена. Загальним недоліком відомих підходів є необхідність наявності (або часткової наявності) апріорної параметричної інформації та відсутність комплексної методики щодо визначення основних параметрів ЧМн.

Метою даної статті є розробка методики автоматизованого розрахунку основних параметрів радіосигналів із багатопозиційною ЧМн в умовах апріорної невизначеності.

Постановка завдання досліджень. Вважається, що сигнал на передавальній стороні сформовано відповідно до визначених вимог [3], він не комбінований та має один із видів багатопозиційної ЧМн. Параметри маніпуляції на ділянці сигналу, що аналізується, постійні, а попередня інформація про їх можливі значення відсутня, що відповідає умовам апріорної параметричної невизначеності.

При розповсюдженні сигнал зазнає впливу каналу, що описується гауссівською моделлю [3, 4]. У такому разі прийнята сигнальна суміш $r(t, U_i)$ складається з корисного сигналу $s(t, U_i)$ та адитивного гауссівського шуму $n(t)$ [7]:

$$r(t, U_i) = s(t, U_i) + n(t), \quad (1)$$

де $U_i = [a \ f_c \ \theta \ R_s \ f_r \ g(t) \ M \ \{f_k\}_{k=1}^M]$ – вектор апріорно невідомих параметрів сигналу;

a – амплітуда сигналу;

f_c – частота несучого коливання;

θ – початкова фаза несучого коливання;

$R_s = 1/T$ – символна швидкість;

f_r – частота рознесення піднесучих ЧМн;

$g(t)$ – імпульсна характеристика формуючого фільтра;

M – кратність маніпуляції;

$\{f_k\}_{k=1}^M$ – частоти піднесучих кінцевого алфавіту ЧМн.

Корисний сигнал для нелінійних цифрових видів модуляції описується виразом [11]:

$$s(t, U_i) = a e^{j(2\pi f_c t + \theta)} e^{j\phi_i(t, f_k)}, \quad (2)$$

де $\phi_i(t, f_k)$ – функція миттєвої фази інформаційної складової, що змінюється за рахунок кутової модуляції та для багатопозиційної ЧМн визначається виразом

$$\phi_{\text{ЧМн}}(t, f_k) = \sum_{k=1}^K 2\pi f_k g(t - kT); \quad (3)$$

$$f_k \in \left\{ (2m - 1 - M) \frac{f_r}{2}, m = 1, \dots, M \right\}, k = 1, \dots, K.$$

Вважається, що апріорна інформація про параметри ЧМн сигналу, що описуються вектором U_i , відсутня. Необхідно автоматично визначити несучу частоту радіосигналу f_c , ширину спектра ΔF , частоту рознесення піднесучих f_r , символну швидкість R_s та кратність маніпуляції M .

Виклад основного матеріалу дослідження

Відомо, що АЧС ЧМн радіосигналу має ряд ділянок на яких зосереджено переважна частина його енергії [3]. Такі ділянки спектру розташовані навколо частот піднесучих та в більшості випадків розрізняються візуально при аналізі АЧС (рис. 1).

Визначення ширини спектру радіосигналу ΔF на основі аналізу АЧС здійснюється шляхом порівняння амплітуди спектральних компонент із встановленим пороговим рівнем [1]. Для зменшення впливу шумових складових на результати розрахунку АЧС згладжується фільтром ковзного середнього.

Ширина спектра ЧМн радіосигналу, відповідно до енергетичного підходу, обмежується таким математичним виразом [1]:

$$\int_{-\Delta F/2}^{\Delta F/2} |S(f)|^2 df = k_k \int_0^{\infty} |S(f)|^2 df, \quad (4)$$

де $k_k = 0.9 \dots 0.99$ – коефіцієнт якості подання сигналу, значення якого встановлюється залежно від цільових задач обробки;

$S(f)$ – спектральна щільність радіосигналу.

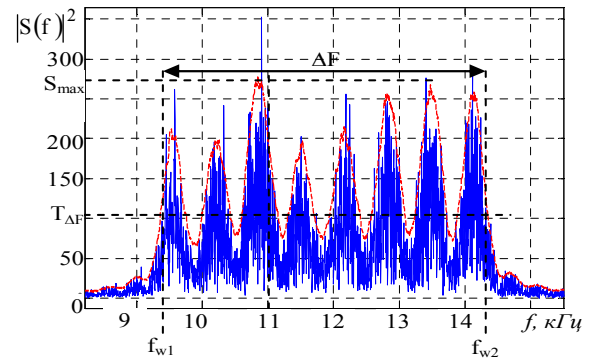


Рис. 1. АЧС радіосигналу із восьмипозиційною ЧМн

На практиці, в більшості випадків, ширину спектра ЧМн радіосигналу визначають за спаданням амплітуди спектральних складових до рівня $1/\sqrt{2}$ (за напругою) та до рівня $1/2$ (за потужністю), що відповідає значенню -3 дБ [1].

Беручи до уваги вище зазначене, автоматизований розрахунок ширини спектра ЧМн радіосигналу має включати таку послідовність операцій:

розрахунок згладженого АЧС та визначення його максимального значення S_{max} ;

розрахунок порогу прийняття рішення $T_{\Delta F} = S_{\text{max}} - 3$ (дБ);

пошук спектральних гармонік, амплітуда яких перевищує поріг ($S(f_{w1}) > T_{\Delta F}$, $S(f_{w2}) > T_{\Delta F}$) та визначення їх частот f_{w1} , f_{w2} (рис. 1);

розрахунок ширини спектра як різниці його граничних частот:

$$\Delta F = f_{w2} - f_{w1}. \quad (5)$$

Несуча частота ЧМн радіосигналу розраховується як середнє арифметичне значення частот піднесучих $f_{sc}(i)$ (рис. 1):

$$f_c = \frac{1}{M} \sum_{i=1}^M f_{sc}(i), \quad (6)$$

де $f_{sc}(i)$ – частота i -ї піднесучої ЧМн радіосигналу;

Частота рознесення піднесучих ЧМн радіосигналу f_r визначається як усереднена різниця частот піднесучих коливань:

$$f_r = \frac{1}{M-1} \sum_{i=1}^{M-1} (f_{sc}(i+1) - f_{sc}(i)). \quad (7)$$

Визначення частот піднесучих коливань $f_{sc}(i)$ радіосигналу з багатопозиційною ЧМн реалізується на основі методу оцінювання спектральної щільності потужності – модифікованої періодограми Уелча [12]. Суть даного методу полягає в утворенні псевдоансамблю періодограм за рахунок розділення аналізованого радіосигналу $r(n)$ на сегменти, що перекриваються, та обробки кожного сегменту за допомогою вікна даних. Якщо дискретний сигнал $r(n)$, $0 \leq n \leq N-1$ розбити на P сегментів по D відліків в кожному із зсувом на S відліків між сусідніми сегментами ($S \leq D$), то максимальне число сегментів буде ціла частина величини $(N - D)/S + 1$. Тоді після

зважування вікном даних $w[n]$, сегмент з номером p буде включати наступні відліки [12]:

$$r^{(p)}(n) = w(n)r(n + pS), 0 \leq n \leq D - 1. \quad (8)$$

Вибірковий АЧС p -го сегменту визначається виразом:

$$P_{xx}^{(p)}(f) = \frac{F_s}{UD} |S^{(p)}(f)|^2, \quad (9)$$

де F_s – частота дискретизації;

$S^{(p)}(f)$ – дискретне віконне перетворення Фур'є p -го сегменту

$$S^{(p)}(f) = \frac{1}{F_s} \sum_{n=0}^{D-1} r^{(p)}(n) e^{-j2\pi fn / F_s}; \quad (10)$$

U – енергетична складова вікна даних:

$$U = \frac{1}{F_s} \sum_{n=0}^{D-1} w^2(n). \quad (11)$$

Тоді модифікована періодограма Уелча, як середнє значення сегментних періодограм, визначається за виразом:

$$P_{we}(f) = \frac{1}{P} \sum_{p=0}^{P-1} P_{xx}^{(p)}(f). \quad (12)$$

Оцінка щільності спектральної потужності з використанням модифікованої періодограми Уелча є асимптотично незміщеною і при цьому консистентною за рахунок ділення сигнальної послідовності на сегменти, що перекриваються, та усереднення періодограм сегментів [12]. Практичні дослідження показали, що застосування до сигналу нелінійного оператора другого порядку зменшує кількість хибних максимумів в періодограмі, в результаті чого підвищується ймовірність правильної ідентифікації спектральних компонентів на частотах піднесучих коливаний.

Модифікована періодограма Уелча радіосигналу з восьмипозиційною ЧМн піднесеного до другого степеня зображена на рис. 2.

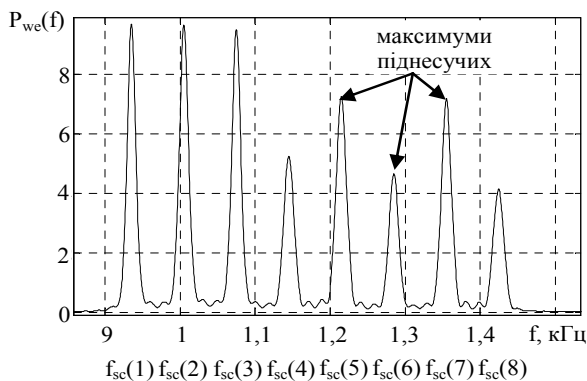


Рис. 2 Модифікована періодограма Уелча радіосигналу з восьмипозиційною ЧМн піднесеного до другого степеня

З рис. 2 видно, що модуль оціненої щільності спектральної потужності має вісім домінантних максимумів розміщених на частотах піднесучих радіосигналу $f_{sc}(i)$. Розрахувавши частоти розміщення таких максимумів та їх кількість визначаються частоти піднесучих $f_{sc}(i)$ та кратність маніпуляції M .

Для підвищення ймовірності правильного визначення кількості піднесучих використовується метод, що ґрунтується на аналізі гістограми миттєвої частоти ЧМн $f_N(k)$ радіосигналу [6]:

$$f_N(k) = \frac{F_s}{2\pi} (\phi_W(k+1) - \phi_W(k)), \quad (13)$$

де $\phi_W(k)$ – розгорнута фаза k -го комплексного відліку радіосигналу.

Осцилограма миттєвої частоти радіосигналу з восьмипозиційною ЧМн зображена на рис. 3.

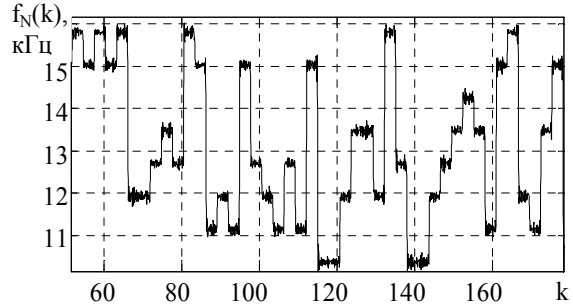


Рис. 3. Осцилограма миттєвої частоти радіосигналу з ЧМн-8

З рис. 3 видно, що частота на осцилограмі змінюється стрибкоподібно між 8-ми рівнями. Отже, гістограма миттєвої частоти матиме максимуми, що відповідатимуть частотам рознесення піднесучих. Приклад згладженої гістограми миттєвої частоти радіосигналу з восьмипозиційною ЧМн зображено на рис. 4.

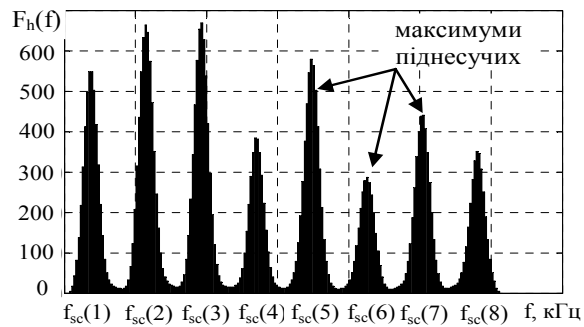


Рис. 4. Гістограма миттєвої частоти радіосигналу з восьмипозиційною ЧМн

На рис. 4 добре видно вісім піків, які знаходяться на частотах піднесучих коливаний, що дозволяє визначатися кратність маніпуляції M та “грубе” значення частот піднесучих коливаний. Точність визначення частоти рознесення піднесучих ЧМн з використанням гістограми миттєвої частоти є нижчою у порівнянні з підходом на основі метода модифікованої періодограми Уелча та залежить від кількості інтервалів розбиття значень миттєвої частоти N_h . Однак порівняння розрахованих даним методом частот піднесучих та кратності маніпуляції із результатами, отриманими на основі модифікованої періодограми Уелча, дає можливість відкинути хибні максимуми в періодограмі та підвищити точність визначення параметрів ЧМн радіосигналу.

Для визначення символної швидкості застосовано підхід, що ґрунтується на пошуку циклостационарних властивостей випадкової функції миттєвої частоти [13]. Його суть полягає в пошуку спектральних гармонік в АЧС комплексної нормованої центрованої функції миттєвої частоти, що відповідають циклостационарним процесам, пов'язаним із ЧМн. Комплексне значення нормованої центрованої миттєвої частоти розраховується за виразом [13]:

$$f_{NC}(k) = \frac{f_{NA}(k)}{E(f_{NA}(k))} - 1, \quad (14)$$

де $f_{NA}(k) = f_N(k) + f_N(k) h_H(n)$ – комплексне значення миттєвої частоти;

$h_H(n)$ – імпульсна характеристика цифрового фільтра Гільбера;

$E(\cdot)$ – операція статистичного усереднення.

В АЧС модуля нормованої центрованої миттєвої частоти

$$S_{NC}(n) = (\text{FFT}(f_{NC}(k)))^2 \quad (15)$$

присутні домінуючі гармоніки на частотах кратних символній швидкості (рис. 5).

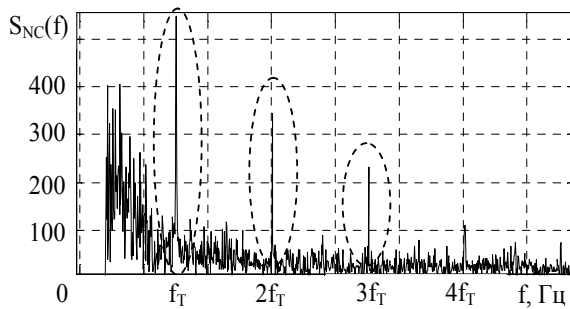


Рис. 5. АЧС комплексної нормованої центрованої функції миттєвої частоти

У більшості випадків гармоніка з максимальною амплітудою розміщена на частоті маніпуляції f_T . Решта домінуючих гармонік мають частоту, кратну символній швидкості. Детально алгоритм пошуку домінуючих гармонік символної швидкості описано в [13].

Таким чином, методика автоматизованого розрахунку параметрів ЧМн в умовах апріорної невизначеності складається із наступних етапів:

розрахунок АЧС та визначення ширини спектра ΔF ;

оцінювання спектральної щільності радіосигналу піднесеного до другого степеня на основі модифікованої періодограми Уелча та пошук частот піднесених коливань $f_{sc}(i)$;

розрахунок функції миттєвої частоти радіосигналу $f_N(k)$;

побудова гістограми миттєвої частоти та пошук частот піднесених коливань $f_{sc}(i)$;

визначення несучої частоти f_c , частоти рознесення піднесених f_r , кратності маніпуляції M ;

розрахунок АЧС комплексної нормованої центрованої функції миттєвої частоти та визначення символної швидкості R_s .

Отримані різними підходами значення параметрів ЧМн дозволяють в подальшому оцінити правильність їх визначення спираючись на властивості даного виду цифрової модуляції. Зокрема можна виділити такі характеристики ЧМн.

Ширина спектра ЧМн близька до значення [14]:

$$\begin{aligned} 1,3(M-1)f_r + 1,4R, 2 \leq m_f \leq 8; \\ 1,1(M-1)f_r + 3,1R, 8 < m_f \leq 20, \end{aligned} \quad (16)$$

де m_f – індекс частотної маніпуляції.

Частота рознесення піднесених більше символної швидкості $f_r > R_s$.

Різниця сусідніх частот рознесення піднесених коливань є постійною величиною:

$$f_{sc}(i+1) - f_{sc}(i) \approx f_{sc}(i+2) - f_{sc}(i+1). \quad (17)$$

Взявши до уваги вказані властивості можна оцінити правильність визначення модуляційних параметрів та, при необхідності, змінити порогові прийняття рішення під час пошуку спектральних піків.

Перевірку правильності роботи та ефективності розробленої методики автоматизованого розрахунку параметрів ЧМн в умовах апріорної невизначеності здійснено відповідно до вимог статистичного моделювання та методів Монте-Карло [15] в програмному середовищі MATLAB 2012b. Сигнальні суміші формувались шляхом генерування радіосигналів із багатопозиційною ЧМн та додавання до них шуму, ймовірнісна модель якого описувалась нормальним законом розподілу ймовірностей. Відношення сигнал/шум (ВСШ) змінювалось у діапазоні від -10 до 15 дБ з дискретністю 1 дБ. Модуляційні параметри сигналу кожної реалізації обирались за випадковим законом. Для кожного значення ВСШ та кратності маніпуляції проведено 300 розрахунків параметрів радіосигналів. У результаті статистичного моделювання отримано графічні залежності відносної похибки визначення несучої частоти, символної швидкості, частоти рознесення піднесених, а також ймовірності правильного розпізнавання кратності маніпуляції від ВСШ (рис. 6, 7).

Проаналізувавши результати моделювання, можна зробити висновок, що похибки визначення несучої частоти та частоти рознесення піднесених збільшуються при підвищенні кратності маніпуляції. Це пов'язано із зростанням кількості хибних піків в модифікованій періодограмі Уелча та "розмиттям" гістограми миттєвої частоти. Однак при ВСШ більше 5 дБ розроблена методика забезпечує необхідну точність визначення параметрів для здійснення наступних операцій з ідентифікації типу передачі та частотної демодуляції.

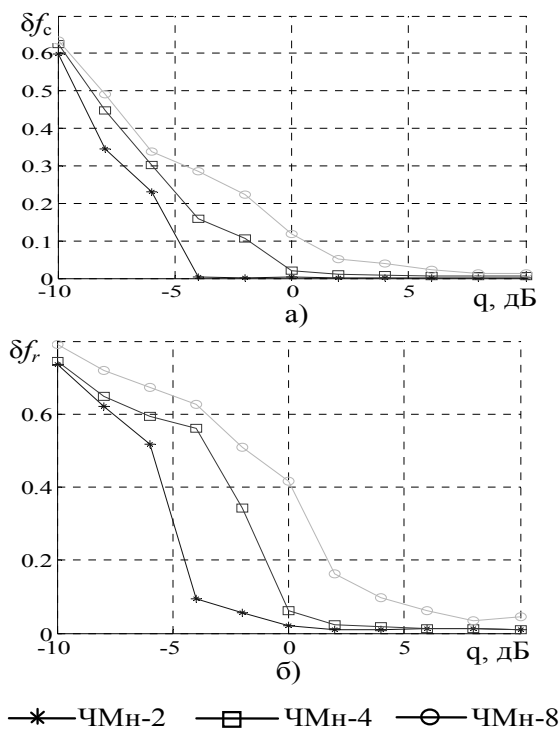


Рис. 6. Залежності відносних похибок визначення несучої частоти (а), частоти рознесення піднесучих (б) ЧМн радіосигналів від ВСШ

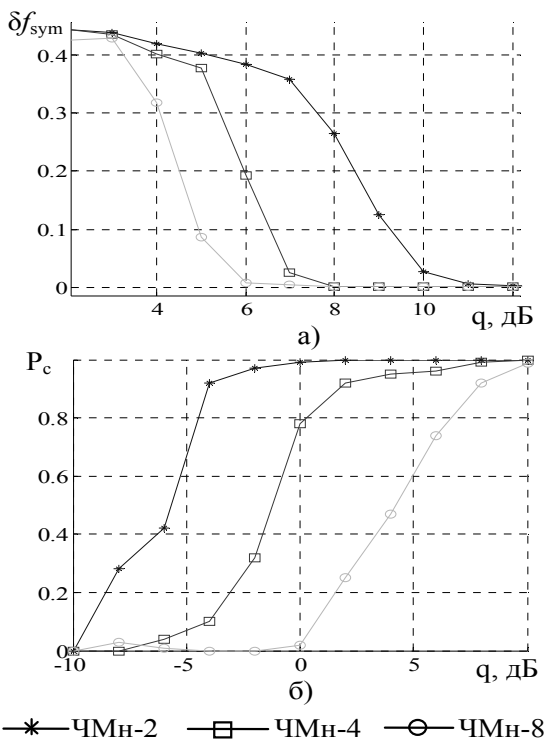


Рис. 7. Залежності відносної похибки

Література

1. Рембовский А. М. Радиомониторинг: задачи, методы, средства / А. М. Рембовский, А. В. Ашихмин, В. А. Козьмин 3-е изд., перераб. и доп. – М.: Горячая линия – Телеком, 2012. – 640 с.
 2. Слободянюк П. В. Радиомониторинг: вчера, сегодня,

визначення символної швидкості (а) та ймовірності правильного визначення кратності маніпуляції (б) ЧМн радіосигналів від ВСШ

При розрахунку символної швидкості підвищення кратності маніпуляції приводить до зменшення похибки її визначення. Однак точність визначення символної швидкості сильно залежить від ВСШ, особливо при застосуванні двопозиційної ЧМн. З рис. 7 (б) видно, що ймовірність правильного визначення кратності маніпуляції близька до одиниці для двопозиційної та чотирипозиційної ЧМн при ВСШ від 5 дБ та для восьмипозиційної ЧМн при ВСШ від 10 дБ.

Комп'ютерне моделювання показало, що для підвищення точності визначення параметрів необхідно удосконалювати алгоритми пошуку доміантних гармонік в АЧС та максимумів в гістограмі із врахуванням можливих математичних співвідношень між різними параметрами. Окрім того похибка визначення параметрів залежить від розміру вибірок радіосигналу, що аналізується, особливо при великих значеннях кратності маніпуляції.

Висновки й перспективи подальших досліджень

Розроблено методу автоматизованого визначення ширини спектру, частоти несучого колювання, частоти рознесення піднесучих, символної швидкості та кратності маніпуляції радіосигналів з багатопозиційною ЧМн в умовах апріорної параметричної невизначеності. Методика забезпечує комплексне визначення вказаних параметрів, що дозволяє підвищити продуктивність праці оператора та підвищити пропускну здатність посту радіомоніторингу.

Наступні дослідження в даному напрямку доцільно спрямувати на удосконалення алгоритмів пошуку спектральних складових, частоти яких математично пов'язані із шуканими параметрами ЧМн, а також на оцінювання ефективності розробленої методики при роботі із сигналами, спотвореними шумами, закон розподілу яких не є гауссівським, та ефектом багатопроменевого розповсюдження.

завтра (Теория и практика построения системы радиомониторинга) / П. В. Слободянюк, В. Г. Благодарный. – Прилуки: ООО “Издательство “Аир-полиграф”, 2010. – 296 с.
 3. Скляр Б. Цифровая связь. Теоретические основы и практическое

применение / Б. Скляр. – М.: Издательский дом “Вильямс”, 2003. – 1104 с. **4. Benvenuto N.** Algorithms for communications systems and their applications / N. Benvenuto, G. Cherubini, – Chichester: John Wiley & Sons, 2003. – 1285 p. **5. Azzouz E. E.** New techniques for the baud duration estimation / E. E. Azzouz, A. K. Nandi // Proceedings of EUSIPCO-96. – Lint Trieste, Italy, 1996. – P. 639–642. **6. Xiong H.** Parameter estimation approach of FSK/PSK Radar Signal / H. Xiong, D. Zeng, X. He, B. Tang. – Journal of electronic science and technology. Vol. 8. – China, 2010. – Num. 4. – P. 341–345. **7. Grimaldi D.** Automatic modulation classification and measurement of digitally modulated signals / D. Grimaldi, A. Palumbo, S. Rapuano // 11 IMEKO TC-4 Symp. Trends in Electrical Measurement and instrumentation. – Lisbon, 2001. – P. 112–116. **8. Hsue S. Z.** Automatic modulation classification using zero crossing / S. Z. Hsue, S. S. Soliman // IEE Radar and Signal Processing, 1990. – P. 459–464. **9. Dobre O. A.** Joint Signal detection and classification based on first-order cyclostationarity for cognitive radios / O. A. Dobre, S. Rajan, R. Inkol // EURASIP journal on

advances in signal processing. – Hindawi Publishing Corporation, 2009. – 12 p. **10. Vito L.** Joint classification and parameter estimation of compressive sampled FSK signals / L. De Vito, O. A. Dobre // 20th IMEKO TC4 international symposium and 18th international workshop on ADC modelling and testing. – Benevento, 2014. – pp. 473–477. **11. Сергиенко А. Б.** Цифровая связь / А. Б. Сергиенко. – СПб.: ГЭТИ “ЛЭТИ”, 2012. – 164 с. **12. Сергиенко А. Б.** Цифровая обработка сигналов / А. Б. Сергиенко. – СПб.: Питер, 2011. – 758 с. **13. Нагорнюк О. А.** Покращення точності оцінювання несучої та символної частоти сигналів з цифровою модуляцією / О. А. Нагорнюк, В. В. Павлюк // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. пр. – Житомир, ЖВІ ДУТ, 2015. – Вип. 10. – С. 132-140 **14. Recommendation** ITU-R SM.328-11. Spectra and bandwidth of emissions, 2006. – 91 p. **15. Mikhailov G. A.** Parametric estimates by the Monte Carlo method / G. A. Mikhailov. – Netherlands, Utrecht: VSP, 1999. – 376 p.

МЕТОДИКА АВТОМАТИЗИРОВАННОГО РАСЧЁТА ПАРАМЕТРОВ ЧАСТОТНОЙ МАНИПУЛЯЦИИ В УСЛОВИЯХ АПРИОРНОЙ НЕОПРЕДЕЛЕННОСТИ

*Александр Анатольевич Нагорнюк (канд. техн. наук)
Владимир Владимирович Павлюк (канд. техн. наук, с.н.с.)*

Житомирский военный институт имени С. П. Королева, Житомир, Украина

В статье предложена методика автоматизированного расчета несущей частоты, ширины спектра, символной скорости, количества и номиналов поднесущих радиосигналов с частотной манипуляцией в условиях отсутствия априорной информации о параметрах сигнала и коммуникационного канала. Методика основывается на анализе спектральных, вероятностных и циклоstationарных характеристик мгновенных значений параметров сигнала. Приводятся зависимости относительной погрешности определения указанных параметров от отношения сигнал / шум.

Ключевые слова: методика; автоматизация; частотная манипуляция; радиосигнал; параметр; измерения; неопределенность.

PROBLEMS AND RECOMMENDATIONS ON CREATION OF AUTOMATED COMMAND AND CONTROL SYSTEMS FOR ARMED FORCES

*Oleksandr A. Nahorniuk (Candidate of Technical Sciences)
Volodymyr V. Pavliuk (Candidate of Technical Sciences, Senior Research Fellow)*

Zhytomyr Military Institute named after S. P. Korolyov, Zhytomyr, Ukraine

The method of automated calculation of the carrier frequency, spectrum width, symbol rate, the number and values of subcarriers of the frequency shift keying radio signals in the absence of a priori information about signal parameters and the communication channel is proposed in the article. The spectral width determination is based on the energy criterion which is implemented in the frequency domain.

Carrier frequency and the frequency shift are calculated on basis of subcarriers values which are estimated using two different approaches. The first approach is based on an analysis of the energy spectrum characteristics estimated by method of Welch modified periodogram. The second approach uses the features of the instantaneous histogram which has peaks on the subcarrier frequencies.

Symbol rate is determined by analyzing the cyclostationary properties of instantaneous frequency function. The amplitude-frequency spectrum of module of such function contains harmonics which frequencies are multiples of the symbol rate value.

In order to ensure more efficient use of computing resources of radio monitoring system the parameters of frequency shift keying are determined by a complex as their calculation involves the implementation of identical operations.

In the article are given the relative error in the determination of parameters dependence of on the signal/noise ratio.

Keywords: method; automation; frequency shift keying; radio signal; parameter; estimation; uncertainty.

References

1. Rembovskij A.M., Ashihmin A.V., Koz'min V.A. (2012), Radio monitoring: tasks, methods, tools. [*Radiomonitoring: zadachi, metody, sredstva*], 3-e izd., pererab. i dop., Moscow: Gorjachaja linija, Telekom, 640 p.
2. Slobodjanjuk P.V., Blagodarnyj V.G. (2010), Radio monitoring: yesterday, today and tomorrow (theory and practice of construction of radio monitoring system). [*Radiomonitoring: vchera, segodnja, zavtra (Teorija i praktika postroenija sistemy radiomonitoringa)*], Priluki: OOO "Izdatel'stvo "Air-poligraf", 296 p.
3. Skljар B. (2003), Digital communication. Theoretical bases and practical application. [*Cifrovaja svjaz'. Teoreticheskie osnovy i prakticheskoe primenenie*], Moscow: Izdatel'skij dom "Vil'jams", 1104 p.
4. Benvenuto N. (2003), Algorithms for communications systems and their applications, G. Cherubini, Chichester: John Wiley & Sons, 1285 p.
5. Azzouz E.E., Nandi A.K. (1996), New techniques for the baud duration estimation, Proceedings of EUSIPCO-96, Lint Trieste, Italy, pp. 639-642.
6. Xiong H. (2010), Parameter estimation approach of FSK/PSK Radar Signal, D. Zeng, X. He, B. Tang, Journal of electronic science and technology. Vol. 8, China, No.4, pp. 341-345.
7. Grimaldi D. (2001), Automatic modulation classification and measurement of digitally modulated signals, D. Grimaldi, A. Palumbo, S. Rapuano, 11 IMEKO TC-4 Symp. Trends in Electrical Measurement and instrumentation, Lisbon, pp. 112-116.
8. Hsue S.Z., Soliman S.S. (1990), Automatic modulation classification using zero crossing, IEE Radar and Signal Processing, pp. 459-464.
9. Dobre O.A. Rajan S., Inkol R. (2009), Joint Signal detection and classification based on first-order cyclostationarity for cognitive radios EURASIP journal on advances in signal processing, Hindawi Publishing Corporation, 12 p.
10. Vito L., Dobre O.A. (2014), Joint classification and parameter estimation of compressive sampled FSK signals, 20th IMEKO TC4 international symposium and 18th international workshop on ADC modelling and testing, Benevento, pp. 473-477.
11. Sergienko A.B. (2012), Digital communication. [*Cifrovaja svjaz'*], Spb.: GJeTI "LETI", 164 p.
12. Sergienko A.B. (2011), Digital signal processing. [*Cifrovaja obrabotka signalov*], Spb.: Piter, 758 p.
13. Nagornjuk O.A., Pavljuk V.V. (2015), Improving the accuracy of estimation of the carrier and symbol frequency signals with digital modulation problems creating, testing, use and maintenance of complex information systems. [*Pokrashchennia tochnosti otsiniuvannia nesuchoi ta symvolnoi chastoty syhnaliv z tsyfrovoiu moduljatsiieiu, Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system*], Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system: zb. nauk. pr., Zhytomyr: ZhVI DUT, No.10, pp. 132-140.
14. Recommendation ITU-R SM.328-11. Spectra and bandwidth of emissions, (2006), 91 p.
15. Mikhalov G.A. (1999), Parametric estimates by the Monte Carlo method, Netherlands, Utrecht: VSP, 376 p.

Отримано: 06.06.2016 року.

УДК 65.012.8

¹В'ячеслав Володимирович Овсянніков (канд. техн. наук)¹Світлана Анатоліївна Паламарчук¹Юрій Олександрович Процюк¹Роман Михайлович Штонда²Сергій Миколайович Островський¹Військовий інститут телекомунікацій та інформатизації, Київ, Україна²Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

АНАЛІЗ АЛГОРИТМІВ ОБРОБКИ ЛОГІЧНИХ СИГНАЛІВ ЗАСОБІВ ВИЯВЛЕННЯ ОХОРОННОЇ СИГНАЛІЗАЦІЇ

Основними тактико-технічними характеристиками, які визначають функціональну ефективність (сигналізаційну надійність) системи збору, обробки, відображення і документування інформації, є імовірність правильного виявлення порушника. Існуючі системи збору, обробки, відображення і документування інформації щодо аналізу сигналів виявлення від засобів виявлення можна класифікувати: на рівні логічних сигналів (сигналів "тривога" з виходів засобів виявлення); на рівні аналогових сигналів з виходів граничних пристроїв засобів виявлення; на рівні оцінок параметрів порушника (зріст, вага, довжина та частота кроку, швидкість руху та ін.).

Розглядаються основні алгоритми виявлення логічних сигналів технічних засобів охоронної сигналізації щодо функціональної ефективності засобів виявлення згідно заданого алгоритму та формування сигналу тривоги, яка визначається імовірністю правильного виявлення порушника та середнім напрацюванням на хибну тривогу, що при комбінванні декількох засобів виявлення потребує визначення їх взаємного впливу та зменшення хибних тривог. Запропоновано варіант оцінки ефективності комбінованих засобів виявлення на основі присвоєння вагових коефіцієнтів. Критерії дозволяють виділити найбільш значущі завадові фактори, яким необхідно приділяти особливу увагу при загальному налаштуванні технічних засобів охоронної сигналізації.

Ключові слова: технічні засоби охоронної сигналізації; комбіновані засоби виявлення; алгоритм обробки логічних сигналів; вага засобів виявлення.

Вступ

З метою ефективного виявлення порушника і забезпечення контролю доступу на об'єкт силами охоронної сигналізації використовуються різноманітні технічні засоби охоронної сигналізації (ТЗОС) периметра об'єкта. До складу

ТЗОС входять: засоби виявлення (ЗВ); система збору, обробки, відображення і документування інформації (СЗОВДІ); додаткові пристрої (ДП) – системи електроживлення, освітлення периметру, оповіщення і т. ін. (рис.1.) [1].

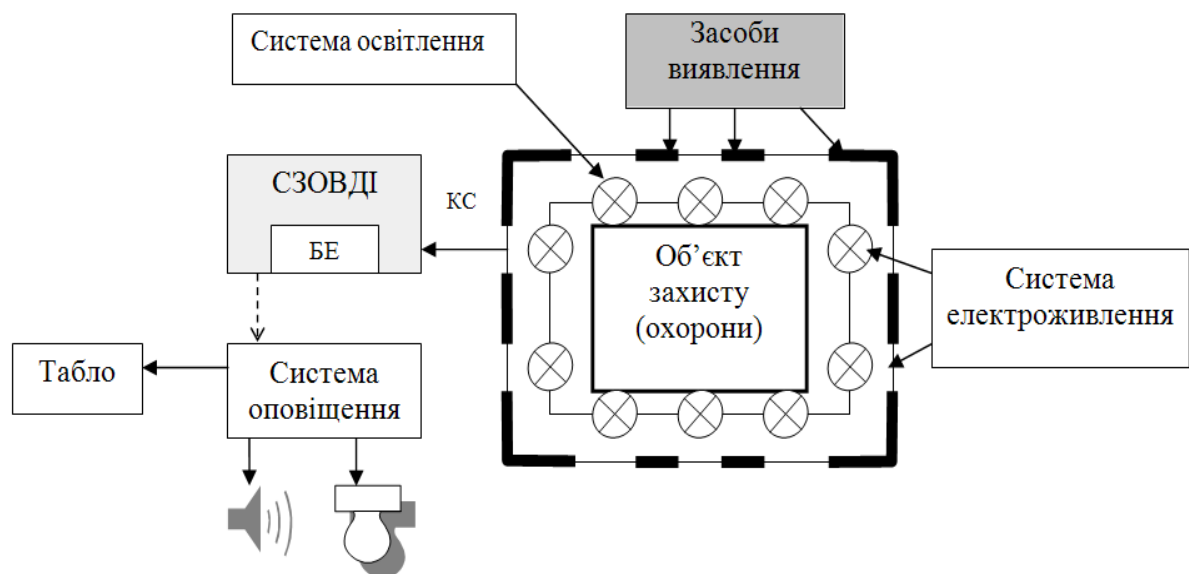


Рис. 1. Склад ТЗОС об'єкта захисту (варіант)

Засоби виявлення за допомогою чутливих елементів (ЧЕ) формують вздовж периметра охорони зону з фізичним полем, що контролюється, зміна стану якого перетворюється в електричний корисний сигнал (КС). Електронний блок (БЕ) СЗОВДІ сприймає корисні сигнали, підсилює, фільтрує і обробляє їх відповідно до заданого алгоритму, а у випадку виконання умов формує сигнал тривоги. Найпростіший БЕ – це пороговий виявлювач (ПВ), що здійснює дискримінацію вхідного сигналу за аналоговим, часовим або цифровим параметром, наприклад, амплітудою, тривалістю та ін. Фактично, в будь-якому ЗВ використовується декілька ПВ або каналів виявлення (комбінування ЗВ), що працюють в різних фізичних полях та об'єднують логіку роботи з метою забезпечення високої сигналізаційної надійності (ефективність засобу). Виявлювачі формують так, щоб отримати відносно незалежну інформацію про порушника, відповідно, чим менша взаємозалежність виявлювачів, тим вище функціональна ефективність ЗВ [1-2].

Основними тактико-технічними характеристиками, які визначають функціональну ефективність (сигналізаційну надійність) СЗОВДІ, є **імовірність правильного виявлення порушника** P_i , де $i \in 1..N$ – кількість ЗВ, що входять до складу ТЗОС, та **середнє напрацювання на хибну тривогу** $T_{лi}$, які визначають відповідно її здатність до виявлення і завадостійкість [1, 3-4]. Обидві характеристики є взаємозалежними – з підвищенням чутливості ЗВ величина P_i зростає, а $T_{лi}$ зменшується. Критерієм СЗОВДІ щодо виявлення порушника є значення $P_i \geq 0,95$, при цьому „добрим” напрацюванням на кожну тривогу може вважатися величина $T_{лi} \geq 720$ годин [4-5]. Напрацювання визначається довготривалими випробуваннями ЗВ (не менше 6 – 12 місяців) в різних природно-кліматичних умовах, що не виходять за межі технічних умов [3].

Фактори природно-кліматичного і промислового характеру, впливаючи на ЗВ, викликають завади, які при певних умовах є причиною хибних тривог. Чим більше статистична різниця сигналів і завод, чим “контрастніше” корисні ознаки порушника, тим його виявлення відбувається з більшою сигналізаційною надійністю. По суті, ЗВ є бінарною (ТАК/НІ) інформаційно-вимірною системою розпізнавання образів порушника і заводових факторів – відповідно КС і завод.

Аналіз останніх досліджень і публікацій. У виробників ЗВ прийнято завищувати характеристику $T_{лi}$ з декількох причин, в основному за кон'юктурними міркуваннями [1, 2-4]. З іншої сторони, об'єктивна верифікація здатності виявлення також ускладнена через розбіжності в моделях поведінки потенційного порушника – різноманітні способи подолання контрольованого периметра по різному

сприймаються конкретним ЗВ [4-6]. У зв'язку з цим, ускладнено порівняння ефективності різних ЗВ одного типу, не говорячи вже про порівняння комбінованих засобів виявлення, побудованих на різних фізичних принципах. Таке порівняння для розробників дає знання які алгоритми обробки сигналів є більш ефективними (при інших рівних умовах, наприклад, вартості), а для користувачів – дозволяє виділити переважну номенклатуру технічних засобів охорони. Комбінування ЗВ, так і застосування незалежних ЗВ на рівні логічних сигналів дозволяє виділити “пріоритетні” ЗВ. При виробленні ними сигналів “тривога” в роботу включаються інші ЗВ, що дає змогу знизити потужність споживання та досягти зменшення частоти хибних тривог при збереженні імовірності виявлення. Тому роботи, пов'язані з оцінкою ефективності різних ЗВ, безумовно, актуальні. У зв'язку з цим представляє інтерес застосування оцінки ефективності, що запропонована в [1] (аналізуються багатомірні статистичні розподіли КС і завод) саме для формування комбінованих ЗВ (КЗВ).

Існуючі СЗОВДІ щодо аналізу сигналів виявлення від ЗВ можна класифікувати: на рівні логічних сигналів (сигналів “тривога” з виходів ЗВ); на рівні аналогових сигналів з виходів граничних пристроїв ЗВ; на рівні оцінок параметрів порушника (зріст, вага, довжина та частота кроку, швидкість руху та ін.).

Аналіз схем формування КЗВ свідчить, що серед розроблених систем, найбільше розповсюдження отримали схеми логічної обробки бінарних сигналів тривоги від окремих ЗВ за алгоритмом “К з N”, тобто при надходженні таких сигналів від К засобів виявлення (від одного або декількох “пріоритетних”) з N наявних, наприклад, “два з трьох”. В загальному випадку область використання алгоритму обмежується ($N > K > 2$) кількістю ЗВ, що застосовуються.

При обробці логічних сигналів від ЗВ за схемою “І” доцільним буде той варіант, коли всі ЗВ забезпечували б однакові імовірності виявлення, при цьому імовірності неправильних спрацювань повинні бути не гірше заданих. ЗВ включаються за схемою “І” з метою підвищення завадостійкості (схема відповідає значенню $K=N$).

При обробці сигналів від ЗВ за схемою “АБО” доцільно, щоб за одиницю часу співпадали величини імовірностей хибних тривог всіх ЗВ, а імовірності виявлення були б не нижче заданих. Як правило, ЗВ включаються за схемою “АБО” (схема відповідає значенню $K=1$), якщо зони виявлення окремих ЗВ не перекриваються (тобто порушник зможе подолати лише одну зону виявлення, наприклад, подолати перешкоду підкопуванням).

Функціонування всіх розроблених схем логічної обробки сигналів (“присутній чи відсутній сигнал тривоги на виході ЗВ”) для КЗВ ґрунтується на тому, що кількість ЗВ, що спрацювали протягом часу пам'яті (часу, протягом

якого повинні прийти сигнали від ЗВ) повинна досягти або перевищити задану величину K для визначеної логіки обробки ("К з N"). В цьому випадку формується загальний сигнал тривоги. Перевагою такої схеми алгоритму обробки сигналів від різноманітних ЗВ є його безумовна простота, але відсутність урахування індивідуальних особливостей і характеристик кожного окремо взятого ЗВ не дозволяє досягти найкращого співвідношення між імовірністю виявлення і імовірністю хибної тривоги КЗВ. В той же час різноманітні окремі ЗВ мають різні значення імовірностей виявлення і тривоги, у зв'язку з чим поява на виході ЗВ сигналу тривоги свідчить про появу порушника з різним ступенем достовірності для різних ЗВ. Таким чином, виникає необхідність застосувати алгоритми логічної обробки для КЗВ, які дозволяють при урахуванні індивідуальних особливостей ЗВ зменшувати імовірності хибної тривоги ЗВ при збереженні заданої імовірності виявлення. Сигнали тривоги від окремих ЗВ у цьому випадку будуть оброблятися не як однаково достовірні, і алгоритм обробки буде змінюватись в залежності від ЗВ, що застосовуються.

Метою статті є проведення аналізу алгоритмів обробки логічних сигналів від ЗВ для зменшення хибних тривог комбінованих засобів виявлення ТЗОС.

На сьогоднішній день відомі два основних алгоритми обробки логічних сигналів від засобів виявлення [5]:

1. На основі можливих комбінацій ЗВ, що спрацювали.

2. На основі присвоєння ЗВ вагових коефіцієнтів.

Для першого алгоритму характерним є те, що кожному із ЗВ відомі імовірності виявлення P_i і імовірності хибної тривоги \bar{P}_i . Поява довільної комбінації при проходженні порушника відбувається для ЗВ, що працюють на різних фізичних принципах дії і характеризується статистичною незалежністю виникнення сигналів тривоги з певною імовірністю. Існують різні можливі комбінації, що залежать від кількості ЗВ і обраного критерію вибору ("два з трьох", "три з п'яти" і т. д.), але для них характерним є виконання умови

$$\sum_{i=1}^N \Delta P_i = \sum_{i=1}^N \Delta \bar{P}_i = 1, \quad (1)$$

де ΔP_i – імовірність появи i -ої комбінації при проходженні порушника;

$\Delta \bar{P}_i$ – імовірність появи i -ої комбінації при наявності впливу завади (перешкоди).

Найкращою схемою логічної обробки сигналів від КЗВ слід вважати ту, яка при забезпеченні заданої імовірності виявлення має найменшу імовірність хибної тривоги, у зв'язку з чим для синтезу такого алгоритму можна запропонувати

наступну процедуру:

1. Розраховується співвідношення $\Delta P_i / \Delta \bar{P}_i$, яке заноситься у таблицю по мірі його зменшення.

2. З таблиці вибираються перші комбінації, які забезпечують задану імовірність виявлення.

Якщо алгоритм функціонування КЗВ побудувати таким чином, щоб саме ці комбінації приводили до формування загального сигналу тривоги, то будь-який інший алгоритм, що забезпечує не гіршу імовірність виявлення, буде мати більшу імовірність хибної тривоги, оскільки він може бути отриманий з вихідного лише шляхом виключення комбінацій з більшим відношенням внеску у імовірність виявлення до внеску у імовірність тривоги і включення комбінацій з меншим відношенням. Недолік такого алгоритму – величезна кількість комбінацій навіть для невеликої кількості ЗВ (пропорційна ступеню від кількості ЗВ).

Для другого алгоритму характерним є те, що у кожного з N розміщених на одному периметрі ЗВ формується логічний сигнал u_i , який з певною імовірністю приймає значення $u_i = 1$ (сигнал тривоги від i -го ЗВ присутній), або значення $u_i = 0$ (сигнал тривоги від i -го ЗВ відсутній). Ці сигнали характеризуються щільностями імовірностей розподілів їх появи при наявності порушника $\omega_{si}(u_i)$ і при наявності впливу завади $\omega_{pi}(u_i)$. Оскільки при наявності порушника сигнал $u_i = 1$ формується з імовірністю, що дорівнює імовірності виявлення P_i , то для щільності імовірності можна записати:

$$\omega_{si}(u_i)_{i=1,2,\dots,N} = \begin{cases} P_i & \text{при } u_i = 1 \\ 1 - P_i & \text{при } u_i = 0 \end{cases} \quad (2)$$

Аналогічно щільність імовірності при наявності впливу завади:

$$\omega_{pi}(u_i)_{i=1,2,\dots,N} = \begin{cases} \bar{P}_i & \text{при } u_i = 1 \\ 1 - \bar{P}_i & \text{при } u_i = 0 \end{cases} \quad (3)$$

де \bar{P}_i – імовірність хибної тривоги i -го ЗВ.

Використовуючи для цього алгоритму критерій Неймана-Пірсона [6], запишемо оптимальне правило рішення у вигляді:

$$\lg \frac{\omega_{si}(u_1, \dots, u_N)}{\omega_{pi}(u_1, \dots, u_N)} > C, \quad (4)$$

де $\omega_s(u_1, \dots, u_N)$ – спільна щільність імовірності сигналів від ЗВ при проходженні порушника;

$\omega_p(u_1, \dots, u_N)$ – те ж при наявності впливу завади, перешкоди;

C – довільна постійна, значення якої визначає імовірність виявлення за алгоритмом (4);

u_1, \dots, u_N – сукупність сигналів, що аналізуються.

При виконанні нерівності (4) приймається рішення про наявність порушника та формується загальний сигнал тривоги.

Оптимальність правила рішення полягає в тому, що при забезпеченні заданої імовірності

виявлення пристрою в цілому P_i (яка залежить від величини C) досягається мінімальна імовірність хибної тривоги \bar{P}_i .

Якщо всі ЗВ працюють на різних фізичних принципах дії, то сигнали, що надходять від них, статистично незалежні і правило рішення може бути представлено у вигляді:

$$\sum_{i=1}^N \lg \frac{\omega_{si}(u_i)}{\omega_{pi}(u_i)} > C$$

Після деяких перетворень і введення позначень кінцевий вигляд правила рішення можна представити у вигляді:

$$\sum_{i=1}^N V_i(u_i) > C, \quad (5)$$

$$V_i(u_i) = \lg \frac{\omega_{si}(u_i)(1 - \bar{P}_i)}{\omega_{pi}(u_i)(1 - P_i)}$$

Якщо виконується нерівність (5), то формується загальний сигнал тривоги. При цьому з (2) і (3) видно, що

$$V_i(u_i)_{i=1,2,\dots,N} = \begin{cases} q_i & \text{при } u_i = 1 \\ 0 & \text{при } u_i = 0 \end{cases}$$

де $q_i = \lg \frac{P_i(1 - \bar{P}_i)}{P_i(u_i)(1 - P_i)}$ – ваговий коефіцієнт,

постійна величина для кожного i -го ЗВ.

Значення q_i розраховуються завчасно згідно імовірності виявлення P_i та імовірності хибної тривоги \bar{P}_i i -го ЗВ (рис. 2).

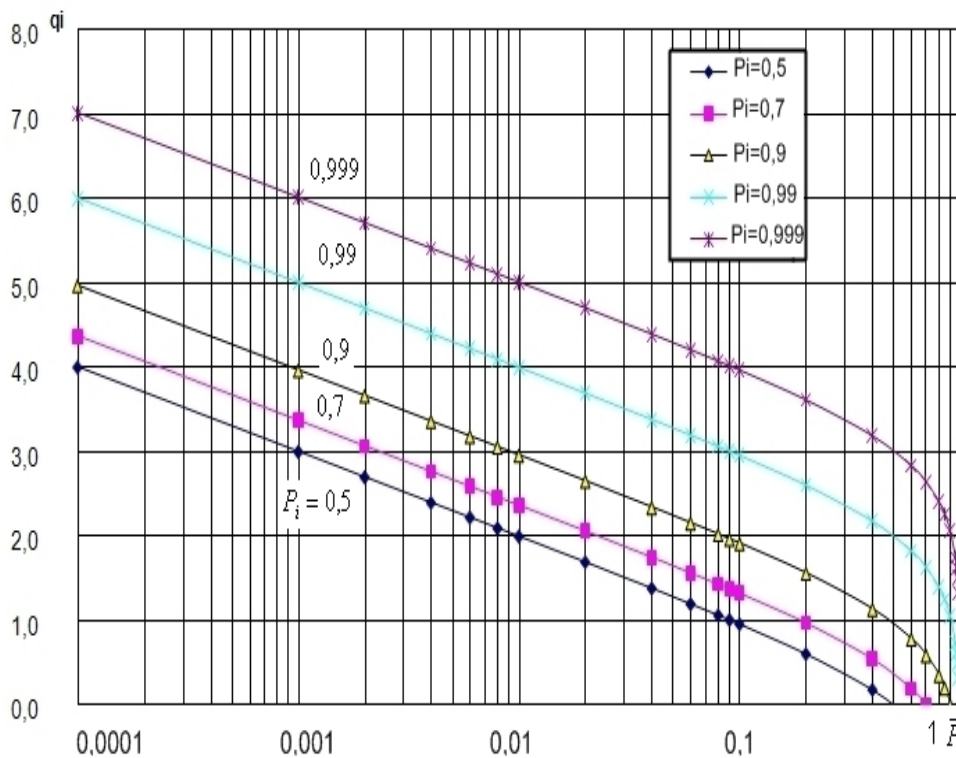


Рис. 2. Графік залежності вагових коефіцієнтів q_i від P_i та \bar{P}_i

На рис. 2. наведені графіки залежності „ваги” i -го ЗВ від його імовірностей P_i та \bar{P}_i . Видно, що „вага” ЗВ q_i тим більша, чим більша імовірність виявлення та чим менша імовірність хибної тривоги.

Вибравши критерій забезпечення заданої імовірності виявлення $P_i^{зад}$ при мінімізації імовірності хибної тривоги $\bar{P}_i \rightarrow \min$, доводиться, що відносна вага q_i може характеризувати порівняльну ефективність (якість) i -го ЗВ:

$$q_i = \lg(1/\bar{P}_i (1 - P_i)). \quad (6)$$

Чим вона більша за величиною, тим вище ефективність ЗВ. Очевидно, що інформаційний критерій (6), який володіє властивістю адитивності, не має протиріч і дозволяє визначити ($q_i \rightarrow \max$) той ЗВ, який при інших рівних умовах буде найкращим. В цьому критерії напрацювання на хибну тривогу виражене неявно, „ховаючись” за величиною \bar{P}_i . Для випадку, коли імовірність \bar{P}_i невідома, в якості критерію якості може слугувати ваговий коефіцієнт [1]:

$$q_i = \lg(1/\bar{N}_s (1 - P_i)), \quad (7)$$

де \bar{N}_3 – кількість хибних тривог за визначений проміжок часу T .

В [3] досліджені критерії (6)–(7) відносно побудови ЗВ, який складається із сукупності декількох незалежних ПВ, що дає можливість провести порівняльну оцінку ваги або ефективності різноманітних виявлювачів, отже, і вибрати найкращий, із яких повинна формуватись базова структура засобу. З'являється також можливість оптимізації порогів, при яких мінімізується якість виявлювачів.

Запропонований в [3] математичний апарат розрахунку максимальної ваги ПВ показує, що при нормальному і релеєвському розподілі щільності імовірності корисного сигналу $\omega_s(u)$ і завади $\omega_p(u)$ оптимальний поріг λ^0 відповідає критерію максимуму правдоподібності $\omega_s(\lambda^0) \approx \omega_p(\lambda^0)$.

Оптимальний алгоритм побудови комбінованих ЗВ та застосування незалежних ЗВ відповідно до (6) і (7) полягає у формуванні згідно сигналу тривоги від i -го ЗВ сигналу заданої амплітуди u_i і визначеного проміжку часу T наступним додаванням сигналів і порівнянням отриманої суми з фіксованим граничним рівнем C , перевищення якого призводить до формування загального сигналу тривоги.

Висновки й перспективи подальших досліджень

Таким чином, розглянувши алгоритми обробки логічних сигналів від ЗВ бачимо, що перевагами

алгоритму присвоєння “вагових” коефіцієнтів є те, що він дозволяє:

1. Забезпечити мінімально можливу імовірність хибної тривоги \bar{P}_i (при заданій імовірності виявлення $P_i^{\text{зад}}$);

2. Значення „вагового” коефіцієнта q_i визначати лише значеннями характеристик ЗВ, яке не залежить від інших ЗВ, що знаходяться в складі КЗВ, тобто q_i i -го ЗВ враховується лише при формуванні сигналу тривоги від i -го ЗВ (цим забезпечується простота нарощування ЗВ в КЗВ);

3. Залишити незмінним граничний рівень C (при нарощуванні або зменшенні ЗВ в КЗВ).

Недоліком даного алгоритму є складність вибору граничного рівня C , що повинен забезпечувати задану імовірність виявлення P_i (або

імовірність хибної тривоги \bar{P}_i) та який можливо реалізувати при довготривалих випробувань або засобами імітаційного моделювання.

Інформаційні критерії оцінки ефективності (6)–(7) ЗВ доцільно використовувати для порівняння ефективності різних ПВ, які формують базову структуру одного ЗВ. Критерії дозволяють виділити найбільш значущі завадові фактори, яким необхідно приділяти особливу увагу при загальному налаштуванні ТЗОС. Напрямок подальших досліджень є розробка імітаційної моделі функціонування ТЗОС.

Література

1. Магауєнов Р. Г. Системы охранной сигнализации: основы теории и принципы построения. – М.: Горячая линия – Телеком, 2004. – 367 с. 2. Звежинский С. С. Проблема выбора периметровых средств обнаружения. – БДИ, 2002, № 4. – С. 36–41. 3. Звежинский С. С. Повышение функциональной эффективности средств обнаружения. – Специальная техника, 2005, № 5. – С. 11–14. 4. Пинчук Г. Н., Петровский Н. П. Оценка функциональных показателей технических средств

обнаружения систем охраны. – Системы безопасности связи и телекоммуникаций, 2000, № 4. – С. 52–56. 5. Звежинский С. С. О сигнализационной надежности периметровых средств обнаружения. – БДИ, 2004, № 2. – С. 32–38. 6. Левин Б. Р. Теоретические основы статистической радиотехники. – М.: Советское радио, 1974–1976, кн.1–3.

АНАЛИЗ АЛГОРИТМОВ ОБРАБОТКИ ЛОГИЧЕСКИХ СИГНАЛОВ СРЕДСТВ ОБНАРУЖЕНИЯ ОХРАННОЙ СИГНАЛИЗАЦИИ

¹Вячеслав Владимирович Овсянников (канд. техн. наук)

¹Светлана Анатольевна Паламарчук

¹Юрий Александрович Процюк

¹Роман Михайлович Штонда

²Сергей Николаевич Островский

¹Военный институт телекоммуникаций и информатизации, Киев, Украина

²Центральный научно-исследовательский институт Вооруженных Сил Украины, Киев, Украина

Основными тактико-техническими характеристиками, которые определяют функциональную эффективность (сигнализационную надежность) системы сбора, обработки, отображения и документирования информации, вероятность правильного обнаружения нарушителя. Существующая система сбора, обработки, отображения и документирования информации для проведения анализа сигналов обнаружения от средств обнаружения можно классифицировать: на уровне логических сигналов (сигналов “тревога” из выходов средств обнаружения); на уровне аналоговых сигналов с

выходов предельных устройств средств обнаружения; на уровне оценок параметров нарушителя (рост, вес, длина и частота шага, скорость движения и др.).

Рассматриваются основные алгоритмы выявления логических сигналов технических средств охранной сигнализации относительно функциональной эффективности средств обнаружения по заданному алгоритму и формированию сигнала тревоги, которая определяется вероятностью правильного обнаружения нарушителя и средней наработкой на ложную тревогу, что при комбинировании нескольких средств обнаружения требует определения их взаимного влияния и уменьшения ложных тревог. Предложен вариант оценки эффективности комбинированных средств обнаружения на основе присвоения весовых коэффициентов. Критерии позволяют выделить наиболее значимые факторы помех, которым необходимо уделять особое внимание при общем настройке технических средств охранной сигнализации.

Ключевые слова: технические средства охранной сигнализации; комбинированные средства обнаружения; алгоритм обработки логических сигналов; вес средств обнаружения.

ANALYSIS OF LOGIC SIGNALS PROCESSING ALGORITHMS OF DETECTION ALARM

¹Viacheslav V. Ovsianikov (Candidate of Technical Sciences)

¹Svitlana A. Palamarchuk

¹Yurii O. Protsiuk

¹Roman M. Shtonda

²Serhii M. Ostrovskiy

¹Military Institute of Telecommunications and Information, Kyiv, Ukraine

²Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine

The main tactical and technical characteristic that determines functional effectiveness (signaling reliability) of system for collecting, processing, displaying and documenting the information is the probability of correct detection of the violator.

Existing systems for data collection, information processing, information presentation and information documentation regarding signal detection and detecting device analysis can be classified as follows: at the level of logic signals (signals "anxiety" of the outputs detection); at the level of analog signals from the outputs of the boundary detecting devices; at the level of violation of parameter estimation (height, weight, length and step frequency, speed, etc.). This article presents the basic algorithms for detection of logical signals of technical security alarm means in relation to the functional efficiency of detecting devices according to a given algorithm and alert signal. Security alarm is defined by the probability of correct identification of the violator and mean life false alarm that requires the recognition of their mutual influence and reduction of false alarms by combining multiple detection. It was suggested the variant of evaluating the effectiveness of combined detecting devices based on assigning weighted coefficients. The criteria enable to emphasis the most significant interference factors that should be taken into account in general settings of technical security alarm means.

Keywords: technical security alarm means, combined detecting devices, algorithm of processing logical signals, the worth of detecting devices.

References

1. Mahauenov R.G. (2004), Alarm systems: basic theory and principles of construction. [Sistemy okhrannoi signalizatsii: osnovy teorii i printcipy postroeniia], Moscow: hotline, Telecom, 367 p.
2. Zvezhynskyy S.S. (2002), Perimeter detection equipment selection problem. [Problema vybora perimetrovykh sredstv obnaruzheniia], BDY, No. 4, pp. 36-41.
3. Zvezhynskyy S.S. (2005), Increase operational efficiency detection means. [Povyshenie funktsionalnoi effektivnosti sredstv obnaruzheniia], Other special technics, No.5, pp. 11-14.
4. Pinchuk G.N., Petrovsky N.P. (2000), Evaluation of functional parameters of technical means of detection security systems. [Otsenka funktsionalnykh pokazatelei tekhnicheskikh sredstv obnaruzheniia sistem okhrany], Communication of security and telecommunications, No. 4, pp. 52-56.
5. Zvezhynskyy S.S. (2004), About signaling reliability of perimeter detection equipment. [O signalizatsionnoi nadezhnosti perimetrovykh sredstv obnaruzheniia], BDY, No. 2, pp. 32-38.
6. Levin B.R. (1974-1976), Theoretical Foundations of Statistical Radio Engineering. [Teoreticheskie osnovy statisticheskoi radiotekhniki], Moscow: Soviet Radio, kn.1-3.

Отримано: 03.08.2016 року.

¹Юрій Євгенович Репіло (д-р військ. наук)²Сергій Вікторович Тарасов¹Національний університет оборони України імені Івана Черняхівського, Київ, Україна²Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

АДАПТАЦІЯ МЕТОДУ НЕЧІТКИХ МНОЖИН ДЛЯ ОЦІНКИ КОРУПЦІЙНИХ РИЗИКІВ У ЗБРОЙНИХ КОНФЛІКТАХ

У статті розглядається методика визначення комплексного показника корупційного ризику в секторі безпеки і оборони під час виникнення, протікання і припинення збройного конфлікту. Дана методика базується на використанні теорії нечіткої логіки, яка дає змогу провести класифікацію сукупного корупційного ризику шляхом розподілу ризикової множини на підмножини рівня небезпеки корупційного ризику.

Використання теорії нечітких систем дозволяє оперувати неповними та неточними вхідними величинами, а також даними, які змінюються в часі. Крім того, методика нечітких систем дає змогу враховувати ймовірнісну природу зроблених висновків про результати вирішення проблем, у яких суб'єктивна думка або оцінка експертів мають істотне значення при появі факту незрозумілості та невизначеності її суті.

Таким чином, запропонована методика оцінки корупційних ризиків в секторі безпеки і оборони під час збройного конфлікту здатна адаптуватися до змін середовища, що дозволить ефективно використовувати її впродовж тривалого часу.

Ключові слова: корупція; військова корупція; корупційні ризики; збройний конфлікт.

Вступ

Постановка проблеми. Корупція у секторі безпеки і оборони, де існують сприятливі умови для її появи, зростання та поширення, ставить під серйозну загрозу ефективність підготовки та застосування військових формувань у воєнних конфліктах, підриває рівень довіри суспільства і міжнародних партнерів держави до її збройних сил, не дозволяє ефективно забезпечувати безпеку громадян і, у її найгіршому прояві, загрожує механізмам демократичного управління та навіть самим фундаментальним принципам існування держави у сучасному світі [1].

Збройними силами, які виконують свої завдання в умовах існування корупції, дуже важко досягти успіху (особливо у конфліктному середовищі). Також їм ускладнює роботу відсутність чітких рекомендацій (інструкцій) щодо її запобігання та протидії. Більш того, як свідчать результати роботи Женевського Центру демократичного контролю над збройними силами [2] чітких процедур щодо визначення та попередження корупційних загроз у збройних конфліктах на міжнародному рівні також не визначено.

Виходячи з цього у теорії та практиці будівництва збройних сил виникло протиріччя між потребою у науково-методичному апараті, який дозволяє визначати ризик прояву загрози ефективності підготовки та застосування військових формувань у воєнних конфліктах з одного боку та відсутністю такого апарату з іншого.

Аналіз результатів останніх досліджень і публікацій свідчить, що рішення проблеми

багатофакторного управління (до якої відноситься і комплексна оцінка корупційного ризику прояву загрози ефективності підготовки та застосування військових формувань у воєнних конфліктах) є нетривіальним завданням. Основні труднощі виникають, коли вхідні параметри стають невизначеними, але одночасно впливають на результати рішення. Крім того, із зростанням числа врахованих факторів зростає ступінь неточності або нечіткості [3]. Нечіткість полягає в тому, що в конкретний момент часу не завжди вдається достовірно виміряти (оцінити) всі вхідні величини [4].

Відомі теоретичні дослідження різних видів ризиків [5, 6] далекі від достовірності, оскільки розробити абсолютно точний показник ризику достатньо складно. Практика оцінювання будь-яких видів ризику [7] показує, що багато сучасних задач управління не завжди вдається розв'язати класичними методами через значну складність математичних моделей, що їх описують. Тому, зазвичай, визначають відносний показник ризику і порівнюють його з середнім для відповідної галузі діяльності. Здебільшого відомі методи визначення показника ризику базуються на використанні експертних оцінок [8].

Проте, останнім часом у публікаціях з'явилися математичні методи [9], які дають змогу врахувати неповну, неточну, а часто і спотворену інформацію про стан небезпеки, а також ймовірнісну природу зроблених при цьому висновків. До них, зокрема, належать нечітко-множинні та логіко-ймовірнісні методи [10, 11]. Ці методи дали змогу оцінювати результати вирішення проблем, у яких суб'єктивна думка або

оцінка експертів мають істотне значення при появі факту незрозумілості та невизначеності їх суті.

Аналізуючи останні дослідження можна зробити висновок, що наведена теорія нечітких множин здебільшого успішно використовується для оцінки ризиків у банківській та фінансових сферах, а також фахівцями в області політичного й економічного аналізу. Проте, галузі безпеки і оборони приділено недостатню увагу, а питання ідентифікації корупційних ризиків у збройних конфліктах не розглядалося взагалі.

Виходячи з цього **метою** статті є адаптація методу нечітких множин для оцінки корупційних ризиків у збройних конфліктах, який базується на правилах нечіткої логіки з передбаченням адаптації вхідних даних до змін середовища для ефективного використання впродовж тривалого часу.

Виклад основного матеріалу дослідження

Нечітка логіка [12, 13], запропонована Л. А. Заді ще в 1965 р., – початкова точка зору, що оперує неточними, не визначеними і навіть не повністю зрозумілими поняттями. З того часу з'явилася величезна кількість робіт з розроблення та використання методів нечіткої логіки [14-16].

Методи нечітких множин особливо корисні за відсутності точної математичної моделі функціонування системи до якої можна віднести і систему загроз ефективності підготовки та

застосування військових формувань у воєнних конфліктах. Теорія нечітких множин дає можливість застосувати для прийняття рішень неточні та суб'єктивні експертні знання про предметну область без формалізації їх у вигляді традиційних математичних моделей.

З використанням теорії нечітких множин вирішуються питання узгодження суперечливих критеріїв прийняття рішень, створення логічних регуляторів систем. Нечіткі множини дають змогу застосовувати лінгвістичний опис складних процесів, встановлювати нечіткі відношення між поняттями, прогнозувати поведінку системи, формувати множини альтернативних дій, виконувати формальний опис нечітких правил прийняття рішень.

Важливим застосуванням теорії нечітких множин є контролери нечіткої логіки, які використовуються у різноманітних системах керування, зокрема у побутових приладах. Замість математичної моделі для опису системи такі контролери використовують інтегровані знання експертів, які за структурою подання наближаються до розмовної мови і описуються за допомогою лінгвістичних змінних та нечітких множин [17-19].

Загальна структура системи нечіткого керування зображена на рис. 1 та містить у своєму складі такі складові: блок фазифікації, база правил нечітких рішень, блок рішень, блок дефазифікації.



Рис. 1. Застосування методу нечітких множин для оцінювання корупційних ризиків

У блоці фазифікації (п.4) чіткі значення величини, описані лінгвістичними змінними у базі вхідних параметрів перетворюються на нечіткі знань. Процес фазифікації передбачає попередній

збір експертної інформації та використання процедур її обробки.

У блоці рішень (п.5) використовуються нечіткі умовні (if – then) правила, що закладені у базі правил, для перетворення нечітких вхідних даних на необхідні керуючі впливи, що мають також нечіткий характер.

База правил систем нечіткого виведення (п.7) призначена для формального подання емпіричних знань або знань експертів в тій чи іншій проблемній області.

У блоці дефазифікації (п.6) нечіткі дані з виходу блоку рішень перетворюються на чітку величину, тобто відбувається знаходження чіткого значення для кожної з вихідних лінгвістичних змінних множини.

З врахуванням означеного, пропонується методика визначення комплексного показника ризику прояву корупції у воєнних конфліктах (рис. 2), яка базується на основних принципах теорії нечітких множин і містить декілька етапів.

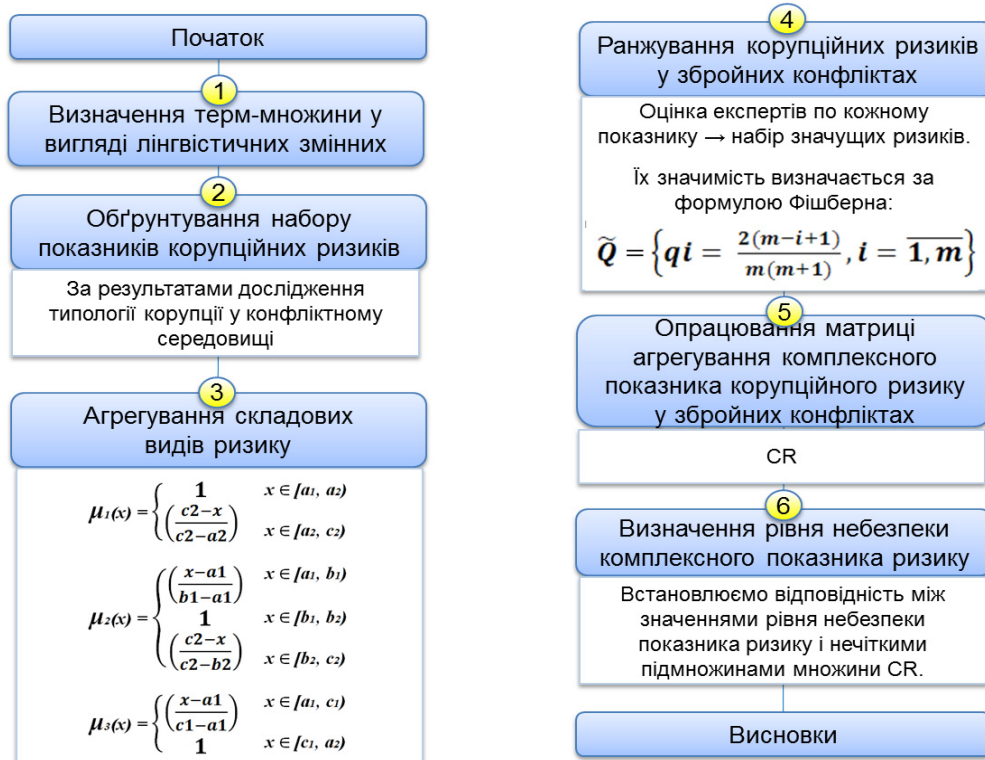


Рис. 2. Методика визначення комплексного показника ризику прояву корупції у воєнних конфліктах

Етап 1. Визначається терм-множини у вигляді лінгвістичних змінних, які задаються на деякій кількісній шкалі та набувають значень у вигляді слів і словосполучень звичайної мови. Лінгвістичні змінні та їх значення слугують для якісного словесного опису деякої кількісної величини. В рамках даного дослідження вводяться

лінгвістичні змінні “ступінь впливу ризику” і “рівень небезпеки ризику” та нечіткі підмножини, які утворюють вичерпну кількість значень введених змінних, а також встановлюють однозначну відповідність між введеними змінними (табл. 1).

Таблиця 1

Відповідність назв лінгвістичних змінних їх значенням

Значення лінгвістичної змінної:			
А– ступінь впливу ризику		В – рівень небезпеки ризику	
a ₁	значний вплив	b ₁	високий ризик
a ₂	незначний вплив	b ₂	середній ризик
a ₃	слабкий вплив	b ₃	низький ризик

Етап 2. Обґрунтовується набір показників корупційних ризиків, які піддаватимуться комплексному оцінюванню:

$$X = \{x_i = f_i(\dots), i = \overline{1, m}\} \quad (1)$$

де: m - кількість видів корупційного ризику;

x_i – корупційний ризик і-го виду, який відповідно до розробленої раніше системи показників та критеріїв оцінювання ефективності попередження корупційних загроз у воєнних конфліктах набуває такого фізичного змісту:

x₁ – військово-політичний ризик, тобто вірогідність впливу корупції, пов’язаної з

неправомірним прийняттям рішень на вищому рівні;

x_2 – військовий ризик, тобто вірогідність впливу корупції, пов’язаної з негативними подіями у внутрішньому середовищі оборонного сектору;

x_3 – операційний ризик, тобто вірогідність впливу корупції, пов’язаної з чинниками, що визначають умови проведення збройного конфлікту;

x_4 – фінансовий ризик, тобто вірогідність впливу корупції, пов’язаної з порушенням визначених процедур проведення державних закупівель;

x_5 – інформаційний ризик, тобто вірогідність впливу корупції, пов’язаної недбалістю при проведенні зовнішнього контролю та недостатнім захистом інформаторів.

Етап 3. Агрегування складових видів ризику до рівня базових видів ризику, здебільшого здійснюється на основі матричної схеми агрегування [17]. Для цього введемо поняття “терм-множина значень”, яка містить значення лінгвістичної змінної $V = \{b_j, j=1, n\}$.

Для рівнів небезпеки ризику вводиться така лінгвістична змінна:

$$\tilde{C} = \{ \tilde{C}_i = \{ \tilde{C}_{ij}, j=1, n \}, i=1, m \} \quad (2)$$

де: C_{ij} – значення j -го рівня небезпеки i -го виду ризику, яка у нашому дослідженні набуває таких значень:

C_{i1} – низький рівень корупційного ризику i -го виду;

C_{i2} – середній рівень корупційного ризику i -го виду;

C_{i3} – високий рівень корупційного ризику i -го виду.

Для цієї лінгвістичної змінної вводиться множина функцій належності:

$$M = \{ \mu_j(x), j=1, n \} \quad (3)$$

де $\mu_j(x)$ – функція j -ої належності, набуває такого вигляду:

$$\mu_1(x) = \begin{cases} 1 & x \in [a_1, a_2) \\ \left(\frac{c_2 - x}{c_2 - a_2} \right) & x \in [a_2, a_2) \end{cases} \quad (4)$$

$$\mu_2(x) = \begin{cases} \left(\frac{x - a_1}{b_1 - a_1} \right) & x \in [a_1, b_1) \\ 1 & x \in [b_1, b_2) \\ \left(\frac{c_2 - x}{c_2 - a_2} \right) & x \in [b_2, c_2) \end{cases} \quad (5)$$

$$\mu_3(x) = \begin{cases} \left(\frac{x - a_1}{c_1 - a_1} \right) & x \in [a_1, c_1) \\ 1 & x \in [c_1, a_2) \end{cases} \quad (6)$$

У цих рівняннях було обрано такі значення степеневих коефіцієнтів, які дають змогу функціям (4)-(6), на наш погляд та думку інших науковців [18,19], отримати значення належності, максимально наближені до реальних думок експертів (рис. 3). Водночас, вони враховують військову сутність наведених вище показників корупційного ризику. Слід зазначити, що різні значення степеневих коефіцієнтів визначають різні швидкості зростання/спадання значень функцій належності за відношенням до приросту значень параметра, що дає змогу оцінити ступінь належності значень параметра до певного лінгвістичного терму.

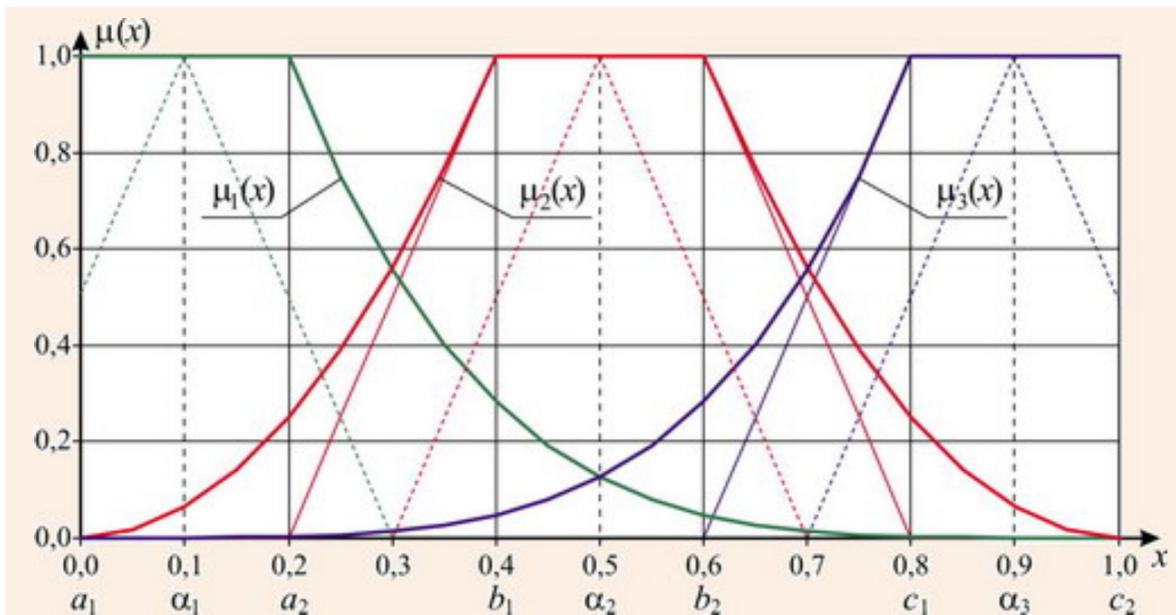


Рис. 3. Система функцій належності на 01-носієві

Носіями лінгвістичної змінної C_{ij} виступають відрізки дійсної осі x на проміжку $[0,1]$. Будь-які скінченно-вимірні відрізки дійсної осі можна звести до відрізка $[0,1]$ шляхом простого лінійного перетворення [18]. Тому виділений відрізок одиничної довжини має універсальний характер і називається 01-носієм. Вибір відрізка такої довжини пов'язаний з тим, що класичним методом оцінювання ризику є імовірнісний, де вірогідність появи ризику також визначається на відрізку $[0,1]$. Отже, при потребі можна зіставити результати дослідження імовірнісного характеру появи ризику з оцінкою ризику, отриманого на основі методів нечітких множин і знань.

Введемо набір так званих вузлових точок $\alpha_j = \{0,2; 0,5; 0,8\}$, які є, з одного боку, абсцисами максимумів відповідних функцій належності $\mu_j(x)$ на 01-носієві, а з іншого – вони рівномірно віддалені один від одного на 01-носієві і симетричні відносно вузла $\alpha_2 = 0,5$. Тоді лінгвістична змінна C_{ij} , визначена на 01-носієві, в сукупності з набором вузлових точок називається трикутним нечітким 01-класифікатором.

Якщо існує набір з m окремих видів ризику з своїми поточними значеннями x_i і кожному виду

ризиків відповідає свій класифікатор, то можна перейти від набору окремих показників їх оцінювання до єдиного комплексного показника CR, значення якого потім розпізнається за допомогою стандартного класифікатора. Кількісне значення комплексного показника визначається за формулою подвійного згортання:

$$CR = \sum d_i \sum \mu_j(x_i) \alpha_j \quad (7)$$

де d_i - вагомість показника корупційного ризику i -го виду в згортці.

Далі комплексний показник CR можна піддати розпізнаванню на основі стандартного нечіткого класифікатора за функціями належності (4)-(6). Вузлові точки в нечіткому класифікаторові виступають як вагові коефіцієнти при агрегуванні системи видів ризику на рівні їх якісних станів.

Етап 4. Проводиться оцінка експертів і здійснюється ранжування поточного рівня корупційного ризику у збройних конфліктах (табл. 2).

Таблиця 2

Матриця рангів і ранжування поточного рівня видів корупційного ризику у збройних конфліктах

Назва показника	Оцінки експертів, ранги						Значимість за формулою Фішберна					
	1	2	3	4	5	сер. знач.	1	2	3	4	5	сер. знач.
X_1	1	2	3	2	1	1,8	0,33	0,27	0,20	0,27	0,33	0,280
X_2	3	1	1	3	2	2,0	0,20	0,33	0,33	0,20	0,27	0,266
X_3	2	3	2	1	4	2,4	0,27	0,20	0,27	0,33	0,13	0,240
X_4	4	5	4	4	3	4,0	0,13	0,07	0,13	0,13	0,20	0,132
X_5	5	4	5	5	5	4,8	0,07	0,13	0,07	0,07	0,07	0,082
Сума:	15	15	15	15	15	15,0	1,0	1,0	1,0	1,0	1,0	1,0

Ідентифікація показників ризику дає змогу побудувати їх профіль, який показує набір значущих ризиків у збройному конфлікті. Після ідентифікації ризиків можна визначити питому вагу кожного виявленого і ідентифікованого показника ризику на основі правила Фішберна [17]:

$$\tilde{Q} = \left\{ q_i = \frac{2(m-i+1)}{m(m+1)}, i = \overline{1, m} \right\} \quad (8)$$

де Q_i - питома вага i -го показника ризику; m - кількість показників. Отримані результати розрахунку наведено в табл. 2.

Етап 5. Після виконання наведених вище дій будується матриця (табл. 3), де по рядках розташовані види корупційного ризику, а по стовпцях – їх якісні рівні. На перетині рядків і стовпців знаходяться значення функцій належності $\mu_j(x_i)$ відповідних якісних рівнів. Матриця доповнюється ще одним стовпцем, у якому знаходяться значення вагових коефіцієнтів d_i ризику i -го виду в згортці (7). Тоді для розрахунку комплексного показника CR в отриманій матриці зібрані всі необхідні вихідні дані, внаслідок чого схема агрегування даних називається матричною.

Матриця агрегування комплексного показника корупційного ризику у збройних конфліктах

Вид ризику, X_i	Ранг, середнє значення	Значущість показника d_i	Значення функції належності для ризику i -го виду j -го рівня			Комплексний показник ризику	
			низький $\mu_1(x_i)$	середній $\mu_2(x_i)$	високий $\mu_3(x_i)$	$r_i = \sum \mu_j(x_i) a_j$	$d_i \cdot r_i$
X_1	1,8	0,280	0,9238	0,2870	0,0030	0,3307	0,0709
X_2	2,0	0,266	1	0,0221	0	0,2111	0,0126
X_3	2,4	0,240	1	0,0717	0,0001	0,2359	0,0253
X_4	4,0	0,132	0,9238	0,2870	0,0030	0,3307	0,0709
X_5	4,8	0,082	0,9238	0,2870	0,0030	0,3307	0,0709
Вузлові точки, a_i			0,2	0,5	0,8	Сума:	0,2506

Таким чином, комплексний показник корупційного ризику у збройних конфліктах за означених в прикладі умов становить $CR = 0,2506$.

Етап 6. Проводиться класифікація поточного значення рівня небезпеки комплексного показника ризику CR , як критерію розбиття ризикової

множини на підмножини. Встановлюється відповідність між значеннями рівня небезпеки показника ризику і нечіткими підмножинами множини CR . Граничний рівень комплексного показника ризику визначається за табл. 4.

Таблиця 4

Шкала для визначення рівня небезпеки комплексного показника ризику

Інтервал значень CR	Назва підмножини		Категорія ризику	Ступінь оцінної упевненості (функція належності)
	Рівень небезпеки комплексного показника ризику			
0,8 – 1,0	CR_3	- високий	A	1
0,6 – 0,8	CR_3	- високий	A	$1 - \mu_2 = \mu_3$
	CR_2	- середній	B	$\mu_2 = m \cdot (0,8 - CR)$
0,4 – 0,6	CR_2	- середній	B	1
0,2 – 0,4	CR_2	- середній	B	$1 - \mu_1 = \mu_2$
	CR_1	- низький	C	$\mu_1 = m \cdot (0,4 - CR)$
0,0 – 0,2	CR_1	- низький	C	1

Отриманий результат не дає змоги експертові або особі, що оцінює рівень комплексного показника корупційного ризику, зробити однозначний висновок щодо визначення певної категорії ризику. Значення комплексного показника корупційного ризику у збройних конфліктах знаходиться в інтервалі від 0,2 до 0,4, при якому з різною мірою упевненості корупційний ризик можна ідентифікувати як низький або середній. На аналізованому об'єкті комплексний показник ризику має низький рівень (ступінь оцінної упевненості $1 - 0,2506 = 0,7494$) і належить до категорії С. Чим більше значення показника наблизитиметься до межі 0,2, тим із більшою упевненістю можна констатувати, що комплексний показник корупційного ризику у збройних конфліктах бази можна буде оцінювати як низький.

Висновки й перспективи подальших досліджень

У статті проведено аналіз існуючих методик управління ризиками в умовах невизначеності та адаптовано методіку нечітких множин для визначення та оцінки корупційних ризиків прояву загрози ефективності підготовки, застосування військових формувань у воєнних конфліктах та повернення до стабільності на базі правил нечіткої логіки з передбаченням адаптації вхідних даних до змін середовища.

Перспективами подальших досліджень може бути обґрунтування механізмів попередження корупційних ризиків та розробка методичних основ оцінювання ефективності заходів щодо запобігання корупції в сфері оборони.

Література

1. **Леліков Г.** Державно-політичні та соціально-економічні аспекти боротьби з корупцією [Текст] / Г. Леліков, О. Оболенський // Вісник УАДУ. – 1998. – №2. – С. 16–22. 2. **Виховання** доброчесності та боротьба з корупцією в оборонному секторі: збірник прикладів (компендіум) позитивного досвіду [Текст]. – Женевський Центр демократичного контролю над збройними силами. – 2010. – 384 с. 3. **Repilo Y., Tarasov S.** Threats assessment review in higher military education system (higher MES). London, TI (UK), 2013. 30 p. 4. **Репіло Ю. Є., Тарасов С. В.** Чим корупція може загрожувати вищій військовій освіті?. Збірник наукових праць "Вісник НУОУ", вип.4(35)/2013, с.327-339. 5. **Репіло Ю. Є., Тарасов С. В.,** Можливість виникнення та існування корупційних загроз у системі вищої військової освіти. Суч. інф. технології у сфері безпеки та оборони № 1 (22)/2015, с. 157-165. 6. **Качалов Р. М.** Управление хозяйственным риском [Текст] / Р. М. Качалов. – М. : Изд-во "Наука", – 2002. – 192 с. 7. **Борисова Т. М.** Теоретичні аспекти управління ризиком на підприємстві [Текст] // Актуальні проблеми економіки. – 2005 р., с. 116-120. 8. **Ризики** в підприємстві: оцінювання та управління: Навчальний посібник [Текст] / А. В. Шегда, М. В. Голованенко; за ред. А. В. Шегди. – К.: Знання, 2008. – 271 с. 9. **Рыхтикова П. А.** Анализ и управление рисками организации [Текст] / П. А. Рыхтикова. – М. : Изд-во ФОРУМ; ИНФРА-М, – 2007. – 240 с. 10. **Бешелев С. Д.** Математико-статистические методы экспертных оценок [Текст] / С. Д. Бешелев, Ф. Г. Гурвич. – 2-е изд., [перераб. и доп.]. – М.: Изд-во "Статистика", – 1980. – 263 с. 11. **Гранатуров В. М.** Экономический риск: сущность, методы измерения, пути снижения : учебн. пособ. [Текст] / В. М. Гранатуров. – 2-е изд., [перераб. и доп.]. – М.: Изд-во "Дело и Сервис", – 2002. – 112 с. 12. **Ротштейн О. П.** Метод побудови функцій належності нечітких множин [Текст] / О. П. Ротштейн, Г. О. Черноволік, Є. П. Ларюшкін // Вісник Вінницького політехнічного інституту : наук. журнал. – Вінниця: Вид-во "Універсум-Вінниця". – 1996. – №3. – С. 72-75. 13. **Матвійчук А. В.** Аналіз та прогнозування розвитку фінансово-економічних систем із використанням теорії нечіткої логіки: монографія [Текст] / А.В. Матвійчук. – К. : Центр навч. літ-ри, – 2005. – 206 с. 14. **Заде Л. А.** Основы нового подхода к анализу сложных систем и процессов принятия решений [Текст] / Л. А. Заде // Математика сегодня. – М. : Изд-во "Знание", – 1974. – С. 549. 15. **Заде Л. А.** Понятие лингвистической переменной и его применение к принятию приближенных решений [Текст] / Л. А. Заде. – М. : Изд-во "Мир", – 1976. – 162 с. 16. **Борисов А. Н.** Принятие решений на основе нечетких моделей: примеры использования [Текст] / А. Н. Борисов, О. А. Крумберг, И. П. Федоров. – Рига : Изд-во "Зинатне". – 1990. – 184 с. 17. **Кравець П.** Системи прийняття рішень з нечіткою логікою [Текст] / П. Кравець, Р. Киркало // Національний університет "Львівська політехніка". – 2009. – С. 115-123. 18. **Zimmerman H.J.** Fuzzy Set Theory and Its Applications / H.J. Zimmerman. – Kluwer, Dordrecht, 1991. – 315 p. 19. **Mamdani E.H.** Application of fuzzy algorithms for the control of a simple dynamic plant / E.H. Mamdani // Proc. IEEE 121, 1974. – P. 1585-1588. 20. **Hguen H.T.** Theoretical aspects of fuzzy control / H.T. Hguen, M. Sugeno, R. Tong, R.R. Yager. – New York, John Wiley & Sons, 1995. – 359 p. 21. **Mudi R.K.** A self-tuning fuzzy PI controller / R.K. Mudi, N.R. Pal // Int. Jo. Fuzzy sets and systems. – № 115. – 2000. – pp. 327-378.

АДАПТАЦИЯ МЕТОДА НЕЧЕТКИХ МНОЖЕСТВ ДЛЯ ОЦЕНИВАНИЯ КОРРУПЦИОННЫХ РИСКОВ В ВООРУЖЕННЫХ КОНФЛИКТАХ

¹Юрий Евгеньевич Репило (д-р воен. наук)

²Сергей Викторович Тарасов

¹Национальной университет обороны Украины имени Ивана Черняховского, Киев, Украина

²Центральный научно-исследовательский институт Вооруженных Сил Украины, Киев, Украина

В статье рассматривается методика определения комплексного показателя коррупционного риска в секторе безопасности и обороны во время возникновения, протекания и прекращения вооруженного конфликта. Данная методика базируется на использовании теории нечеткой логики, которая позволяет провести классификацию совокупного коррупционного риска путем распределения множества рисков на подмножества уровня опасности коррупционного риска.

Использование теории нечетких систем позволяет оперировать неполными и неточными входными величинами, а также данными, которые изменяются во времени. Кроме того, методика нечетких систем позволяет учитывать вероятностную природу сделанных выводов о результатах решения проблем, в которых субъективное мнение или оценка экспертов имеют существенное значение при появлении факта непонятности и неопределенности ее сути.

Таким образом, предложенная методика оценки коррупционных рисков в секторе безопасности и обороны во время вооруженного конфликта способна адаптироваться к изменениям среды, что позволит эффективно использовать ее в течение длительного времени.

Ключевые слова: коррупция; военная коррупция; коррупционные риски; вооруженный конфликт.

ADAPTING THE FUZZY SETS METHOD FOR THE EVALUATION CORRUPTION RISKS IN CONFLICT ENVIRONMENT

¹Yuriy Y. Repilo (Doctor of Military Sciences)

²Serhii V. Tarasov

¹National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

In this article the method of determination the complex index is represented to assess the corruption risk in security and defense sector during the pre-deployment period, armed conflict itself and post conflict (return to stability) environment. This method is based on the theory of fuzzy logic, which allows to classify the total corruption risk by allocating many risks according to the level of corruption risk.

Using the theory of fuzzy systems allows to operate with incomplete and inaccurate input data, as well as changeable ones over time. In addition, the technique of fuzzy systems takes into account the probabilistic nature of the conclusions of the results of problem solving in which a subjective opinion or expert evaluation are essential when a fact of uncertainty and incomprehensibility take place.

Thus, the proposed method of assessing the corruption risk in the security and defense sector during the armed conflict is quite adaptable to changes, which in its turn allows to use it effectively for a long period of time.

Keywords: corruption; military corruption; corruption in operations; armed conflict.

References

- Lelikov G.** (1998), Public-political and socio-economic aspects of the fight against corruption, Alexander Obolensky, Bulletin of the Academy of Public Administration. [Derzhavno-politychni ta sotsialno-ekonomichni aspekty borotby z koruptsiieiu], No.2, pp. 16-22.
- Building Integrity and Reducing Corruption in Defense: a collection of examples (compendium) positive experience,** (2010), [Vykhovannia dobrochesnosti ta borotba z koruptsiieiu v oboronnomu sektori: zbirnyk prykladiv (kompndium) pozytyvnoho dosvidu], Genève Centre for the Democratic Control of Armed Forces, 384 p.
- Repilo Y., Tarasov S.** (2013) Threats assessment review in higher military education system (higher MES). London, TI (UK), 30 p.
- Repilo Y., Tarasov S.** (2013), How corruption can threaten military higher education? [Chym koruptsiia mozhe zahrozhuvaty vyshchii viiskovii osviti?], Collected Works "Journal NDU" edition 4 (35), pp. 327-339.
- Repilo Y., Tarasov S.** (2015), The possibility of the existence of corruption and the threat of higher military education. [Mozhlyvist vynykennnia ta isnuvannia koruptsiinykh zahroz u systemi vyshchoi viiskovoi osvity], Modern information technology in the sphere of security and defense No. 1 (22), pp. 157-165.
- Katchalov P.** (2002), Management of economic risk. [Upravlenie hozjajstvennym riskom], P. Katchalov, Moscow: Publishing "Science", 192 p.
- Borisova T.** (2005), Theoretical aspects of risk management in the enterprise. [Teoretychni aspekty upravlinnia ryzykom na pidpriemstvi], Actual problems of economy, pp. 116-120.
- Risks in business, management and evaluation: Textbook,** (2008), [Ryzyky v pidpriemnystvii: otsiniuvannia ta upravlinnia: Navchalnyi posibnyk], A. Szegdy, N. Holovanenko, Kyiv: Knowledge, 271 p.
- Ryhtikova P.** (2007), Analysis and Risk Management Organization. [Analiz i upravlenie riskami organizacii], Moscow: Publishing House of the Forum; INFRA-M, 240 p.
- Beshelev S.** (1980), Mathematical and statistical methods of expert assessments. [Matematiko-statisticheskie metody jekspertnyh ocenok], S. Beshelev, F. Gurvich, 2nd ed., Moscow: Publishing House of the "Statistics", 263 p.
- Granaturov V.** (2002), Economic risk: essence, measurement methods, ways to reduce: Training. Collec. [Jekonomicheskij risk: sushhnost', metody izmerenija, puti snizhenija], 2nd ed. Moscow: Publishing House of the "Business and Service", 112 p.
- Rothstein A.** (1996), Method of constructing functions of fuzzy sets. [Metod pobudovy funktsii nalezhnosti nechitkykh mnozhyn], G. Chernovolyk, E. Lariushkin, Herald of Vinnitsa Polytechnic Institute: Science. magazine. - Ball: "Universum-Vinnitsia", No.3, pp. 72-75.
- Matviychuk A.** (2005), Analysis and forecasting of financial and economic systems with the use of fuzzy logic: monograph. [Analiz ta prohnozuvannia rozvytku finansovo-ekonomichnykh system iz vykorystanniam teorii nechitkoi lohiky: monohrafiia], Kyiv: Center teach, 206 p.
- Zade L.** (1974) A new approach to the analysis of complex systems and decision-making processes. [Osnovy novogo podhoda k analizu slozhnykh sistem i processov prinjatija reshenij], Mathematics today, Moscow: Publishing house "Knowledge", 549 p.
- Zade L.** (1976), The concept of linguistic variable and its application to the adoption of approximate solutions. [Ponjatie lingvisticheskoy peremennoj i ego primenenie k prinjatiju priblizhennykh reshenij], Moscow: Publishing House of the "World", 162 p.
- Borisov A.** (1990), Decision-making based on fuzzy models: examples of using. [Prinjatie reshenij na osnove nechetkih modelej: primery ispol'zovanija], O Krumberg, Riga: Publishing house "Zinatne", 184 p.
- Kravets P.** (2009), Decision-making systems with fuzzy logic. [Systemy pryiniattia rishen z nechitkoiu lohikoiu], R. Kyrkalo, National University "Lviv Polytechnic", pp. 115-123.
- Zimmerman H.J.** (1991), Fuzzy Set Theory and Its Applications, Kluwer, Dordrecht, 315 p.
- Mamdani E.H.** (1974), Application of fuzzy algorithms for the control of a simple dynamic plant, Proc. IEEE 121, pp. 1585-1588.
- Hguen H.T.** (1995), Theoretical aspects of fuzzy control, M. Sugeno, R. Tong, R.R. Yager, New York, John Wiley & Sons, 359 p.
- Mudi R.K.** (2000), A self-tuning fuzzy PI controller, N.R. Pal, Int. Jo. Fuzzy sets and systems, No. 115, pp. 327-378.

Отримано: 01.07.2016 року.

¹Михайло Олексійович Шишанов (д-р техн. наук, професор)²Володимир Іванович Коцюруба (канд. військ. наук, с.н.с, доцент)¹Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ, Україна²Національний університет оборони України імені Івана Черняхівського, Київ, Україна

БАЛІСТИЧНА МОДЕЛЬ ТРАЛЕННЯ ВИБУХОВИХ ПРИСТРОЇВ З НАТЯЖНИМ ДАТЧИКОМ ЦІЛІ

На основі аналізу існуючих підходів щодо моделювання процесів розмінування, зокрема використання засобів для тралення вибухових пристроїв з натяжними датчиками цілі, запропонована балістична модель, яка, на відміну від існуючих, враховує приріст питомої маси засобу для тралення (комбінація елемента, що тралить, і тросу) під час польоту. Одним із найбільш складних питань під час моделювання є визначення залежності параметрів польоту елемента, що тралить, від динаміки приросту маси тросу. Балістичними параметрами елемента, що тралить, які досліджуються, є: кут вильоту, дальність, висота, час, швидкість польоту. Запропоновані удосконалення математичної моделі та послідовності проведення розрахунків дозволять підвищити точність результатів моделювання процесу тралення вибухових пристроїв з натяжними датчиками цілі під час обґрунтування вимог до засобів розмінування даного типу. Напрямами подальших досліджень є математичне моделювання процесу польоту елемента, що тралить, які входять до складу засобів для тралення вибухових пристроїв з натяжними датчиками цілі, та обґрунтування, на основі використання його результатів, раціональних балістичних параметрів

Ключові слова: балістична модель; вибуховий пристрій; натяжний датчик цілі; тралення; засіб для тралення.

Вступ

В результаті ведення наземної мінної війни на сході нашої країни [1] значна площа території місцевості виявилася замінованою. Більшість вибухових пристроїв (ВП), які використовувались, оснащені натяжними датчиками цілі. Точні відомості про місця їх встановлення відсутні. Тому такі ВП становлять велику загрозу для військ, які ведуть бойові дії, унеможливають використання території місцевості та замінованих об'єктів у господарчих цілях.

Постановка проблеми. Одним із найбільш ефективних способів протидії ВП даного типу залишається їх тралення, яке у Збройних Силах України здійснюється закиданням на заміновану ділянку місцевості елемента, що тралить (ТЕ), («кішки») вручну із подальшим його підтягуванням за допомогою тросу. Але такий варіант виконання завдання має низку серйозних недоліків, серед яких основними є великий ризик для особового складу, низька точність попадання ТЕ, обмеження щодо використання таких засобів у забудованій та залісеній місцевості. Визначені недоліки можуть бути усунуті за рахунок впровадження в практику розмінування місцевості та об'єктів перспективних засобів тралення ВП із натяжним датчиком цілі. За таких умов постає проблемне питання обґрунтування вимог до засобів розмінування даного типу із врахуванням балістичних параметрів процесу дистанційного тралення. Актуальність останнього підтверджується вимогами керівних документів

[2-4] та набутим досвідом [1,5]. Вирішення визначеного проблемного питання стає можливим за рахунок моделювання із використанням удосконаленого науково-методичного апарату.

Аналіз останніх досліджень і публікацій показав, що питанням дослідження процесу тралення ВП із натяжним датчиком цілі приділялася недостатня увага. Так в [5] розглядається порядок дій підрозділів на території де можливе застосування саморобних вибухових пристроїв в тому числі і з натяжними датчиками цілі. Оцінювання ефективності подовжених зарядів розмінування розглянуті в [6], згідно з чим ефективність зосереджених, подовжених та сітчастих зарядів розмінування оцінюється з боку впливу вибуху на міну. Крім того оцінюється вибухостійкість інженерних боєприпасів із натяжними датчиками цілі. Механічне тралення у роботах [5,6] не розглядається. У [7] розглянута задача визначення параметрів польоту тіла кинутого під кутом до горизонту, яка може бути покладена в основу балістичної моделі тралення ВП з натяжним датчиком цілі. На відміну від тіла, яке розглядається у [7], в нашому випадку сума маси ТЕ m і питомої маси тросу $m_{\delta\delta}$ під час польоту буде змінюватись внаслідок витягування (зміни довжини l) останнього. Отже, для визначення балістичних параметрів засобу для тралення (ЗТ) під час їх використання підхід [7] потребує удосконалення.

Враховуючи вищезазначене метою статті є висвітлення основних положень розробленої

балістичної моделі тралення вибухових пристроїв з натяжним датчиком цілі в умовах змінної маси ЗТ.

Виклад основного матеріалу дослідження

Одним із найбільш складних питань під час моделювання є визначення залежності параметрів

польоту ТЕ від динаміки збільшення маси $m(x)$ ЗТ (комбінація ТЕ і тросу).

На початок умовно представимо ТЕ як тіло постійної маси кинуте під кутом. Розрахункова схема метання такого тіла представлена на рис. 1.

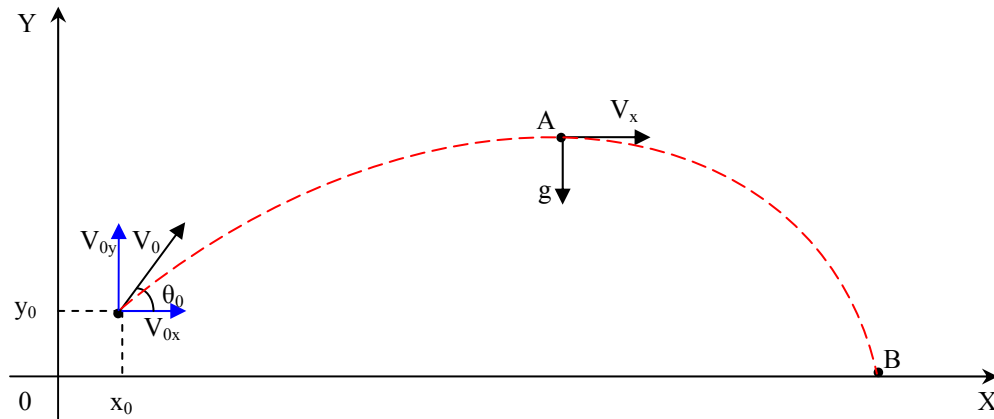


Рис. 1. Побудова траєкторії польоту тіла, кинутого під кутом.

До балістичних параметрів польоту ТЕ відносяться: кут вильоту θ_0 , максимальна дальність L , висота H , час T , швидкість V_x польоту ТЕ.

ТЕ, отримавши початкову швидкість V_0 , рухається у середовищі, що чинить опір, по деякій траєкторії до тих пір, доки не впаде на землю. Для дослідження параметрів визначеної траєкторії побудуємо рівняння польоту ТЕ, які кинуті під кутом θ_0 з початковою швидкістю V_0 , на основі схеми (рис. 1).

Розглянемо рух ТЕ, кинутого під кутом θ_0 з початковою швидкістю V_0 . Проецируємо початкову швидкість \vec{V}_0 та прискорення \vec{a} на осі X та Y . Проекція початкової швидкості на вісь X дорівнює $V_{0x} = V_0 \cdot \cos \theta_0$. Проекція прискорення $a_x = 0$, оскільки вектор \vec{g} перпендикулярний осі X . Тому рух ТЕ вздовж осі X буде рівномірним. Проекція швидкості V_x та координата x ТЕ, що летить, визначається співвідношеннями

$$V_x = V_0 \cdot \cos \theta_0, \\ x = x_0 + V_0 \cdot t \cdot \cos \theta_0.$$

Проекція початкової швидкості на вісь Y дорівнює $V_{0y} = V_0 \cdot \sin \theta_0$. Проекція прискорення $a_y = -g$, оскільки вектор \vec{g} спрямований у протилежному осі Y напрямку. Тому вздовж осі Y рух ТЕ рівнозмінний. В цьому випадку проекція швидкості V_y та координата y ТЕ, що летить, задається формулами

$$V_y = V_0 \cdot \sin \theta_0 - g \cdot t,$$

$$y = y_0 + V_0 \cdot t \cdot \sin \theta_0 - \frac{g \cdot t^2}{2}. \quad (1)$$

Коли ТЕ досягне точки A (рис. 1), тобто максимальної висоти підйому, проекція його швидкості на вісь Y буде рівною $V_y = 0$. Тоді час підйому до максимальної висоти $t_1 = V_0 \cdot \sin \theta_0 / g$. Враховуючи це значення максимальна висота польоту ТЕ дорівнює

$$H_{\max} = \frac{V_0^2 \cdot \sin^2 \theta_0}{2g}. \quad (2)$$

Якщо ТЕ кинутий з поверхні ґрунту ($y_0 = 0$), тоді загальний час польоту буде рівний часу підйому

$$T = \frac{2V_0 \cdot \sin \theta_0}{g} = 0,903 \sqrt{H_{\max}}. \quad (3)$$

Відстань L , яку пролітає ТЕ за певний час, визначається підстановкою часу t_0 польоту у залежність $x(t)$: $L = x_0 + V_0 \cdot t_0 \cdot \cos \theta_0$. При $x_0 = 0$ та $y_0 = 0$ дальність польоту ТЕ дорівнює

$$L = \frac{V_0^2 \cdot \sin 2\theta_0}{g}. \quad (4)$$

Максимальна дальність польоту тіла, яке кинуте з поверхні землі, згідно [7] досягається при куті кидання $\theta_0 = 45^\circ$, оскільки в цьому випадку $\sin 2\theta_0 = 1$.

Визначимо, по якій траєкторії рухається ТЕ, тобто складемо рівняння, яке зв'яже між собою координати ТЕ по осях x та y . Для цього виразимо час із залежності $x(t)$

$$t = \frac{x - x_0}{V_0 \cdot \cos \theta_0}$$

та підставимо його до формули (1)

$$y = y_0 + V_0 \left(\frac{x - x_0}{V_0 \cdot \cos \theta_0} \right) \cdot \sin \theta_0 - \frac{g}{2} \left(\frac{x - x_0}{V_0 \cdot \cos \theta_0} \right)^2 = y_0 + (x - x_0) \operatorname{tg} \theta_0 - \frac{g(x - x_0)^2}{2V_0^2 \cdot \cos^2 \theta_0}.$$

Якщо вибрати систему координат таким чином, що $x_0 = 0$, $y_0 = 0$, тоді формула спрощується

$$y = x \cdot \operatorname{tg} \theta_0 - \frac{g \cdot x^2}{2V_0^2 \cdot \cos^2 \theta_0}. \quad (5)$$

Врахування характеристик ТЕ та сили опору повітря швидкість польоту визначається виходячи із експоненціального закону затухання швидкості ТЕ при польоті тіла та здійснюється за виразом

$$V_x = V_0 \cdot \exp(-A \cdot x), \quad (6)$$

де A – балістичний коефіцієнт;

x – змінна координата відстані польоту ТЕ.

Коли політ ТЕ відбувається в умовах поступового збільшення ваги пристрою, що тралить, поточна швидкість польоту буде зменшуватись більш ніж при польоті тіла з постійною (не змінною) масою для таких саме умов. Це можна врахувати шляхом удосконалення виразу, який наведено в [7], для визначення балістичного коефіцієнта A . В роботі його пропонується визначати із врахуванням зміни маси пристрою, що тралить, за формулою

$$A(x) = \frac{\rho_{\text{п}} \cdot c_x \cdot \Phi}{\sqrt[3]{8\gamma_0^2 \cdot (m + 1 \cdot m_{\text{тр}})}} \approx \frac{\rho_{\text{п}} \cdot c_x \cdot \Phi}{\sqrt[3]{8\gamma_0^2 \cdot (m + x \cdot m_{\text{тр}})}}, \quad (7)$$

Література

1. Інформаційний бюлетень з протимінної діяльності у ході проведення АТО у Донецькій та Луганській областях. – К.: ГУОЗ, 2014. – 16 с. **2. Конвенція** про заборону застосування, накопичення запасів, виробництва і передачі протипіхотних мін та про їхнє знищення. – К.: Варта, 2004. – 25 с. **3. Закон України** від 22.12.04 №2281-IV “Про прийняття Протоколу про вибухонебезпечні предмети – наслідки війни”. **4. Спільний наказ** Міністра оборони України, Міністра України з питань надзвичайних ситуацій та в справах захисту населення від наслідків Чорнобильської катастрофи, Голови Державного комітету в справах

де $\rho_{\text{п}}$ – щільність повітря вздовж траєкторії польоту (для повітря дорівнює $1,293 \text{ кг/м}^3$);

c_x – коефіцієнт лобового опору;

γ_0 – щільність матеріалу ТЕ;

m – маса ТЕ;

Φ – параметр форми ТЕ;

l – змінна довжина тросу пристрою, що тралить, m (може бути прийнята $l \approx x$);

$m_{\text{тр}}$ – питома маса тросу, кг/м .

Тоді вираз (5) буде мати вигляд

$$V_x = V_0 \cdot \exp(-A(x) \cdot x). \quad (8)$$

Висновки й перспективи подальших досліджень

Таким чином, запропонована балістична модель, яка, на відміну від існуючих, враховує приріст питомої маси ЗТ під час польоту дозволить підвищити точність розрахунків під час обґрунтування балістичних параметрів засобів розмінування даного типу. Напрямами подальших досліджень є висвітлення результатів моделювання.

охорони Державного кордону України № 131\155\261 від 26.05.2008 року “Про організацію робіт щодо виявлення та знешкодження ВВП на території України”.

5. Дії підрозділів на території де можливе застосування саморобних вибухових пристроїв: Методичний посібник. – К.: ГУОЗ, 2012. – 57 с. **6. Ментус І. Е.** Ефективність інженерних боєприпасів: навчальний посібник. – Кам’янець-Подільський: ФВП ПДАТУ, 2008. – 80 с. **7. Кошкин Н. И.** Справочник по элементарной физике // [Н. И. Кошкин, М. Г. Ширкевич]. – М.: “Наука”, 1976. – 256 с.

БАЛЛИСТИЧЕСКАЯ МОДЕЛЬ ТРАЛЕНИЯ ВЗРЫВНЫХ УСТРОЙСТВ С НАТЯЖНЫМИ ДАТЧИКОМ ЦЕЛИ

¹Михаил Алексеевич Шишанов (д-р техн. наук, профессор)

²Владимир Иванович Коцюруба (канд. воен. наук, с.н.с, доцент)

¹Центральний науково-дослідницький інститут озброєння і військової техніки Вооруженных Сил України, Київ, Україна

²Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

На основе анализа существующих подходов по моделированию процессов разминирования, а именно использования средств для траления взрывных устройств с натяжным датчиком цели, предложена баллистическая модель, которая, в отличие от существующих, учитывает прирост текущей массы средства для траления взрывных устройств (комбинация тралящего элемента и троса) во время полета. Одним из наиболее сложных вопросов при моделировании является определение зависимости параметров полета тралящего элемента от динамики прироста массы троса. Баллистическими параметрами тралящего элемента, которые рассматриваются, являются: угол вылета, дальность, высота, время, скорость полета. Предложенные усовершенствования математической модели и последовательность проведения расчетов позволят повысить точность

результатов моделирования траления взрывных устройств с натяжным датчиком цели при обосновании требований к средствам разминирования данного типа. Направлением продолжения исследования в этой области является математическое моделирование процесса полета тралящего элемента, которые входят в состав средств траления взрывных устройств с натяжным датчиком цели, и обоснования, на основе использования его результатов, рациональных баллистических параметров.

Ключевые слова: баллистическая модель; взрывное устройство; натяжной датчик цели; траление; средство для траления.

BALLISTIC EXPLOSIVE SWEEPING MODEL WITH A PULL-ACTION TARGET-SENSOR

¹*Mykhailo O. Shyshanov (Doctor of Technical Sciences, Professor)*

²*Volodymyr I. Kotsiuruba (Candidate of Military Sciences, Senior Research Fellow, Associate Professor)*

¹*Central Research Institute of Armaments and Military Equipment of Armed Forces of Ukraine, Kyiv, Ukraine*

²*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

Based on the analysis of existing approaches to modeling processes of mine disarming, including the use of explosive sweeping devices with pull-action target-sensors, the ballistic model which, unlike the existing ones, takes into account the increase of instantaneous sweeping device weight (a combination of sweeping element and cable) during the flight was proposed. One of the most difficult issues in modeling is to determine flight parameters of sweeping element dependence on the weight gain dynamics of the rope. The investigated ballistic parameters of the sweeping element are the following: exit angle, distance, altitude, time, speed. The proposed improvements of the mathematical model and sequence of calculations will increase the accuracy of modeling the explosive sweeping process with a pull-action target-sensors during the validation of requirements to mine disarming devices of this type. Mathematical modeling of the flight process of the sweeping elements included in explosive sweeping with pull-action target-sensors and validation on the basis of its results, rational ballistic parameters, are the directions of the further research.

Keywords: ballistic model; explosive; pull-action target-sensor; sweeping; sweeping device.

References

1. Newsletter of mine action in the course of ATO in Donetsk and Luhansk regions. [*Informatsiyni biuleten z protyminnoi diialnosti u khodi provedennia ATO u Donetskii ta Luhanskii oblastiakh*], (2014), Kyiv: HUUZ, 16 p.
2. The Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction. [*Konventsiiia pro zaboronu zastosuvannia, nakopychennia zapasiv, vyrobnytstva i peredachi protypikhotnykh min ta pro yikhnie znyshchennia*], (2004), Kyiv: Varta, 25 p.
3. Law of Ukraine of 22.12.04 №2281-IV "On adoption of the Protocol on explosive remnants - of war".
4. Joint Order of the Minister of Defense of Ukraine, the Minister of Ukraine of Emergencies and Affairs of Population Protection from

the Consequences of Chornobyl Catastrophe, Head of the State Committee for State Border Protection of Ukraine number 131\155\261 of 26.05.2008, "On the organization works to identify and neutralize GDP in Ukraine."
5. Actions within the territory where the possible use of improvised explosive devices. [*Dii pidrozdiliv na terytorii de mozhyve zastosuvannia samorobnykh vybukhovnykh prystroiv*], (2012), Metodychnyi posibnyk, Kyiv: HUUZ, 57 p.
6. Mentus I.E. (2008), Efficiency Engineering ammunition. [*Efektivnist inzhenernykh boieprypasiv*], navchalnyi posibnyk, Kamianets-Podilskyi: FVP PDATU. 80 p.
7. Koshkyn N.Y., Shirkevich M.G. (1976), Handbook of elementary physics. [*Spravochnik po elementarnoi fizike*], Moscow: "Nauka", 256 p.

Отримано: 13.06.2016 року.

¹Дмитро Анатолійович Чопа (канд. техн. наук, с.н.с.)²Анатолій Йосипович Дерев'янчук (канд. техн. наук, професор)²Денис Русланович Москаленко²Дмитро Віталійович Бичко¹Національний університет оборони України імені Івана Черняхівського, Київ, Україна²Сумський державний університет, Суми, Україна

ПІДХІД ДО СТВОРЕННЯ WEB-ІНТЕРФЕЙСУ ІНФОРМАЦІЙНО-ДИСТАНЦІЙНО-ТРЕНАЖЕРНОЇ СИСТЕМИ

У статті розглядається підхід до створення моделі web-інтерфейсу інформаційно-дистанційно-тренажерної системи підготовки військових спеціалістів Ракетних військ і артилерії. Пропонується розглянути досвід кафедри військової підготовки Сумського державного університету у розробці web-орієнтованого програмного додатку, який дозволяє керувати та здійснювати взаємодію всіх складових інформаційно-дистанційно-тренажерної системи (ІДТС). Висвітлюється підхід та алгоритми створення потужного, гнучкого, функціонального web-інтерфейсу для оптимізації взаємодії компонентів ІДТС в цілому. Проаналізовані інструменти сучасних інформаційних технологій, необхідних для проектування якісних web-додатків, які дозволяють на початковій стадії виконання проекту обрати та реалізувати зазначений підхід. Наводиться функціональне забезпечення розроблюваного web-інтерфейсу, що надає можливості швидкого налагодження зв'язків між основними об'єктами ІДТС.

Ключові слова: web-інтерфейс; web-орієнтовані інформаційні технології; проектування інтерфейсного середовища; тренажерна online система підготовки військових спеціалістів.

Вступ

Постановка проблеми. З появою перших комп'ютерів у минулому столітті, був даний старт стрімкому розвитку комп'ютерних, та інформаційних технологій. Для отримання потрібної різноманітної інформації раніше необхідно було користуватися бібліотеками, архівами, використовувати складені конспекти тощо. Бурхливий розвиток комп'ютерних технологій, особливо мережі Інтернет змінює парадигму отримання необхідної інформації людством. Друковані інформаційні носії прискореними темпами витісняються їх електронними аналогами. Використовуючи "всесвітнє павутиння" люди мають можливість отримувати відкритий доступ до всілякої інформації та різних джерел, які допомагають нам всебічно розвиватися. Змінюються підходи до обробки та використання інформації у всіх сферах людської життєдіяльності. Не виключенням є сфера освіти, до якої стрімко впроваджуються сучасні інформаційні засоби для якісної підготовки майбутніх фахівців. Більш за все, це питання актуальне під час підготовки військових спеціалістів, особливо майбутніх офіцерів, що навчаються за програмою підготовки офіцерів запасу на кафедрах військової підготовки, оскільки насичений розклад занять та невелика кількість навчальних годин не дають можливості якісно засвоїти навчальну програму та отримати практичні навички.

Усі сучасні навчальні заклади мають власні системи, які надають можливість отримувати освітні послуги не виходячи із дому. Але між

військовою підготовкою та звичайною вищою освітою – існує "прірва", яка стала особливо помітною під час проведення антитерористичної операції на сході України. В ході мобілізації до лав Збройних Сил України було призвано велику кількість військовослужбовців запасу, у тому числі випускників-офіцерів кафедр військової підготовки, військовозобов'язаних з невеликим строком служби різного командного складу, рівень підготовки яких виявився недостатнім для виконання бойових задач. Зі сказаного вище випливає, що держава потребує висококваліфікованих військових спеціалістів, в тому числі і офіцерів запасу, які мали б якісні знання та навички, і які можуть бути відновленими швидко та самостійно під час особливого періоду.

Однією із проблем відновлення знань військовослужбовцями запасу є відсутність не тільки відповідної літератури (технічних описів, керівництв з експлуатації озброєння і військової техніки (ОВТ), пам'яток, альбомів рисунків тощо), але й відсутність комплектів ОВТ, тренажерів, що надали б можливість здійснювати тренування і набуття практичних навичок за умови віддаленості від місця дислокації основних підрозділів.

На нашу думку, поряд із використанням традиційних форм навчання, впровадження у систему підготовки військових фахівців комп'ютерних технологій, зокрема 3D моделей, розробка та широке застосування інформаційно-дистанційно-тренажерних систем (ІДТС) призведе до зростання рівня професійної підготовки і якості навчання військових спеціалістів, формування у них первинних практичних навичок, отримання знань на протязі тривалого часу. Наприклад,

створення ІДТС дозволяє вивчати ОВТ навіть без реальних зразків. 3D модель максимально відображає будову усіх вузлів і механізмів зразка, моделює процеси і явища які відбуваються у середині (наприклад, за бронєю, корпусом, кожухом тощо).

Отже пошук і визначення підходів до удосконалення підготовки військовослужбовців запасу у особливий період є актуальною науковою задачею, оскільки її вирішення дозволить зробити попередні висновки про доцільність створення та використання ІДТС.

Мета статті. Аналіз проблемних питань у розробці зручного та достатньо функціонального web-інтерфейсу для функціонування ІДТС та проблем створення і реалізації закритого ресурсу підготовки військових спеціалістів у особливий період з віддаленим доступом, використовуючи сучасні інформаційні технології.

Останні дослідження та публікації. Застосування лише традиційних методів навчання вже не відповідає сучасним вимогам до військових спеціалістів, особливо до тих, хто знаходиться у зоні АТО, оскільки вони не забезпечують

достатніх знань слухачам. Тому пошук нових прийомів і методів підвищення якості навчання військовослужбовців, які знаходяться за межами ВВНЗ, навчальних центрів, полігонів присвячена низка робіт. Так, в роботі [1] проведений аналіз різних моделей створення дистанційного навчання. У роботі [2] розглянуто підхід до створення адаптивних систем оцінки знань слухачів. У роботах [3,4] здійснено аналіз різних підходів щодо розробки матеріалів дистанційного навчання, є спроби застосування тренажерів у системі дистанційного навчання [5]. Однак порушення питань щодо створення ІДТС у сучасних публікаціях не виявлено.

Виклад основного матеріалу дослідження

Сьогодні існують деякі системи, що дозволяють віддалено проводити підготовку фахівців. У рамках статті буде розглянуто web-інтерфейс – один із складових компонентів цілісної ІДТС та будуть надані основні етапи його створення (Рис.1), для функціонування та управління ІДТС.

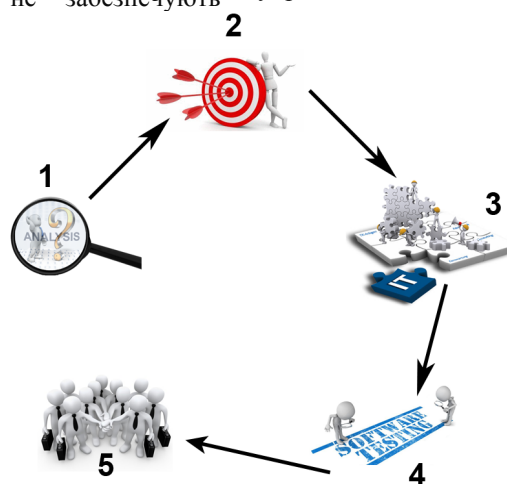


Рис. 1. Схема етапів створення web-інтерфейсу

Для створення будь-якого програмного продукту необхідно:

1. Провести аналіз предметної області та дослідження ринку продукту стосовно наявності аналогу. Необхідно для отримання інформації для створення та розвитку ідеї майбутнього проекту і можливості створення його унікальним.

2. Створити модель, яка зможе наглядно показати майбутній “результат”. Уявлення чітких меж можливостей, які має продукт, що розроблюється, для представлення конкретного переліку завдань та функцій засобу, який створюється. Такий принцип дозволяє виконувати всі подальші етапи в рамках умовного “контейнера”, не виходячи за його межі.

3. Здійснити реалізацію моделі засобами інформаційних технологій. Це безпосередній етап, на якому виконується весь перелік робіт технічних робіт зі створення web-інтерфейсу.

4. Етап тестування програмного продукту. Включає в себе проведення всіх необхідних заходів для виявлення та усунення проблем у

роботі та функціонуванні продукту, що розроблюється.

5. Впровадження програмного засобу в експлуатацію. Етап являє собою розгортання розробленої частини або системи в цілому на апаратно-технічних засобах (комп’ютерний клас з робочими місцями, сервер тощо) та комплекс мір для підготовки персоналу, який обслуговує систему.

представлений вище підхід застосовується як для розробки окремих частин ІДТС, так і системи в цілому.

Створення ІДТС має на меті: зібрання всієї наявної інформації в одному місці; отримання доступу слухачами до всього навчального матеріалу в межах підготовки за спеціальністю; отримання консультацій викладачів кафедри в режимі online; отримання як теоретичних знань, так і відпрацювання практичних питань на online тренажерах; реалізація автоматизованого контролю отриманих знань і навичок.

Виходячи із вище наданих міркувань, вдалося створити унікальний продукт, в якому поєднуються теоретичні і практичні процеси, та ігровий аспект процесу навчання (кожен слухач має власного підлеглого, якого можна “прокачати”, використовуючи зароблені бали під час проходження завдань).

Як відомо, дистанційне навчання – це інформаційна система, яка дозволяє отримати якісні знання, навчаючись у зручний час у будь-якому місці.

ІДТС має закритий доступ. За допомогою аутентифікаційних даних (логіну (login) та паролю (password)), користувач через web-інтерфейс може здійснювати вхід до ІДТС, де може вільно користуватися усіма ресурсами. Дані для входу у систему унікальні, генеруються для кожного користувача системи адміністратором та видаються кожному користувачу окремо. Для зручності користування web-інтерфейс розробляється на 2 мовах: українській та російській.

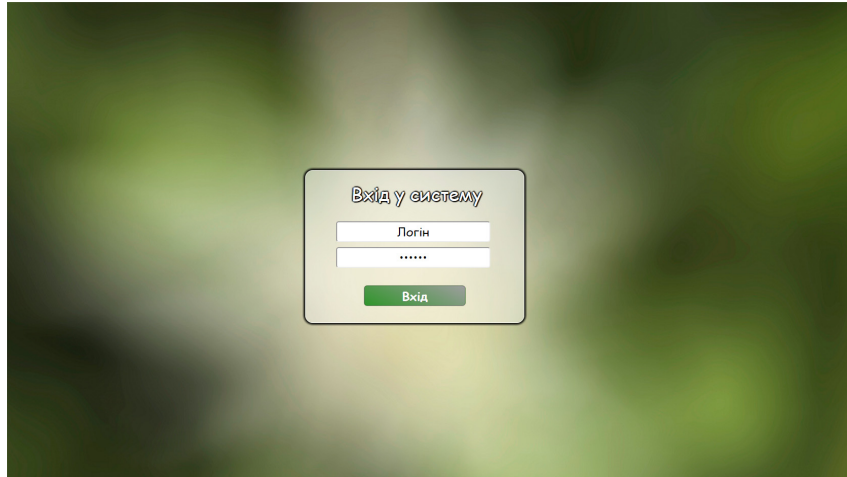


Рис. 2. Вікно введення аутентифікаційних даних у ІДТС.

Програмним інструментарієм інформаційних технологій для роботи з графічним контентом створюється ескіз – шаблон для розміщення компонентів web-інтерфейсу, який згодом програмується.

Наступним кроком є створення зовнішнього графічного вигляду безпосередньо web-інтерфейсу, через який користувач може використовувати всі функції ІДТС, а адміністратор здійснювати управління та наповнення ІДТС новими матеріалами.

Для подальшого функціонування створеної візуалізації, відбувається її кодування мовами PHP, JavaScript, CSS, HTML, що дозволяє

отримувати доступ до web-інтерфейсу ІДТС із браузера.

Так як доступ до web-інтерфейсу здійснюється лише з ПК, то доцільно використовувати “гнучкий” макет. Розроблений web-інтерфейс підтримує роботу з усіма сучасними браузерами Google Chrome, Opera, Firefox, Internet Explorer, а його головною перевагою є підтримка різної роздільної здатності екрану. Web-інтерфейс автоматично пристосовується до розміру екрана користувача, а функції “min-width” і “max-width” дозволяють обмежити ширину екрану, що надає можливість контенту завжди знаходитися у полі зору користувача (Рис. 3).

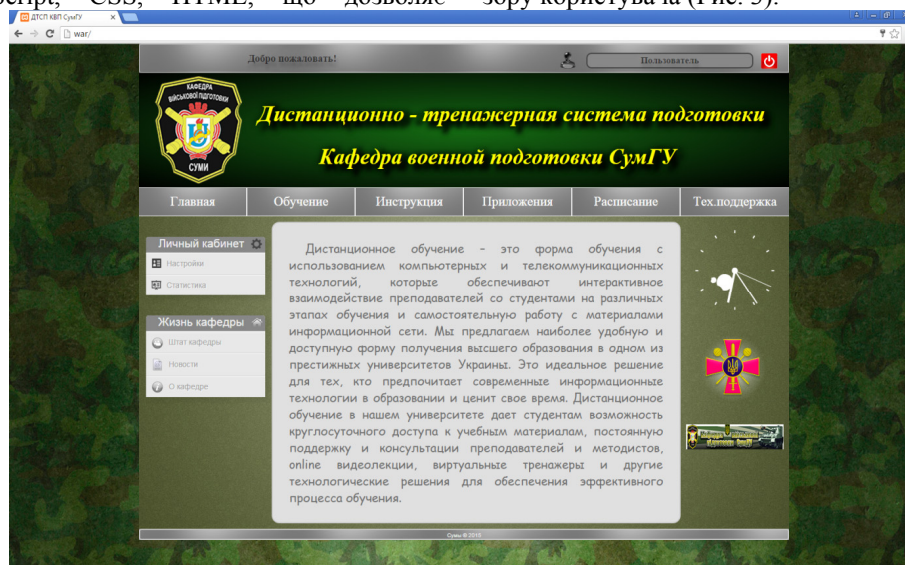


Рис. 3. Головна сторінка web-інтерфейсу ІДТС

За допомогою JavaScript, підключається функція “Click to Call”, що дозволяє спілкуватися та обмінюватися текстовими повідомленнями з

викладачами або адміністрацією, використовуючи “Skype” (Рис.4).

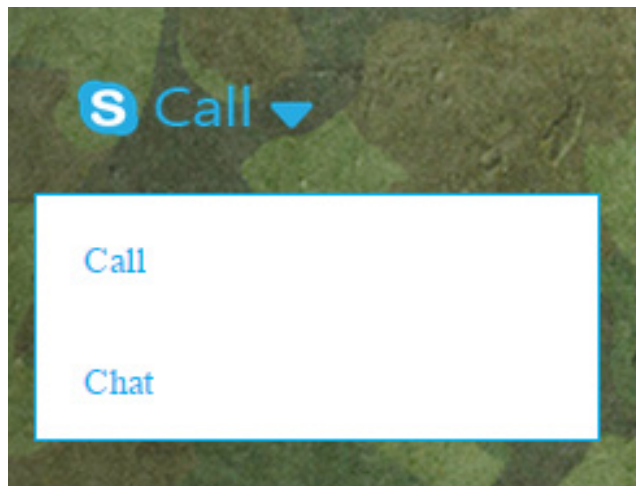


Рис 4. Реалізація функції “Click to Call”.

Наявність функції online спілкування, дозволяє проводити заняття, консультації з одним або групою користувачів в режимі реального часу не виходячи з ІДТС у будь-якому місці.

Web-інтерфейс підтримує роботу з модулями, які містять інтерактивну 3D графіку, що дає можливість відпрацьовувати практичні навички в online режимі, наприклад збирати або розбирати вузли та механізми артилерійських систем.

Висновки й перспективи подальших досліджень

Таким чином, виходячи з викладеного і результату дослідження проблеми, було розроблено концептуальну модель web-інтерфейсу

ІДТС на базі web-орієнтованих інформаційних технологій. Web-інтерфейс розроблений максимально зручним та гнучким для роботи, управління та налагодження ІДТС. Web-інтерфейс не має залежності від типу апаратного і виду програмного забезпечення, що встановлений на комп'ютері, та має можливість працювати в умовах високої завантаженості локальних мереж.

Подальші дослідження у даному напрямку полягають у розробці мобільного додатку на базі Android OS, Mac OS, що надасть можливість користуватися ІДТС за допомогою сучасні мобільних гаджетів.

Література

1. **Рябцев В. В.** Модель дистанційного навчання у національному університеті оборони України Ж // “Сучасні інформаційні технології в сфері безпеки та оборони” - №1(14) С. 35, Київ, 2009.
2. **Дерев'янчук А. Й., Баранова І. В., Москаленко Д. Р., Горайнов Д. Ю.** Підхід до створення адаптивних систем оцінки знань при підготовці військових спеціалістів, “Сучасні інформаційні технології в сфері безпеки та оборони” - №2(17) С. 115-119, Київ-2013.
3. **Віртуальний університет:** Навч.-метод. посібник / М. Козяр, О. Зачко, Т. Рак. – Львів: Львів. Держ. ун-т безпеки життєдіяльності, 2009. – 168 с.
4. **Шуневич Б.**

Методичне забезпечення для практичних занять з дисципліни “Теорія і практика дистанційного навчання” // Проблеми та перспективи розвитку економіки і підприємництва та комп'ютерних технологій в Україні: Збірник матеріалів V міжвузівської науково-технічної конференції науково-педагогічних працівників, м. Львів, 15 березня – 31 квітня 2010 року. – Львів: Вид. відділ Інституту підприємництва і прогресивних технологій, 2010. – С. 303-304.

5. **Сумцов Д. В.** Дистанційне навчання. Основи, концепції, перспективи / Д. В.Сумцов, І. О. Романенко, В. В. Калачова, О. П. Сук – Харків: НТУ “ХПІ”, 2010. – 284 с.

ПОДХОД К СОЗДАНИЮ WEB-ИНТЕРФЕЙСА ИНФОРМАЦИОННО-ДИСТАНЦИОННО-ТРЕНАЖЕРНОЙ СИСТЕМЫ

¹Дмитрий Анатолиевич Чопа (канд. техн. наук, с.н.с.)

²Анатолий Йосифович Деревянчук (канд. техн. наук, профессор)

²Денис Русланович Москаленко

²Дмитрий Витальевич Бичко

¹Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

²Сумской государственной университет, Сумы, Украина

В статье рассматривается подход к созданию web-интерфейса информационно-дистанционно-тренажерной системы подготовки (ИДТС, военных специалистов Ракетных войск и артиллерии. Предлагается рассмотреть опыт кафедры военной подготовки Сумского государственного

университета в области разработки web-ориентированного приложения, которое позволяет управлять и осуществлять взаимодействие всех компонентов ИДТС. Рассматриваются подход та алгоритмы создания мощного, гибкого, функционального web-интерфейса для оптимизации взаимодействия компонентов ИДТС в целом. Проанализированы инструменты современных информационных технологий, необходимых для проектирования качественных web-приложений, позволяющих на начальной стадии реализации проекта выбрать и реализовать указанный подход. Представляется функциональное обеспечение разрабатываемого web-интерфейса, имеющее возможности установления быстрой связи между основными объектами ИДТС.

Ключевые слова: web-интерфейс; web-ориентированные информационные технологии; проектирование интерфейсной среды; online тренажерная система подготовки военных специалистов.

THE APPROACH TO THE CREATION OF THE WEB-INTERFACE INFORMATION AND REMOTE-TRAINING SYSTEMS

¹*Dmytro A. Chopa* (Candidate of Technical Science, Senior Research Fellow)

²*Anatoli Y. Derevianchuk* (Candidate of Technical Sciences, Professor)

²*Denys R. Moskalenko*

²*Dmytro V. Bychko*

¹*National Defense University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine*

²*Sumy State University, Sumy, Ukraine*

The article discusses the approach to creating web-interface information and distance-training systems (IDTS) training of Artillery specialists. It is proposed to consider the experience of the department of military training Sumy State University in the development of web-based application that allows to manage and implement the interaction of all components IDTS. We consider approach and algorithms create a powerful, flexible, functional web-interface for optimization of IDTS components interaction as a whole. Been analyzed tools of modern information technologies required for the design of high-quality web-applications that allow to select and implement the indicated approach at the initial stage of the project. Proposed the obtaining of experience having the possibility of establishing a quick connection between the general objects of IDTS.

Keywords: web-interface; web-oriented IT; design the environment interface; online simulator system for training military specialists.

References

- 1. Ryabtsev V.V.** (2009). "The model of distance education at the National University of Defense of Ukraine." [Model' dystantsiynoho navchannya u natsional'nomu universyteti oborony Ukrayiny], Modern Information Technologies in the Sphere of Security and Defence, No.1(4), Kyiv, pp. 35-42.
- 2. Derevyanchuk A.Y., Baranova I.V., Moskalenko D.R., Goryanov D.Y.** (2013). The approach to creation of adaptive knowledge testing systems when training of military specialists. [Pidkhid do stvorennya adaptivnykh system otsinky znan' pry pidhotovtsi viys'kovykh spetsialistiv], Modern Information Technologies in the Sphere of Security and Defence, No.2(17), Kyiv, pp. 115-119.
- 3. Kozyar M., Zachko, O., Rak T.** (2009). Virtual University. [Virtual'nyy universytet], Textbook, Lviv, State University of Life Safety, pp. 168-172.
- 4. Shunevich B.,** (2010), Methodological support for practical training on discipline. Theory and practice of distance education. [Metodychne zabezpechennya dlya praktychnykh zanyat' z dystsypliny. Teoriya i praktyka dystantsiynoho navchannya], Problems and prospects of the economy and business and computer technology in Ukraine: Proceedings of the V Interuniversity scientific conference of teaching staff, Lviv, Department of the Institute of Entrepreneurship and advanced technology, pp. 303-304.
- 5. Sumtsov D.V., Romanenko I.O., Kalachova V.V., Suk O.P.** (2010). Distance Learning. Fundamentals, concepts, perspectives. [Dystantsiine navchannia. Osnovy, kontseptsii, perspektyvy], Kharkov, STU "KPI", pp. 284-290.

Отримано: 20.07.2016 року.

¹Леонід Михайлович Артюшин (д-р техн. наук, професор)²Тимур Ленурович Куртсеитов (д-р техн. наук)²Володимир Іванович Мірненко (д-р техн. наук, професор)³Ольга Леонідівна Сидорчук (канд. техн. наук)¹Державний науково-дослідний інститут авіації, Київ, Україна²Національний університет оборони України імені Івана Черняхівського, Київ, Україна³Житомирський військовий інститут імені С.П. Корольова, Житомир, Україна

МОЖЛИВОСТІ ЗАСТОСУВАННЯ ПРОТИРАДІОЛОКАЦІЙНИХ ПОКРИТТІВ У АНТЕННИХ СИСТЕМАХ ЗАСОБІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ З МЕТОЮ ЗМЕНШЕННЯ ЇХ РАДІОЛОКАЦІЙНОЇ ПОМІТНОСТІ

Наведено результати аналізу досліджень про можливість застосування протирадіолокаційних покриттів для зниження радіолокаційної помітності антенних систем засобів озброєння і військової техніки. Розглянуто відомі підходи зниження радіолокаційної помітності озброєння і військової техніки, методи і способи застосування протирадіолокаційних покриттів, що використовуються для зниження радіолокаційної помітності антенних систем озброєння і військової техніки. Доведено, що для реалізації пропонованих способів зниження радіолокаційної помітності проєктованих антенних систем, необхідно здійснювати оптимальний підбір габаритних розмірів антен і матеріалів для їх виготовлення на їхню абсолютним діелектричним і магнітної проникності, а також амплітудно-частотних характеристиках. Показані приклади конструктивних рішень впровадження радіопоглинаючих матеріалів і їх інтерференційних властивостей в нових конструкціях рупорних опромінювачів дзеркальних антенних систем, що дозволило знизити їх радіолокаційну помітність.

Ключові слова: радіолокаційна помітність; рупорний опромінювач; антена система; протирадіолокаційні покриття; зниження ефективної поверхні розсіювання

Вступ

Постановка проблеми. Одним з основних напрямків розвитку сучасних засобів озброєння і військової техніки (ОВТ) є створення літаків, безпілотних літальних апаратів, зразків наземної (бронетанкової) військової техніки та кораблів з малою радіолокаційною помітністю, що оцінюється значенням їх ефективної поверхні розсіювання (ЕПР). Проте більшість сучасних об'єктів ОВТ оснащено значною кількістю антенних систем і, за ствердженням багатьох джерел, саме антени виступають основним джерелом високих рівнів їх ЕПР [1–5].

Спроби вирішення проблеми створення техніки і об'єктів, що є малопомітними для радіоелектронних засобів (РЕЗ) проводились з часів початку розвитку радіорозвідки. У зв'язку з цим з'явилося поняття – радіоелектронний захист, що передбачає комплекс технічних рішень, направлених на зниження радіорозвідки противника [3–5]. У свою чергу, радіоелектронний захист проводиться шляхом тактичного маскуванню дій військових частин (підрозділів) для забезпечення їх прихованості та досягається застосуванням табельних засобів маскуванню і місцевих матеріалів, розсіювальних (поглинаючих) покриттів, матеріалів (конструкцій), видозмінюванням озброєння і військової техніки [3,4].

Аналіз останніх досліджень і публікацій. Радіоелектронний захист наземних рухомих РЕЗ в умовах розгортання згідно з інструкцією, наведено на рис. 1. У ході антитерористичної операції він проводиться шляхом пасивного захисту радіолокаційної станції (РЛС), як приклад – капонуванням (окопуванням) у рівень з висотою машини до 2,4 м з однією або двома апарелями. Таким чином, для зондуючої літакової бортової радіолокаційної станції (ЛБРЛС) ЕПР кунга або причепа буде дорівнювати площі Міделя ($S_{\text{Міделя}}$) його верхньої частини. Наприклад для Урала 375-Д вона буде досить малою і не інформативною з точки зору радіолокаційного портрету станції. У такому випадку саме за відбитою потужністю практично лише від антенної системи буде визначатися ймовірність виявлення всієї наземної РЛС зондуючою ЛБРЛС противника.

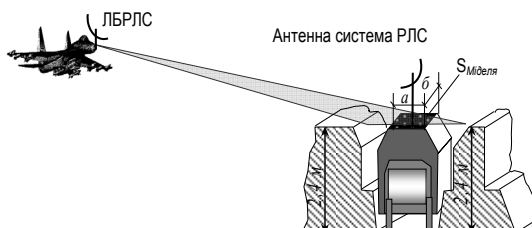


Рис. 1. Приклад радіоелектронного захисту РЛС на базі Урала-375-Д капонуванням у рівень з висотою машини до 2,4 м з двома апарелями.

Рівень зменшення помітності засобу ОВТ передбачає зменшення потужності відбитого сигналу (Дб) та нормується до еталону у м². Такі дослідження належать до Стелс-технологій (Stealth technology) та проводяться у радіолокаційному, інфрачервоному та інших областях спектра виявлення (рис. 2) шляхом системного підходу функціонально-структурного проектування із застосування спеціально розроблених геометричних форм, радіопоглинаючих матеріалів і покриттів тощо та оптимізації розсіювання від усієї системи [4,6]. Це дозволяє зменшити силу відбитого сигналу у бік джерела випромінювання і за рахунок цього лишатися непоміченим. Однак суттєвого результату у зниженні радіовидимості можна досягти лише у випадку різкого зниження ЕПР. Так зменшення ЕПР об'єкта ОВТ у 16 разів скорочує дальність його радіолокаційного виявлення лише у 2 рази [5].

Напрямки функціонально-структурного проектування складних технічних систем засобів ОВТ за технологією “Стелс” на основі системного підходу наведено на рис. 2. Вони включають:

- теорію дифракції електромагнітних хвиль на тілах складної форми;
- дослідження протирадіолокаційних покриттів;
- оцінку ефективності заходів, щодо зниження ЕПР об'єкта ОВТ, у тому числі до складу якого входять антенні системи.

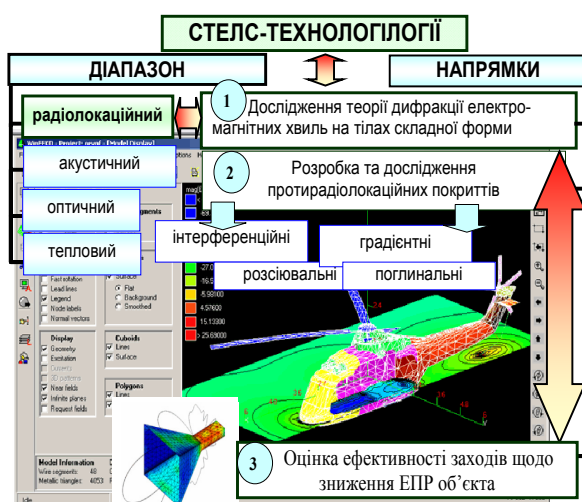


Рис. 2. Напрямки функціонально-структурного проектування технічних систем засобів ОВТ за технологією “Стелс”

Дослідження за технологією “Стелс”, що передбачають застосування протирадіолокаційних покриттів, технології їх нанесення, оцінка ефективності заходів, щодо зниження ЕПР об'єкта з такими покриттями було розпочато для зменшення ЕПР повітряних засобів. Однак, останніми роками, такі технології поширено практично на всі об'єкти ОВТ [3]. У [4] надано наступне формулювання. Протирадіолокаційними покриттями називаються матеріали, призначені для нанесення на об'єкти з ціллю суттєвого зниження їх ЕПР або викривлення характеристик

відбитого поля. За видами вони бувають: інтерференційні, поглинаючі, невідбиваючі структури та комбіновані.

У іншому джерелі [5] під протирадіолокаційними покриттями розуміють неметалеві матеріали, що забезпечують при взаємодії з електромагнітними хвилями поглинання, розсіювання і інтерференцію енергії. За принципом дії їх розділяють на градієнтні і інтерференційні.

Градієнтними [5] широкодіапазонними поглинаючими матеріалами покривають малорухомі або нерухомі об'єкти і споруди (кораблі, мости). Транспортні засоби ОВТ, що розгорнуті на місцях для виконання завдань (кунги, причепи) можуть покриватися градієнтними матеріалами із пористого каучуку, що змішаний з вугільним пилом, або пінополістиролу, вкритого вугільною плівкою для зменшення їх ЕПР. В результаті твердості такого покриття інтенсивність відбиття мало залежить від кута падіння радіохвиль, тому коефіцієнт їх відбиття не перевищує одного відсотку потужності [5].

Інтерференційні покриття [5] за принципом дії пов'язані із довжиною хвилі, що падає і тому ефективні лише в обмеженому діапазоні радіохвиль. Такі покриття можуть складатися з електропровідної плівки, що прошарками накладання падаючої плоскої хвилі на прошарок плівки та відбиття від діелектрика виникають стоячі хвилі, які блокують перевипромінювання. Зазвичай покриття роблять багат шаровими і концентрацію радіопоглинаючого матеріалу збільшують від одного шару до іншого. Таким чином робочий діапазон покриття збільшується у 3-4 рази за нормальної поляризації падаючої хвилі, а відбита енергія має послаблення у декілька десятків разів. За інших напрямків інтенсивність відбиття різко падає [5]. До інтерференційних належать: пластмасові покриття, що складаються з фазового зсувного прошарку з поглинаючого і розсіюючого слоїв; металеві сітки, що розміщені на відстані чверті хвилі ($\lambda/4$) від об'єкта; діелектричні матеріали, нанесені на металеву поверхню та ін. [5].

Загальним недоліком, що обмежує застосування практично усіх протирадіолокаційних покриттів для маскування техніки і об'єктів є мала діапазонність і значна маса. Тому їх наносять на ті частини об'єктів і засобів ОВТ, що найбільш відбивають електромагнітну енергію. Такі місця називають блискучими точками. До них належать стики, різкі переходи, що діють як кутові відбивачі, гострі кромки та інше [5].

Найбільш суттєвою блискучою точкою на військових радіотехнічних об'єктах зазвичай є їх антенна система. Наприклад внесок антенної системи станції П-18 за деяких ракурсів спостереження може складати до 98% від

загальної ЕПР об'єкта. До того ж саме технічні характеристики антенної системи визначають дальність дії радіотехнічних засобів і за принципом оберненості відповідають і за дальність її виявлення радіорозвідкою противника. Таким чином найбільш демаскуючим елементом, особливо в умовах зниження радіолокаційної помітності радіотехнічного зразка ОВТ, є саме його антенна система [6-12].

Відомі підходи до зменшення радіолокаційної помітності зразків ОВТ за рахунок видозмінювання їх форми, повного покриття радіопоглинаючим матеріалом тощо є непридатними для зниження ЕПР їх антенних систем [4,5,7-11]. Складність полягає у неможливості уникнути перевипромінювання, оскільки за своєю специфікою будь яка антена розсіює не менше половини падаючої на неї енергії [1,2,6]. Також відомо, що якщо в антенну систему поступає деяка потужність, то це може мати місце лише за наявності розсіювання. Розсіяна антеною потужність перевищує прийняту, або дорівнює їй [1,2,7,9]. Тому найчастіше у багатьох джерелах припускалось, що застосування протирадіолокаційних покриттів для об'єктів є непридатним для зменшення ЕПР їх антенних систем [4,7,8].

Аналіз досліджень можливості практичної реалізації застосування протирадіолокаційних покриттів для нових антенних систем показує наступне. Заходи із застосуванням радіопоглинаючих матеріалів для зниження радіолокаційної помітності антен у багатьох випадках утруднені, оскільки такі матеріали, нанесені на антену, поряд із поглинанням електромагнітного випромінювання РЛС розвідки порушують нормальне функціонування антени у робочому діапазоні хвиль. Тому перспективні способи і засоби зменшення ЕПР умовно поділено на три групи [4,8,11].

Перша група ґрунтується на екрануванні антен частотно-поляризаційно-селективними структурами з незмінними у часі параметрами або нанесенні таких структур на робочі ділянки антен, наприклад на дзеркало антенної системи. Такі структури прозорі або відбивають як метал на робочих частотах або поляризаціях антени та непрозорі, або сильно поглинають на всіх інших частотах або поляризаціях. Вказані структури можна виконати на базі плоскошарових середовищ із незмінними параметрами, що складаються з прилеглих один до одного слоїв радіопрозорого діелектричного матеріалу [5,8,11].

Друга група штучно погіршує характеристики антен у неробочі проміжки часу шляхом змінювання властивостей проходження або відбиття електромагнітної хвилі за рахунок прикриття антен електрично-керованими у часі середовищами або дистанційно керованими металевими екранами. У робочі проміжки часу антенні характеристики відновлюються [5,8,11].

Третя група мініатюризує антени при збереженні їх основних робочих характеристик. В результаті за рахунок зменшення габаритних розмірів антен потужність вторинного випромінювання суттєво падає [5,8,11].

За огляду матеріалів друкованих видань [7,8,10-16] розглянемо можливості практичної реалізації способів зменшення ЕПР антен.

У [12] наведено метод зниження радіолокаційної помітності дзеркальних антенних систем шляхом застосування радіопоглинаючих матеріалів на окремих елементах ЛБРЛС переднього огляду, що використовуються на бойових літаках Миг-29, Су-24. Зниження помітності таких антен за рахунок надання ним спеціальної форми є неприйнятним, оскільки форма дзеркала визначається необхідністю формування направлено випромінювання антени. У такому випадку для дзеркальних антен на перше місце виступає застосування радіопоглинаючих матеріалів на зломах поверхні, основними з яких є кромка дзеркала. Вибір матеріалу і товщини радіопоглинаючого покриття, що наноситься на кромку дзеркала суттєво залежить не тільки від розмірів дзеркальної антени, але й від конкретного діапазону частот та кутів її опромінювання зондуючою РЛС [12]. Вплив опромінювача на загальну ЕПР антенної системи і можливості зниження його ЕПР у [12] не надано.

У [5] наведено короткий опис встановленого на дзеркалі антени захисного фільтру на основі плоскошарових середовищ, основною функцією якого є відбиття падаючої на нього електромагнітної хвилі у напрямленнях, що не співпадають з геометричною віссю антени. І знову про вплив опромінювача мова не йде.

У дослідженнях [13] пропонується винесення опромінювача вздовж фокальної осі на незначну відстань, за якої антенна система має прийнятний коефіцієнт корисної дії. Такі дії дійсно підвищують розвідзахищеність антенної системи, проте в області головної пелюстки діаграми спрямованості вплив опромінювача становить до 20 дБ від загальної ЕПР. Таким чином виникає проблема зменшення ЕПР самого опромінювача і, як варіант, пропонується нанесенням радіопоглинаючого матеріалу на його зовнішню поверхню [13].

Для зменшення радіолокаційної помітності резонансних антен короткохвильового та ультракороткохвильового діапазонів у [10] пропонується на металеві стрижні наносити прошарок радіопоглинаючого матеріалу, що не здійснює суттєвого впливу на амплітуду сигналу, який приймає антена [8]. Таким чином можна суттєво зменшити ЕПР, наприклад РЛС П-18, внесок антенної системи якої складає до 98% від загальної ЕПР всієї конструкції у передній півсфері [10]. Прошарок такого поглиначу підвищує поперечний перетин провідника, що трохи збільшує його ЕПР, але одночасно зменшує

довжину, що необхідна для резонансу на заданій частоті. Зменшення довжини вібратора разом із поглинанням енергії на заданій частоті знижує ЕПР у сантиметровому радіолокаційному діапазоні довжин хвиль. Експерименти, що проведено на макетах вібраторних антен, доводять можливість зменшення їх ЕПР до 15 дБ при дозволеному зниженні коефіцієнту корисної дії антени [8,10].

Таким чином в якості практичної реалізації перспективного способу зменшення ЕПР антен – їх мініатюризації при збереженні основних робочих характеристик було спроектовано нові антени, що наведено рис. 3, 4. Під час проектування використано теорію дифракції електромагнітних хвиль на тілах складної форми, властивості протирадіолокаційних покриттів та проведено оцінку ефективності заходів, щодо зниження ЕПР об'єкта ОВТ до складу якого входять подібні антенні системи.

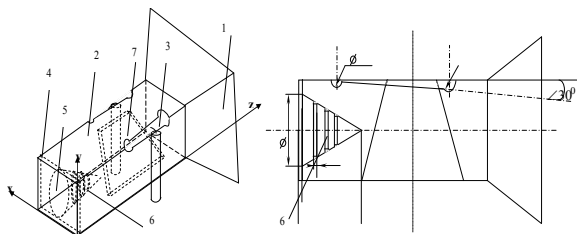


Рис. 3. Ескіз малогабаритної рупорної антени з конусоподібним поглиначем вищих гармонік

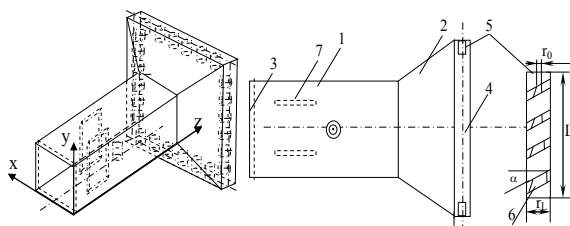


Рис. 4. Рупорна антена зі зменшеною ЕПР від кромки

За результатами дослідження нові конструкції доводять можливість впровадження радіопоглинаючих матеріалів та їх інтерференційних властивостей у антенні системи, що мають пірамідальний рупор у якості опромінювача. У сукупності з конструктивними змінами це дозволяє знизити ЕПР таких антенних систем у найбільш небезпечному секторі кутів опромінення (передня півсфера) при збереженні інших основних характеристик.

Таким чином, метою статті є дослідження можливості застосування протирадіолокаційних покриттів у проектуванні нових антенних систем засобів ОВТ з метою зменшення їх радіолокаційної помітності.

Виклад основного матеріалу дослідження.

Як приклад застосування радіопоглинаючих матеріалів та їх інтерференційних властивостей на рис. 3. наведено малогабаритну рупорну антену з конусоподібним поглиначем вищих гармонік (патент на винахід № 96661 від 13.07.2011).

В основу винаходу поставлено задачу вдосконалення рупорної антени колової поляризації з метою зменшення її ЕПР. Спільними елементами конструкції антени прототипу та антени-винаходу є послідовно встановлені пірамідальний рупор 1 та відрізок квадратного хвилеводу 2 з фазуючою секцією, по кутах якої прорізані дві довгі гантелеподібні щілини 3, які навантажено коаксіальними лініями, а на короткозамкненій стінці встановлено поглинаюче навантаження 4.

На відміну від прототипу запропонована конструкція (рис. 3) має введений діелектричний конус 5 з поглинаючими канавками 6, прикріплений до поглинаючої пластини 2. Для створення колової поляризації встановлено фазуючу секцію 7, яку виконано у вигляді трапецієподібної діелектричної пластини та розміщено по діагоналі квадратного відрізка хвилеводу 2. Поглинаючі канавки заповнено градієнтним матеріалом. Для проведення експерименту в якості радіопоглинаючого матеріалу використано хром та звичайну сажу [16].

Експеримент показав, що завдяки введенню додаткового хвилеводного навантаження у вигляді діелектричного конуса з поглинаючими канавками зменшується рівень відбитої хвилі, що призводить до зменшення ЕПР антени. Фазуюча трапецієподібна діелектрична пластинка окрім забезпечення колової поляризації поліпшує узгодження хвилеводу з довгими неоднорідними гантелеподібними щілинами. Таким чином запропонована рупорна антена колової поляризації працює у широкій смузі частот (більше 35%), має добре узгодження двох довгих неоднорідних гантельних щілин з відрізком квадратного хвилеводу і суттєво меншу ЕПР.

Проведені дослідження запропонованої антени у діапазоні 8-12 ГГц довели, що значення її ЕПР в області головної пелюстки діаграми спрямованості було зменшено на 12 дБ, порівняно з 20 дБ штатної антени. Коефіцієнт еліптичності складав 0,82-0,85 дБ, коефіцієнт стоячої хвилі по навантаженню коливався 1,25-1,3 а втрати були 0,5-0,7 дБ.

На рис. 4 наведено інший приклад впровадження градієнтних та інтерференційних радіопоглинаючих покриттів для рупорних опромінювачів (патент № 97037 від 26.12.2011).

На відміну від прототипів, що містять відрізок прямокутного хвилеводу 1, пірамідальний рупор 2 і поглинаюче навантаження 3, нова конструкція антени містить прямокутний поглинаючий фланець у вигляді каркасу 4 вздовж сторін якого встановлена решітка циліндричних діелектричних стрижнів довжиною, що дорівнює чверті хвилі $\lambda/4$ в діелектрику. Під кутом α до твірної циліндра прорізані канавки 6 в які напилена металева плівка, а зміна радіусу канавок визначається виразом

$$\operatorname{tg} \alpha = \frac{\Gamma_L - \Gamma_0}{L}$$

де r_0 – радіус найменшої канавки,

r_L – радіус циліндричного діелектричного стрижня;

L – довжина циліндричного діелектричного стрижня.

Проведено експериментальне дослідження запропонованої конструкції антени (рис. 4) в діапазоні 8-12,5 ГГц. Для експерименту була зібрана установка з використанням ефекту Доплера. Для виділення відбитого від об'єкта сигналу на фоні завад – відбиттів від предметів, що знаходяться поруч, використано ефект зміни частоти через рух джерела електромагнітного випромінювання, що дозволило значно зменшити вплив відбиття від нерухомих об'єктів, а вплив випадкових варіацій було виключено.

Для проведення експерименту дослідний зразок нового опромінювача, а саме пірамідальний рупор 1 та відрізок квадратного хвилеводу 2 було виготовлено з міді. Діелектрична проникність матеріалу циліндричних діелектричних стрижнів 5 решітки 4 дорівнювала $2,4 \div 2,7$. Канавки, що прорізані у діелектричних стрижнях, заповнено металевою плівкою з хрому. За проведеними вимірюваннями з'ясовано, що однопозиційну ЕПР нової антени в області головної пелюстки діаграми розсіювання, що співпадає з напрямком діаграми спрямованості було знижено з 20 дБ до 8 дБ, у порівнянні з прототипом. Проте такі результати спостерігаються лише за кутів опромінювання нової антени $\theta = 0^\circ \dots 5^\circ$.

У роботі [6] наведено дослідження ЕПР рупорних антен [16], [17], з розмірами розкриття $a_p \times b_p \times l = (1,2 \times 1,5 \times 4)$, та кутом розкриття 20° .

На рис. 5 наведено порівняльний аналіз експериментальних і розрахункових даних нових конструкцій антен зі зменшеною ЕПР. Їх характеристики було знято на центральній частоті діапазону. Результати вимірювання однопозиційної ЕПР довели, що такі антени у 2-х сантиметровому діапазоні хвиль працюють з величиною втрат 0,5–0,6 дБ при коефіцієнті посилення ≈ 24 -25 дБ.

Література

1. Козлов Б. А. Справочник по расчёту надёжности аппаратуры радиоэлектроники и автоматики / Козлов Б. А., Ушаков И. А. – М.: Советское радио, 1975. – 472 с. 2. Гнеденко Б. В. Вопросы математической теории надёжности. / Гнеденко Б. В., Беляев Ю. К., Коваленко И. А., Под редакцией академика АН УССР, Б. В. Гнеденко – М.: Советское радио, 1983. – 376 с. 3. Острейковский В. А. Теория надёжности – М.: Высшая школа, 2003. – 463 с. 4. Половко А. М. Основы теории надёжности. Практикум / Половко А. М., Гуров С. В. – СПб.: БХВ-Петербург, 2006. – 559 с. 5. Беляев Ю. К. Надёжность технических систем, Справочник / Беляев Ю. К., Богатырёв В. А., Болотин В. В. и др. Под редакцией И. А. Ушакова – М.:

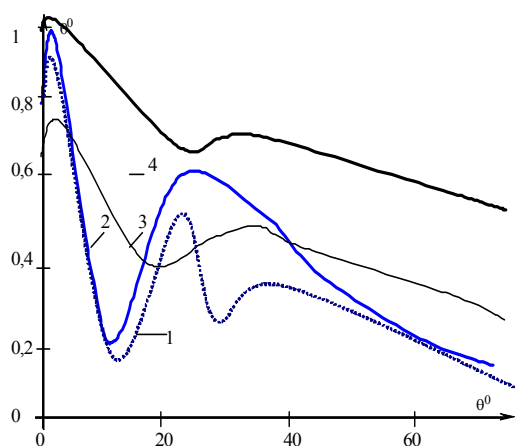


Рис. 5. Порівняльний аналіз розрахункових та експериментальних даних нових конструкцій антен: 1– антена, патент № 96661 – розрахункові дані; 2– антена, патент № 96661 – експериментальні дані; 3– антена, патент № 97037 – розрахункові дані; 4– антена, патент № 97037 – експериментальні дані.

ЕПР наведених на рис. 3 та 4 антен в області головної пелюстки було зменшено на 12,5 дБ [18]. Порівняння розрахункових даних і експериментальних доводить їх добру відповідність.

Висновки й перспективи подальших досліджень.

Таким чином проведено аналіз досліджень, щодо можливості застосування протирадіолокаційних покриттів для зниження радіолокаційної помітності антенних систем. Проте такі способи потребують оптимального підбору габаритних розмірів антен та матеріалів для їх виготовлення за їх абсолютними діелектричними та магнітними проникненнями, а також амплітудно-частотними характеристиками. Запропоновані та захищені патентами на винахід конструкції мають суттєво меншу ЕПР у порівнянні зі штатними антенними системами завдяки впровадженню нових конструктивних рішень, радіопоглинаючих матеріалів та їх інтерференційних властивостей. Це дозволить суттєво знизити радіолокаційну помітність об'єктів ОБТ до складу яких входять такі антени у найбільш небезпечному куті опромінювання – в передній півсфері.

Радио и связь, 1985. – 609 с. 6. Шышмарёв В. Ю. Надёжность технических систем – М.: Изд.центр Академия, 2010. – 304 с. 7. ДСТУ 3942-2000 (ГОСТ 27.506-2000). Надійність техніки. Плани випробувань для контролю середнього наробітку до відмови (на відмову). Частина 2. Дифузійний розподіл, 2001. – 36 с. 8. Стрельников В. П. О методических погрешностях прогнозирования ресурса высоконадёжных изделий электронной техники / В. П. Стрельников, К. А. Антипенко // Математичні машини і системи. – 2004. – №3 – С.164-167. 9. ДСТУ 2862-94. Надійність техніки. Методи розрахунків показників надійності. Загальні вимоги. – 1996. – 39 с.

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ПРОТИВОРАДИОЛОКАЦИОННЫХ ПОКРЫТИЙ В АНТЕННЫХ СИСТЕМАХ СРЕДСТВ ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ В ЦЕЛЯХ СОКРАЩЕНИЯ ИХ РАДИОЛОКАЦИОННЫХ ЗАМЕТНОСТИ

¹Леонид Михайлович Артюшин (д-р техн. наук, профессор)

²Тимур Ленурович Куртсейтов (д-р техн. наук)

²Владимир Иванович Мирненко (д-р техн. наук, профессор)

³Ольга Леонидовна Сидорчук (канд. техн. наук)

¹Государственный научно-исследовательский институт авиации, Киев, Украина

²Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

³Житомирский военный институт имени С.П. Королева, Житомир, Украина

Приведены результаты анализа исследований о возможности применения противорадиолокационных покрытий для снижения радиолокационной заметности антенных систем средств вооружения и военной техники. Рассмотрены известные подходы снижения радиолокационной заметности вооружения и военной техники, методы и способы применения противорадиолокационных покрытий, используемые для снижения радиолокационной заметности антенных систем вооружения и военной техники. Доказано, что для реализации предлагаемых способов снижения радиолокационной заметности проектируемых антенных систем, необходимо осуществлять оптимальный подбор габаритных размеров антенн и материалов для их изготовления по их абсолютным диэлектрическим и магнитным проницаемостям, а также амплитудно-частотным характеристикам. Показаны примеры конструктивных решений внедрения радиопоглощающих материалов и их интерференционных свойств в новых конструкциях рупорных облучателей зеркальных антенных систем, что позволило снизить их радиолокационную заметность.

Ключевые слова: радиолокационная заметность; рупорный облучатель; антенная система; противорадиолокационные покрытия; снижение эффективной поверхности рассеяния.

APPLICATION OF COATINGS CONFUSIONAL ANTENNA SYSTEM WEAPONRY AND MILITARY EQUIPMENT TO REDUCE THEIR RADAR SIGNATURE

¹Leonid M. Artyushyn (Doctor of Technical Sciences, Professor)

²Tymur L. Kurtseytov (Doctor of Technical Sciences)

²Volodymyr I. Mirnenko (Doctor of Technical Sciences, Professor)

³Ol'ha L. Sydorчук (Candidate of Technical Sciences)

¹State Scientific and Research Institute of Aviation, Kyiv, Ukraine

²National Defence University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine

³Zhytomyr Military Institute named after Sergei Korolev, Zhytomyr, Ukraine

Results of the research are given brought about possibility of application of antiradar coatings to reduce radar visibility of antenna systems of armament and military equipment. Describes the known approaches to reduce radar visibility of armament and military equipment, methods of application of antiradar coatings are used for the decline of radar visibility of the antenna systems of armament and military equipment. It is well-proven that for realization of the offered methods of decline of radar visibility of the designed antenna systems, it is necessary to carry out the optimal selection of overall sizes of aeriels and materials for their making on their absolute dielectric and magnetic permeabilities, and also gain-frequency characteristics. The examples of structural decisions of adsorbing materials introduction and their interference properties are shown in the new constructions of megaphone irradiators of the mirror antenna systems, that allowed to reduce their radar visibility.

Keywords: radar visibility; feed horn; the antenna system; antiradar coating; reducing the effective scattering surface.

References

1. Kozlov B.A., Ushakov I.A. (1975), Guide to the calculation of grade electronics and automation equipment. [Spravochnik po raschyotu nadyozhnosti apparaturyi radioelektroniki i avtomatiki], Moscow: Sovetskoe radio, 472 p.
2. Gnedenko B.V., Belyaev Yu.K., Kovalenko I.A. (1983), Questions mathematical reliability theory. [Voprosyi matematicheskoy teorii nadyozhnosti], Pod redaktsiyei akademika AN USSR, Moscow: Sovetskoe radio, 376 p.
3. Ostreykovskiy V.A. (2003), Reliability Theory. [Teoriya nadyozhnosti], Moscow: Vysshaya shkola, 463 p.
4. Polovko A.M., Gurov S.V. (2006), Fundamentals of reliability theory. Practicum. [Osnovy teorii nadyozhnosti. Praktikum], SPb.: BHV-Peterburg, 559 p.
5. Belyaev Yu.K., Bogatyryov V.A., Bolotin V.V. (1985), Reliability of technical systems. [Nadyozhnost tehnikeskikh sistem] Spravochnik Pod redaktsiyei I.A.Ushakova, Moscow: Radio i svyaz, 609 p.
6. ShyishmarYov V.Yu. (2010), Reliability of technical systems. [Nadyozhnost tehnikeskikh sistem], Moscow: Izd.tsentr Akademiya, 304 p.
7. DSTU 3942-2000 (GOST 27.506-2000), (2001), [Nadiynist tehniki. Plani viprobuvan dlya kontrolyu serednogo narobitku do vidmovi (na vidmovu). Chastina 2. Difuziyniy rozpodil], 36 p.
8. Strelnikov V.P., Antipenko K.A. (2004), On methodological errors of forecasting resource highly reliable electronic articles. [O Metodicheskikh pogreshnostyah prognozirovaniya resursa vyisokonadyozhnyih izdeliy elektronnoy tehniki], Matematichni mashini i sistemi, No.3, pp.164-167.
9. DSTU 2862-94. (1996), [Nadiynist tehniki. Metodi rozrahunkiv pokaznikov nadiynosti. Zagalni vimogi], 39 p.

Отримано: 23.06.2016 року.

ОСОБЛИВОСТІ ВЕДЕННЯ БОЙОВИХ ДІЙ У ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

В статті на основі аналізу тенденцій розвитку збройної боротьби визначені особливості ведення бойових дій у інформаційному середовищі. Сучасне інформаційне середовище має значний вплив на процес управління військами у ході ведення бойових дій та ведення бойових дій в цілому. Проведений аналіз дозволив визначити вплив інформаційного середовища на ведення бойових дій і визначити шляхи підвищення ефективності ведення бойових дій у сучасному інформаційному середовищі. Визначені підходи дозволять офіцерам органів військового управління переглянути свої погляди на процес прийняття рішень під час управління військами у ході ведення бойових дій у інформаційному середовищі.

Ключові слова: інформаційне середовище ведення бойових дій; управління військами; бойові дії; прийняття рішень.

Вступ

Бурхливий розвиток наприкінці ХХ і початку ХХІ століття інформаційних технологій, широка інформатизація суспільства і безпосередньо збройних сил провідних країн світу значно змінили характер, методи і способи діяльності державних, урядових політичних і економічних структур, вплинули на соціальні взаємозв'язки, характер, форми і способи ведення бойових дій, сформувавши нові інформаційні загрози та виклики.

Постановка проблеми. Фундаментальна зміна характеру, форм і способів ведення бойових дій вимагає розробки більш гнучкої стратегії застосування, будівництва та організації управління збройними силами, розробки доктрини ведення інформаційного протиборства, інформаційних операцій забезпечення інформаційної безпеки України та її Збройних сил.

Аналіз останніх досліджень і публікацій.

У Першій світовій війні бойові дії велися в основному у двох середовищах - у наземному і морському. У Другій світовій війні [2] до них додалося третє середовище - повітряне. ХХ століття стало століттям радіо. Радіозв'язок став основою управління збройними силами. Він зробив управління військами (силами) більш гнучким і оперативним, а війська - маневренішими, але більш уразливими. Разом з тим виникла перша реальна інформаційна загроза. Можливість радіоперехоплення і придушення перешкодами засобів радіозв'язку, радіолокації і радіонавігації приводила до розкриття задумів і намірів командування.

Ведення радіо- і радіотехнічної розвідки (РРТР) дало можливість випереджати супротивника у прийнятті рішень. Але при цьому радіоелектронні засоби демаскували війська і їх пункти управління. По суті, боротьба у інформаційному середовищі у Другій світовій війні вже велася, але сама інформація, видобута РРТР, ще не носила характер стратегічного ресурсу. "Війна в ефірі", як її тоді

називали, ще не була всеосяжною і часто носила лише епізодичний характер.

У подальшому "війна в ефірі" набула більш масовий характер і проводилась протягом всього часу ведення бойових дій. Особливо це проявилось у ході війни у Перський затоці у 1991 році [1], після якої з'явилося нове поняття у військовій справі - інформаційне середовище.

Метою статті є розгляд основних особливостей ведення бойових дій у інформаційному середовищі.

Виклад основного матеріалу дослідження

У чому ж суть особливостей ведення бойових дій у інформаційному середовищі?

Щоб зрозуміти суть, характер, роль і значення ведення бойових дій у інформаційному середовищі, необхідно оцінити ступінь загрози, пов'язаної з їх появою, треба розглянути більш детально особливості, що відрізняють їх від інших бойових дій.

До таких особливостей інформаційного середовища та ведення у ньому бойових дій можна віднести, зокрема, відсутність чітких меж під час ведення бою (операції) (по території, часу, простору) [5, 7].

Інформаційне середовище ведення бойових дій (ІСБД) може одночасно охоплювати не лише локальні, а й глобальні райони ведення бойових дій (своїх і противника) і життєво важливі території та об'єкти державного значення протиборчих сторін про що свідчить досвід проведення анти терористичної операції на сході України.

Для ІСБД не існує державних кордонів і закритих територій. ІСБД може мати локальний, глобальний характер, або той чи інший одночасно, що підтверджується веденням, так званої, гібридної війни проти України з боку Російської Федерації. ІСБД властиві висока анонімність і

скритність дій, труднощі виявлення автора і використуваних ним коштів.

Бойові дії у інформаційному середовищі можуть:

впливати (іноді вирішально) на ефективність та успішність ведення бойових дій в інших середовищах;

передувати бойовим діям у інших середовищах, вестися одночасно з бойовими діями у інших середовищах або після їх завершення, а також бути спонуканням до початку, продовження, припинення бойових дій або відмови противника від своїх намірів;

забезпечити досягнення і утримання інформаційної переваги над противником, підвищити їх ефективність, скорочувати втрати і забезпечувати успішність завершення бою (операції);

створювати сприятливі умови для досягнення як військових, так і політичних цілей своєю стороною, надаючи когнітивний вплив на особовий склад збройних сил та осіб, що беруть участь у підготовці та прийнятті рішень.

Бойові дії в інформаційному середовищі скорочують часовий цикл підготовки і прийняття рішень на ведення бойових дій і забезпечують можливість упередження противника у прийнятті рішень; підвищують оперативність виконання окремих бойових завдань та операції у цілому [3, 4]. Бойові дії в інформаційному середовищі не мають аналогій з історичним оперативно-стратегічним та оперативно-тактичним досвідом ведення бойових дій на землі, у повітрі і на морі.

За поглядами військових фахівців США і НАТО [8], бойові дії в інформаційному середовищі, що позбавляють можливості використання 50 і більше відсотків інформаційних

систем і комп'ютерних мереж під час ведення бою (операції), є умовою, що спонукає до початку або продовження ведення бойових дій.

Висновки й перспективи подальших досліджень

Таким чином, можна сказати, що особливості самого інформаційного середовища, бойових дій у ньому та їх вплив на всі інші середовища протиставлення сторін набувають все більшого впливу і масштабу, які надають глобального впливу не тільки на ефективність бою (операції) збройних сил, а й на військово-політичне керівництво сторін, стан економіки і політику, оскільки у проведенні інформаційних операцій можуть брати участь не тільки війська (сили) збройних сил, але і війська (сили) інших силових структур і цивільні засоби масової інформації протиставлених сторін.

Протиставлення в інформаційній сфері стало носити багатопрофільний характер суспільно-економічних, військово-політичних і державних відносин. Її метою стало не лише підвищення ефективності бойових дій шляхом завоювання інформаційної переваги, але і завоювання всебічної загальної переваги над потенційним противником, щоб забезпечити свої економічні, політичні, а якщо необхідно, то і військові цілі [9, 10]. Тому створення у Збройних Силах України спеціального органу військового управління, який буде здійснювати координацію дій підпорядкованих йому кібернетичних підрозділів, надасть можливість вдосконалити стратегію ведення бойових дій у інформаційному середовищі, що підвищить бойову ефективність Збройних Сил України.

Література

1. **Боевые действия** в Персидском заливе. Аналитический обзор. – М.: ИНФО-ТАСС, АСОНТИ, 1991. 2. **Нейл Грант**. Конфликты XX века. – М.: “Физкультура и спорт”. 1995. 3. **Дасс Р.** Зерно на мельнице. – Киев: “София”, 1993 г. 4. **Делаграмматик М.** Последний солдат суперимперии, или кому нужна “кибервойна” // “Литературная Россия” от 26.04.96, №17 (1733). 5. **Завадский И. И.** “Информационная война – что это такое?” // Защита информации. “Конфидент”. №4, 1996 г. 6. **Ларина Е., Овчинский В.** Кибервойны XXI века. О чем умолчал Эдвард Сноуден. Книжный мир, 2014 г.

7. **Расторгуев С. П.** Информационная война как целенаправленное информационное воздействие информационных систем. // “Информационное общество”. №1. 1997. 8. **Строев В.** Системы с искусственным интеллектом в сухопутных войсках // “Зарубежное военное обозрение”. №3, 1997 г. С.: 27–30. 9. **Г. Смолян, В. Цыгичко, Д. Черешкин.** Новости информационной войны // Защита информации. “Конфидент”. №6. 1996 г. 10. **Черешкин Д. С., Смолян Г. Л., Цыгичко В. Н.** Реалии информационной войны. // Защита информации. “Конфидент”. №4. 1996.

ОСОБЕННОСТИ ВЕДЕНИЯ БОЕВЫХ ДЕЙСТВИЙ В ИНФОРМАЦИОННОЙ СРЕДЕ

Виктор Евгеньевич Бобылёв (канд. воен. наук, с.н.с.)

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье на основе анализа тенденций развития вооруженной борьбы определены особенности ведения боевых действий в информационной среде. Современное информационное пространство может влиять на процесс управления войсками в ходе ведения боевых действий и ведения боевых действий в целом. Проведенный анализ позволил определить влияние информационной среды на ведение боевых действий и определить пути повышения эффективности ведения боевых действий в современной информационной среде. Определены подходы, позволяющие офицерам органов военного управления

пересмотреть свои взгляды на процесс принятия решений при управлении войсками в ходе ведения боевых действий в информационной среде.

Ключевые слова: информационная среда ведения боевых действий; управления войсками; боевые действия; принятие решений.

FEATURES OF WARFARE IN THE INFORMATION ENVIRONMENT

Viktor Y. Bobylov (Candidate of Military Sciences, Senior Research Fellow)

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

The article is based on analysis of trends of the armed struggle by the features of warfare in the information environment of modern information environment has a significant impact on the control of troops in the course of combat and warfare in general. The analysis allowed to establish the impact of the information environment to conduct military operations and identify ways to improve the efficiency of warfare in the modern information environment. The approaches allow officers of the military authorities to reconsider their views on the decision-making process in the control of troops during warfare in the information environment.

Keywords: information environment of warfare; command and control; combat; making decisions.

References

- 1. The fighting in the Persian Gulf. Analytical overview** (1991), Modeling. [*Boevye dejstvija v Persidskom zalive. Analiticheskij obzor*], Moscow, INFO-TASS, ASONTI.
- 2. Neil Grant** (1995), The conflicts of the XX century. [*Konflikty XX veka*], Moscow, Fizkul'tura i sport.
- 3. Dass R.** (1993), Grain to the mill. [*Zerno na mel'nicu*], Kyiv, Sofija.
- 4. Delagrammatik M.** (1996), Last super soldier of the empire, or who need a "cyberwar". [*Poslednij soldat superimperii, ili komu nuzhna "kibervojna"*], Literaturnaja Rossija from 26.04.96, №17 (1733).
- 5. Zavadskij I.I.** (1996), Information War - what is it? [*Informacionnaja vojna – chto jeto takoe?*], Zashhita informacii, "Konfident", No.4.
- 6. Larina E., Ovchinskij V.** (2014), Cyber war of the XXI century. What silent Edward Snowden. [*Kibervojny XXI veka. O chem umolchal Jedvard Snouden*], Knizhnyj mir.
- 7. Rastorguev S.P.** (1997), Information warfare as purposeful information influence of information systems. [*Informacionnaja vojna kak celenapravlennoe informacionnoe vozdejstvie informacionnyh sistem*], Informacionnoe obshhestvo, No.1.
- 8. Stroev V.** (1997), Systems of artificial intelligence in the Army. [*Sistemy s iskusstvennym intellektom v suhoputnyh vojskah*], Zarubezhnoe voennoe obozrenie, No.3, pp. 27-30.
- 9. Smoljan G., Cygichko V., Chereskin D.** (1996), News information war. [*Novosti informacionnoj vojny*], Zashhita informacii. "Konfident", No.6.
- 10. Chereskin D.S., Smoljan G.L., Cygichko V.N.** (1996), The realities of the information war. [*Realii informacionnoj vojny*], Zashhita informacii. "Konfident", No.4.

Отримано: 19.07.2016 року

АНАЛІЗ МЕХАНІЗМІВ ЗАПОБІГАННЯ ВІЙН І ВОЄННИХ КОНФЛІКТІВ

В статті автором викладено погляд на суть способів і механізмів запобігання війнам і воєнним конфліктам в сучасних умовах розвитку військово-політичної обстановки. Визначено поняття механізму запобігання війнам та воєнним конфліктам. Проведено аналіз воєнних доктрин країн які мають ядерний статус, також розглянуті підходи до запобігання війнам і воєнним конфліктам в країнах які не мають ядерної зброї і не входять до системи колективної безпеки, виділено їх загальноприйнятні дії і взаємозв'язок цих дій з воєнною доктриною України. Визначені основні завдання діяльності в інформаційному просторі для запобігання війнам і воєнним конфліктам. Загострення відносин між Україною та Російською Федерацією є прикладом недооцінки питань запобігання воєнним конфліктам, та демонструє можливість інформаційного впливу на різні прошарки населення і їх наслідки, які спровокували викривлене бачення загрози воєнній безпеці.

Ключові слова: воєнна доктрина; інформаційні заходи; запобігання війнам і воєнним конфліктам.

Вступ

Проблему запобігання війнам і воєнним конфліктам можна без перебільшення назвати однією з глобальних проблем людства. Історично стан війни був частішим явищем на планеті, ніж мирний стан. З 3600 р. до н.е. на Землі сталося близько 15 тис. воєнних конфліктів, в яких загинуло приблизно 3,5 млрд. чоловік [1].

З крахом СРСР і Організації Варшавського Договору число воєнних конфліктів в різних регіонах світу значно зросло. Однополярна модель світового військово-політичного устрою виявилася менш стабільною і збалансованою. В її рамках, транснаціональні корпорації заради економічної вигоди чинять політичний тиск на уряди країн, провокуючи їх на застосування військової сили для досягнення цілей свого бізнесу. Розширення кількості країн, що мають ядерну зброю, не сприяє зміцненню світової стабільності. Численні осередки напруженості на Кавказі, Близькому Сході, в Азії і Африці несуть в собі зачатки майбутніх потенційних великомасштабних зіткнень. Анексія Криму з боку Російської Федерації, триваючий конфлікт на сході України стали яскравим прикладом силового сценарію вирішення міждержавних протиріч та задоволення амбіцій керівництва держави, яка бажає відновити статус-кво на світовій арені.

Розглянуті тенденції свідчать про важливість і актуальність дослідження способів і механізмів запобігання воєнним конфліктам.

Постановка проблеми. Теоретичні аспекти запобігання воєнним конфліктам розглядалися багатьма ученими в різні історичні епохи. На рівні практичних дій проблемою запобігання світова спільнота почала займатися тільки з 1899 року, коли за ініціативою Росії була скликана 1-а мирна конференція в Гаазі. Саме таким малим терміном практики миротворчості можна пояснити

відсутність дієвих результатів в запобіганні війн і воєнних конфліктів [4].

Аналіз останніх досліджень та публікацій.

Проблеми запобігання і стримування воєнних конфліктів викладені в працях Першина А.А., Белькова О.А., Рыжова О.А., Мізеру А.А., Капто А.С., Серебрянникова В.В., Лебедевой М.М., Кутахова Ю.А., Кузнецова В.Н., Тоффлера Э., Ротфельда А.Д. та ін.

Метою статті є викладення погляду автора на суть способів і механізмів запобігання війнам і воєнним конфліктам в сучасних умовах розвитку військово-політичної обстановки.

Виклад основного матеріалу дослідження

Згідно Воєнної доктрини України, воєнним конфліктом називається спосіб вирішення протиріч між державами з використанням військової сили або у разі збройного зіткнення всередині держави [2].

Воєнний конфлікт не виникає спонтанно, але, за рівнем соціальної напруженості та заходах, які вживаються для вирішення протиріч, є вищою стадією політичного конфлікту. Джерелами війн і воєнних конфліктів можуть виступати протиріччя в різних сферах громадського життя: а) економічній; б) соціально-політичній; в) духовній та ін. [3].

Узагальнюючи існуючі підходи, запобігання війн і воєнних конфліктів можна визначити як діяльність суб'єктів політичних стосунків, спрямовану на нейтралізацію виниклого протиріччя між двома і більше державами чи озброєними структурами, які мають державний статус.

Під механізмом запобігання війнам і воєнним конфліктам розуміється цілеспрямована діяльність одного або декількох суб'єктів запобігання, спрямована на стримування небажаного розвитку

обстановки, створення умов для запобігання конфлікту на ранній стадії його розвитку, яка сприяє встановленню миру в регіоні або окремій державі. Такий механізм може ґрунтуватися на: компромісному узгодженні національних інтересів держав; договірному обмеженні рівнів їх військової потужності; дотриманні норм міжнародного права і порядку їх здійснення. Усе це припускає необхідність об'єднання зусиль держав в процесі запобігання воєнним конфліктам, створенню системи колективної безпеки, а також використанню превентивної дипломатії.

У тому випадку, якщо яка-небудь держава спробує військовими методами порушити на свою користь баланс інтересів, що склався, необхідно шукати можливість протиставити їй свідомо ефективні сили і засоби силового стримування, а також комплекс політичних, економічних і інших невоєнних заходів міжнародної дії, силових актів, що роблять наслідки, не вигідними для неї. У разі зневаги зробленими кроками у подальшому повинні слідувати акції примусу, що зупиняють агресію і служать уроком не лише для конкретного агресора, але і для його можливих послідовників [5].

В основу розробки способів і механізмів запобігання війнам і воєнним конфліктам можна покласти метод SWOT - аналізу.

Так, для кожної із сторін конфлікту можна визначити її сильні (Strengths) і слабкі (Weaknesses) сторони, а також можливості (Opportunities) для реалізації своїх сильних сторін і загрози (Threats) для слабких сторін.

Сторона – ініціатор конфлікту намагається використати можливості зовнішнього середовища для реалізації своїх сильних сторін, створюючи, тим самим, загрози для слабких сторін противника. Очевидно, що перевага сильних сторін (при сприятливих можливостях) однієї сторони над слабкими сторонами противника, обов'язково призводить до перемоги в конфлікті.

Відповідно, для запобігання воєнному конфлікту необхідно продемонструвати ініціаторові конфлікту (переконати його) такі свої сильні сторони (власні можливості, загрози для противника), які змусять його відмовитися від агресії.

Крім того, у разі участі у конфлікті трьох і більше сторін, для запобігання воєнному конфлікту можна акцентувати увагу усіх сторін на загальних загрозах, які виникнуть у разі початку конфлікту.

Цей підхід знайшов своє відображення у воєнних доктринах провідних країн світу. Загальним для них є чотири основні напрями:

міжнародна співпраця і партнерство у військовій сфері;

зміцнення систем колективної безпеки;

підтримка на достатньому рівні потенціалу ядерного стримування;

розвиток власних збройних сил і підтримка їх в необхідному ступені бойової готовності.

Так, у Воєнній доктрині Російської Федерації, основними завданнями по стримуванню і запобігання воєнним конфліктам визначені [6]:

оцінка і прогнозування розвитку військово-політичної обстановки на глобальному і регіональному рівні, а також стани міждержавних відносин у військово-політичній сфері з використанням сучасних технічних засобів і інформаційних технологій;

нейтралізація можливих військових небезпек і військових загроз політичними, дипломатичними і іншими невоєнними засобами;

підтримка стратегічної стабільності і потенціалу ядерного стримування на достатньому рівні;

підтримка Збройних Сил і інших військ в заданому ступені готовності до бойового застосування;

зміцнення системи колективної безпеки у рамках Організації Договору про колективну безпеку (ОДКБ) і нарощування її потенціалу, посилення взаємодії в області міжнародної безпеки у рамках Співдружності Незалежних Держав (СНД), Організації по безпеці і співпраці в Європі (ОБСЄ) і Шанхайській організації співпраці (ШОС), розвиток стосунків в цій сфері з іншими міждержавними організаціями (Європейським союзом і НАТО);

розширення кола держав-партнерів і розвиток співпраці з ними на основі загальних інтересів у сфері зміцнення міжнародної безпеки відповідно до положень Статуту ООН і інших норм міжнародного права;

дотримання міжнародних договорів в області обмеження і скорочення стратегічних наступальних озброєнь;

укладення і реалізація угод в області контролю над звичайними озброєннями, а також здійснення заходів щодо зміцнення взаємної довіри;

створення механізмів регулювання двосторонньої і багатосторонньої співпраці в області протиракетної оборони;

укладення міжнародного договору про запобігання розміщенню в космічному просторі будь-яких видів зброї;

участь в міжнародній миротворчій діяльності, у тому числі під егідою ООН і у рамках взаємодії з міжнародними (регіональними) організаціями;

участь у боротьбі з міжнародним тероризмом.

Аналогом Воєнної доктрини в США можна вважати сукупність трьох документів: Національної військової стратегії США, Національної оборонної стратегії і, затвердженого 5 січня 2012 року Президентом США Бараком Обамою, документу Пентагону під назвою "Підтримка глобального лідерства США: пріоритети для XXI століття". У цих документах вказується, що Сполучені Штати прагнуть до побудови безпечного і стійкого світового порядку без ядерної зброї. Але до тих пір, поки держава зброя знаходиться на озброєнні інших держав, наявність його в американських арсеналах є стримуючим чинником для запобігання ядерному нападу на США, союзників і партнерів. Американські збройні сили планують здійснювати

стратегічне стримування і забезпечувати виконання зобов'язань перед союзниками і партнерами, використовуючи наявні засоби ядерного ураження і можливості елементів системи протиракетної оборони, розташованих на заоканських територіях.

США також мають намір боротися з поширенням зброї масового ураження, оскільки це представляє серйозну загрозу. Діючи спільно з різними міжнародними інститутами, союзами і коаліціями, США планують знищити мережі поширення зброї масового ураження, перешкодити неконтрольованому транспортуванню початкових матеріалів для його виробництва, поліпшити можливості щодо розслідування ядерних інцидентів, а також підвищити безпеку ядерних матеріалів, хімічних речовин і біологічних агентів по всьому світу. США мають намір надавати допомогу союзникам і партнерам в розвитку можливостей самостійного виявлення і знищення зброї масового ураження для захисту населення своїх країн. Командувачі об'єднаними командуваннями повинні здійснювати ретельне планування і знаходитися в готовності знищити джерела поширення зброї масового ураження, надаючи, таким чином, президентові США широкий вибір варіантів застосування військової сили, коли і де це необхідно.

США повинні зберегти можливості по надійному стримуванню потенційних агресорів звичайними засобами. Стимування і виконання своїх зобов'язань вимагають володіння здібностями до швидкого і глобального проектування сили в усіх сферах. У свою чергу, складові елементи військової потужності, які базуються як в передових зонах на постійній основі, так і розгорнуті на принципі ротації, мають бути розосереджені, мобільні, маневрені і готові зробити політичну підтримку партнерам.

Для стримування противника США мають намір застосовувати комплексний підхід, при якому використовуватиметься увесь державний потенціал, включаючи економічні, дипломатичні і військові методи. Перешкодження противникові в отриманні вигоди від його діяльності є таким же ефективним способом боротьби з ним, як і зміна його стратегічних планів через побоювання отримати адекватну відповідь на свою агресію. Найбільш ефективні підходи до стримування агресії поєднують в собі обидва способи і, в той же час, надають потенційному противникові можливість змінити напрям своїх дій.

Принципи стримування агресії, які використовуються США сьогодні, мають бути адаптовані до умов військово-політичної обстановки ХХІ століття. США планують збільшити потенціал стримування агресії в повітрі, космосі і кіберпросторі завдяки розширенню можливостей по діях в складних умовах обстановки, а також за рахунок своєчасного виявлення і відображення атак на системи забезпечення життєдіяльності або допоміжну інфраструктуру.

У Китаї сьогодні діє стратегія “активної оборони”, яка по суті і є воєнною доктриною

Китаю ХХІ століття. Ця стратегія полягає в здійсненні превентивних заходів політичного, дипломатичного, економічного і військового характеру, спрямованих на створення сприятливих зовнішніх умов і мінімізації чинників нестабільності. Одночасно, наслідуючи світову тенденцію у військовій області і спираючись на зростаючу економічну потужність, Китай взяв курс на вдосконалення якісних параметрів оборонного потенціалу на базі досягнень науки і передових технологій.

Згідно нової стратегії країна повинна мати порівняно компактні, добре збалансовані за видами і родами збройних сил, готовими як до оборонних, так і до наступальних дій відповідно до формули: “Китай не збирається ні на кого нападати, але у разі агресії відповість контрударом”.

Ядерна стратегія Китаю, який зобов'язався не застосовувати ядерну зброю першим, відповідає концепції “ядерного стримування”: КНР не прагне досягти ядерного паритету з розвиненими країнами, але його ядерні сили при будь-якому розвитку військово-політичної обстановки мають бути здатні завдати суттєвого збитку противникові, що змусить останнього відмовитися від застосування ядерної зброї. В той же час, не можна не відмітити, що стратегічні ядерні сили Китаю за своїми бойовими можливостями є наступальною зброєю і роль їх в глобальному балансі ядерних сил значна [7].

Особливий інтерес представляють підходи до запобігання військовим конфліктам в тих країнах, які не мають ядерної зброї і не входять в системи колективної безпеки.

Загальними для подібних країн є наступні напрями діяльності:

- поглиблення і розвиток міжнародної співпраці;
- акцентування зовнішньої політики на власному “нейтральному” (позаблоковому) статусі;
- демонстрація негативних наслідків втрати цього статусу для іноземних держав.

Крім того, абсолютна більшість усіх нейтральних країн сьогодні дуже велику увагу приділяють розвитку власних збройних сил.

Ще одним напрямом діяльності щодо запобігання воєнним конфліктам усіх без виключення країн світу є проведення відповідних заходів в інформаційному просторі.

Основними завданнями діяльності в інформаційному просторі для запобігання воєнним конфліктам доцільно визначити:

- забезпечення власної інформаційної безпеки;
- зміцнення позитивного іміджу власної держави на міжнародній арені;
- демонстрація власної обороноздатності, готовності і рішучості до відбиття агресії, здатності завдати агресорові істотного ураження;
- формування позитивного відношення і підтримки міжнародним співтовариством власних дій, засудження дій агресора;
- інформування міжнародного співтовариства про порушення противником (агресором) норм міжнародного гуманітарного права (прав людини).

Висновки й перспективи подальших досліджень

Таким чином, в статті розглянуті сучасні підходи до запобігання війнам і воєнним конфліктам. На особливу увагу заслуговує комплекс заходів інформаційного характеру.

Загострення відносин між Україною та Російською Федерацією є прикладом недооцінки питань запобігання воєнним конфліктам, та

демонструє можливість інформаційного впливу на різні прошарки населення і їх наслідки, які спровокували викривлене бачення загроз воєнній безпеці. У сучасних умовах Україна є об'єктом безперервного інформаційно-психологічного впливу, тому розуміння змісту та спрямованості інформаційних заходів, що будуть проводитись в інтересах запобігання воєнним конфліктам є життєво важливим.

Література

1. Капто А. С. Енциклопедія світу : 2-е видавництво, уточн. і доп. - М.: Книга і бізнес, 2005; 2. Воєнна доктрина України (у редакції Указу Президента України від 24 вересня 2015 року № 555/2015). 3. Рыжов О. А., Коваленко Б. В., Пирогів А. И. Політична конфліктологія, М.: 2001. 4. Кутахов Ю. Л. Монографія. Запобігання: Стан і динаміка політики запобігання виникненню небезпек і загроз людині в міжнародних відносинах ХХІ століття. М.: 2005. 5. Калмыков П. В.

Политические технологии предотвращения военных конфликтов. Автореферат диссертации. Режим доступа: <http://www.disscat.com/content/politicheskie-tehnologii-predotvrashcheniya-voennykh-konfliktov>. 6. Військова доктрина Російської Федерації (у редакції Указу Президента Російської Федерації від 5 лютого 2010 року № 146). 7. Annual Report to Congress "Military Power of the People.

АНАЛИЗ МЕХАНИЗМОВ ПО ПРЕДОТВРАЩЕНИЮ ВОЙН И ВОЕННЫХ КОНФЛИКТОВ

Александр Владимирович Войтко

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье автором изложен взгляд на суть способов и механизмов предотвращения войн и военных конфликтов в современных условиях развития военно-политической обстановки. Определено понятие механизма предотвращения войн и военных конфликтов. Проведен анализ военных доктрин стран, которые имеют ядерный статус, также рассмотрены подходы к предотвращению войн и военных конфликтов в странах, которые не имеют ядерного оружия и не входят в систему коллективной безопасности, выделены их общепринятые действия и взаимосвязь этих действий с военной доктриной Украины. Определены основные задачи деятельности в информационном пространстве для предотвращения войн и военных конфликтов. Обострение отношений между Украиной и Российской Федерацией является примером недооценки вопросов предотвращения военных конфликтов, демонстрирует возможность информационного воздействия на различные слои населения, а также их последствия, которые спровоцировали искаженное восприятие угроз военной безопасности.

Ключевые слова: военная доктрина; информационные мероприятия; предотвращение войн и военных конфликтов.

ANALYSIS OF MECHANISMS TO PREVENT WARS AND MILITARY CONFLICTS

Oleksandr V. Voitko

National Defense University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine

In the article the author stated view of the nature of the methods and mechanisms to prevent wars and military conflicts in modern conditions of military-political situation. The concept of a mechanism for preventing wars and military conflicts. The analysis of military doctrines of the nuclear status, and the approaches to the prevention of wars and military conflicts in countries that do not have nuclear weapons and are not included in the system of collective security, highlighted their common action and the relationship of these actions with military doctrine of Ukraine. The main tasks of the media space in order to prevent wars and military conflicts. Relations between Ukraine and Russia is an example of underestimating the prevention of armed conflict, and demonstrates the possibility of information impact on different segments of the population and their consequences that provoked a distorted view of threats to military security.

Keywords: military doctrine; information activities; preventing wars and military conflicts.

References

1. Капто А.С. (2005), The World Encyclopedia: [Entsyklopediia svitu], Moscow: Knyha i biznes.. 2. Military Doctrine of Ukraine (as amended by the Decree of the President of Ukraine from September 24, 2015 number 555/2015). 3. Ryzhov O.A., Kovalenko B.V., Pirogov A.I. (2001), Political Conflict. [Politychna konfliktologhiia], Moscow. 4. Kutakhov Yu.L., (2005), Monograph. Prevention: Status and dynamic policy preventing dangers and threats to people in the twenty-first century international relations. [Monohrafiia. Zapobihannia: Stan i dynamika

polityky zapobihannia vynyknenniu nebezpek i zahroz liudyni v mizhnarodnykh vidnosynakh XXI stolittia], Moscow. 5. Kalmykov P.V. Political technologies to prevent military conflicts. [Politicheskie tekhnologii predotvrashcheniia voennykh konfliktov], Abstract of the thesis. Access mode: <http://www.disscat.com/content/politicheskie-tehnologii-predotvrashcheniya-voennykh-konfliktov>. 6. Military Doctrine of the Russian Federation (as amended by Presidential Decree on February 5, 2010 № 146). 7. Annual Report to Congress "Military Power of the People.

Отримано: 03.08.2016 року

Анатолій Анатолійович Головка (канд. військ. наук)

Національний інститут стратегічних досліджень при Президентіві України, Київ, Україна

НЕДЕРЖАВНІ СУБ'ЄКТИ ПРОТИДІЇ ЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ В ІНФОРМАЦІЙНІЙ СФЕРІ

Практичне втілення завдань захисту інформаційного простору вимагає від усіх суб'єктів (як державних так і недержавних) активної співпраці та спільної координації зусиль, ресурсів і можливостей у протидії сучасним загрозам і викликам. За посередництва недержавних інститутів суспільство має в розпорядженні своєрідні важелі впливу на державну політику в сфері забезпечення інформаційної безпеки. В умовах гібридної війни такі зв'язки є особливо необхідними, оскільки дозволяють суспільним і державним інститутам виступити одним фронтом проти зовнішнього ворога. Як і в зарубіжних країнах так і в Україні важливу роль в реалізації цілей національної безпеки в інформаційній сфері грають громадські об'єднання, неурядові організації, професійні спілки і т.д. В статті представлено цілісне бачення ключових структурних елементів недержавної системи забезпечення інформаційної безпеки. Основний акцент зроблений на дослідженні недержавних суб'єктів інформаційної безпеки. У фокусі наукового аналізу знаходяться такі інститути як громадські об'єднання, неурядові аналітичні центри та засоби масової інформації, що виступають у ролі стратегічних партнерів уряду в секторі безпеки. За основу було взято досвід України в умовах гібридної війни та зовнішнього інформаційного тиску. Крім того, в статті систематизовано базові канали взаємодії між громадським сектором та державою у процесі забезпечення інформаційної безпеки. В результаті дослідження були сформульовані висерпні висновки.

***Ключові слова:** національна безпека; інформація; загрози; суб'єкти; громадські об'єднання; аналітичні центри; ЗМІ.*

Вступ

Постановка проблеми. Модерні інформаційні виклики, що постали перед сучасними національними державами в епоху глобалізації безпосередньо детермінують всю систему суспільно-політичних відносин. Висока динаміка науково технічного прогресу обумовила високу залежність сучасного суспільства від інформаційних технологій, що в свою чергу зробило його вразливим перед загрозами, які наявні в даній сфері. Саме тому, перед державою стоїть гостра необхідність у виробленні дієвих механізмів протидії таким ризикам.

Для реалізації подібної мети сил держави, зазвичай, не вистачає, що спонукає владу шукати альтернативні джерела ресурсів та інструментів (кадрових, інтелектуальних, організаційних). Стратегічним партнером держави в цих пошуках стає громадянське суспільство, що володіє достатнім потенціалом для підтримки безпекових та виконавчих структур у ході побудови дієвої системи безпеки в інформаційній сфері. Особливо яскраво подібна тенденція проявляється при аналізі сучасних українських реалій, оскільки Україна зараз знаходиться в стані постійного воєнно-інформаційного тиску з боку Росії та проросійських сил.

Аналіз останніх досліджень та публікацій: вивчення безпекового виміру діяльності недержавних інституцій традиційно знаходиться у фокусі наукових пошуків багатьох українських (О. Корнієвський, В. Крутов, Г. Почепцов,

Ю. Якименко, Л. Євдоченко, А. Качинський, К. Павлюк, І. Климпуша та інших) та зарубіжних (Дж. МакГан, С. Томпсон, Дж. Браян, М. Абдурахманов, С. Расторгуев, Ф. Гансен) науковців.

Однак питання комплексного наукового аналізу їх місця та ролі саме в секторі інформаційної безпеки залишається відкритим. Цей фактор і актуалізує наукові пошуки в даному сегменті наукового знання. Особливо важливим є побудова теоретичних основ розуміння місця недержавних суб'єктів у загальній системі інформаційної безпеки держави.

Метою статті є систематизація недержавних суб'єктів інформаційної безпеки та визначення їх місця і ролі у протидії зовнішнім ризикам та загрозам національній безпеці України.

У відповідності з метою дослідження постають наступні наукові завдання:

1. Визначення основних недержавних суб'єктів забезпечення інформаційної безпеки України;
2. Науковий аналіз принципів та шляхів їх залучення до протидії інформаційним загрозам національній безпеці.

Викладення основного матеріалу дослідження

Сьогодні, високий рівень розвитку інституту громадянського суспільства є невід'ємним атрибутом сучасної правової держави. Принципи ліберальної демократії, які взяли за основу всі високорозвинені країни заходу, ґрунтуються на ідеї підтримки постійних взаємозв'язків між владою та

соціумом. В Україні інститут громадянського суспільства поки, що знаходиться на етапі формування. Це пов'язано з комплексом соціально-політичних, культурних та історичних факторів [1, с. 85]. До них слід віднести відсутність достатнього досвіду власної державності, часту зміну політичних режимів за час незалежності (від більш демократичних до більш авторитарних), несформована політична культура громадянського суспільства, високий рівень політичного песимізму та абсентеїзму і т.д. У процесі наукового аналізу чітко простежується нинішня неефективність взаємодії органів державної влади і громадянського суспільства [1, с. 113]. Саме тому, пошук ефективних методів та інструментів вдосконалення співпраці між інститутами громадянського суспільства в соціально значимих питаннях є стратегічним пріоритетом для України [1, с. 85].

Як уже було згадано вище, особливо важливе вдосконалення взаємодії між державою та громадянським суспільством в секторі інформаційної безпеки, де використання недержавних ресурсів є обов'язковою умовою ефективного захисту від широкого спектру зовнішніх ризиків. При використанні правильних методів залучення громадського сектору до політики безпеки можна ефективно протидіяти усім наявним викликам як в інформаційній так і в інших сферах.

В даному контексті важливо чітко визначити інститути громадянського суспільства, які власне і виступають суб'єктами забезпечення інформаційної безпеки України. Доцільно виділити наступні групи:

- До *першої групи* слід віднести громадські об'єднання, тобто різного роду організації, спілки, асоціації і т. д. Прикладом тут можуть слугувати ГО "Академія національної безпеки", Всеукраїнська асоціація "Інформаційна безпека та інформаційні технології", Центр військово-політичних досліджень (більш відома завдяки своєму проекту "Інформаційний опір");

- *Другу групу* складають неурядові аналітичні центри, як позадержавні експертні та наукові установи. До них варто віднести Український центр економічних і політичних досліджень ім. Олександра Разумкова (або просто Центр Разумкова), Український інститут публічної політики, Центр політико-правових реформ;

- *Третя група* об'єднує усі недержавні засоби масової інформації, що діють на території України, а саме друковані джерела (журнали, газети), телевізійні канали, радіостанції, інтернет-ресурси. Тут можна згадати газету "Інформаційний бюлетень", інтернет-видання "Українська правда", телевізійні канали "112.ua", "Перший український інформаційний — 5 канал", "телевізійний канал 24" і т. д. [1, с. 104].

Всі вищеперераховані інститути мають у розпорядженні достатню кількість інструментів для аналітичного / експертного / організаційного

супроводу політики уряду. Це дозволяє їм брати участь в захисті інформаційного простору країни та формування сталих зв'язків із державними безпековими та виконавчими структурами. Проте, слід відмітити, що тут все залежить від рівня розвитку політичної культури, як суспільства так і органів влади.

Недержавні суб'єкти виконують різні завдання щодо забезпечення національної безпеки в інформаційній сфері:

- 1) допомога державі забезпечувати національну безпеку, виконання окремих функцій державних органів;

- 2) доповнення державної системи національної безпеки, виконання тих функцій щодо захисту життєво важливих інтересів особистості й суспільства, які держава не виконує свідомо, або не може виконувати через обмеженість ресурсів, або з інших причин;

- 3) створення сприятливих умов для діяльності органів влади та управління щодо забезпечення безпеки;

- 4) контроль за діяльністю держави у виконанні функцій забезпечення національної безпеки інформаційній сфері;

- 5) оцінка ефективності діяльності держави щодо забезпечення національної безпеки;

- 6) спонукання держави до вживання заходів щодо захисту інтересів особистості й суспільства, виправлення допущених помилок;

- 7) захист особистості та суспільства від сваволі держави та її чиновників;

- 8) підготовка кадрів, здатних посідати державні посади у сфері забезпечення національної безпеки;

- 9) здійснення наукових досліджень з актуальних проблем в інформаційній безпеці;

- 10) інформаційно-аналітична робота [4].

Усі вищеназвані функції недержавних інститутів підтверджують об'єктивну необхідність постійного контакту держави та громадянського суспільства. В ході реалізації національних інтересів України в інформаційній сфері механізм взаємодії державних органів безпеки та правопорядку із суб'єктами недержавної підсистеми повинен визначитись, насамперед, мірою їх участі у вирішенні актуальних проблем українського державотворення. Це, у свою чергу, передбачає, що метод державного регулювання діяльності недержавних суб'єктів системи інформаційної безпеки має базуватися не на забороні, а на створенні умов для активного використання її з метою забезпечення безпеки держави, суспільства, особистості [4].

Тому слід проаналізувати механізм такої взаємодії. Сьогодні доцільно виділяти наступні шляхи співпраці між громадянським суспільством та державою:

- Створення та подальша робота громадських рад при державних структурах, а саме міністерствах, окремих відомствах, силових та безпекових структурах (зазвичай цей метод характерний для співпраці між державою та громадськими об'єднаннями).

- Укладення угод між державою з однієї сторони та інститутами громадянського суспільства з іншої.

- Реалізація спільних управлінських, дослідницьких, інформаційно-аналітичних та інших соціально значимих проєктів.

- Проведення спільних наукових та просвітницьких заходів, а саме конференцій, семінарів, круглих столів присвячених питанням інформаційної безпеки із залученням представників державних органів і громадськості;

Громадські слухання, консультації та реалізація громадських ініціатив [1, с. 104].

Висновки й перспективи подальших досліджень

Отже, в сучасних умовах громадянське суспільство є невід'ємною частиною загальної системи протидії інформаційним загрозам та ризикам. Це обумовлено тим, що ресурсів та можливостей уряду, як правило, замало для ефективної реалізації національних інтересів в даній сфері, що і спонукає до пошуку альтернативних джерел. До основних недержавних

інститутів, які виступають у ролі суб'єктів забезпечення інформаційної безпеки варто відносити громадські об'єднання, недержавні аналітичні центри, засоби масової інформації. Постійна динамічна модернізація механізму взаємодії громадянського суспільства та державних структур у процесі забезпечення реалізації цілей національної безпеки (зокрема в інформаційній сфері) є стратегічним пріоритетом для сучасних держав, у тому числі і для України.

Враховуючи важливість даної проблематики перед нами постає необхідність подальших наукових розвідок в даному напрямку. Зокрема, перспективними цілями тут є вдосконалення понятійно-категоріального апарату, який необхідний для комплексного дослідження із питань інформаційної безпеки; визначення основних проблем у сегменті взаємодії громадянського суспільства та держави; вдосконалення механізму залучення недержавних інститутів до політики безпеки в інформаційній сфері.

Література

1. Головка А. А. Громадянське суспільство як суб'єкт забезпечення інформаційної безпеки України / Анатолій Анатолійович Головка // "Україна в процесах глобального інформаційного обміну" (м. Львів, 26-27 травня 2016р.). – Львів: Національний університет "Львівська політехніка", 2016. – С. 103-105.
2. Головка А. А. Сучасні реалії взаємодії між державою та громадянським суспільством в Україні / Анатолій Анатолійович Головка // "Актуальные научные исследования в современном мире" (м. Переяслав-Хмельницький 26-27 червня 2016). – Переяслав-Хмельницький: "iScience", 2016. – С. 84-87.
3. Мартиненко В. Взаємодія органів державної влади і

громадянського суспільства у законодавчо-нормативному вимірі / Володимир Мартиненко // Збірник матеріалів міжнародної науково-практичної конференції "Розвиток взаємодії держави і громадянського суспільства в контексті впровадження європейських принципів належного врядування" (12 грудня 2012 р., м. Київ) К. : НІСД, 2013. – С. 112-118.

4. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки [Електронний ресурс] / Ганна Сащук // Сайт Інституту журналістики – КНУ ім. Тараса Шевченка. – Режим доступу: http://www.journ.univ.kiev.ua/trk/publikacii/satshuk_publ.p hp.

НЕГОСУДАРСТВЕННЫЕ СУБЪЕКТЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Анатолій Анатольевич Головка

Национальный институт стратегических исследований при Президенте Украины, Киев, Украина

Практическое воплощение задач защиты информационного пространства требует от всех субъектов (как государственных так и негосударственных) активного сотрудничества и совместной координации усилий, ресурсов и возможностей в противодействии современным угрозам и вызовам. При посредничестве негосударственных институтов общество располагает своеобразными рычагами влияния на государственную политику в сфере обеспечения информационной безопасности. В условиях гибридной войны такие связи особенно необходимы, поскольку они позволяют общественным и государственным институтам выступить одним фронтом против внешнего врага. Как и в зарубежных странах так и в Украине важную роль в реализации целей национальной безопасности в информационной сфере играют общественные объединения, неправительственные организации, профессиональные союзы и т.д. В статье представлено целостное видение ключевых структурных элементов негосударственной системы обеспечения информационной безопасности. Основной акцент сделан на исследовании негосударственных субъектов информационной безопасности. В фокусе научного анализа находятся такие институты как общественные объединения, неправительственные аналитические центры и средства массовой информации, выступающие в роли стратегических партнеров правительства в секторе безопасности. За основу был взят опыт Украины в условиях гибридной войны и внешнего информационного давления. Кроме того, в статье систематизированы базовые каналы взаимодействия между общественным сектором и государством в процессе

обеспечения информационной безопасности. В результате исследования были сформулированы исчерпывающие выводы.

Ключевые слова: национальная безопасность; информация; угрозы; субъекты; общественные объединения; аналитические центры; СМИ.

NON-GOVERNMENTAL ACTORS COUNTERING THREATS OF NATIONAL SECURITY THREATS IN THE INFORMATION SPHERE

Anatolii A. Holovka

The National Institute for Strategic Studies, Kyiv, Ukraine

Practical realizing of tasks concerning the protection of informative space requires from all subjects (both state and non-state) an active cooperation and general co-ordination of efforts, resources and possibilities in counteraction to the modern threats and challenges. Through the mediation of the nongovernmental institutes, peculiar control sticks in providing of informative safety are available in the society. In the conditions of hybrid war, such relations are especially necessary, as they allow the public and state institutes to perform as a united front against an external enemy. Both in foreign countries and in Ukraine public associations, non-governmental organizations and trade unions play an important role in the realization of aims of the national security in the sphere of information etc. The article presents a holistic vision of key structural elements of non-state systems of information security. The main focus is on the research of non-state actors information security. Scientific analysis dedicated are institutions such as public associations, think tanks and the mass media, which act as strategic partners in the government security sector. Was based on the experience of Ukraine in conditions of hybrid warfare and external information pressure. In addition, the article presents the basic channels of cooperation between the public sector and in the state of information security. The study result were formulated comprehensive conclusions.

Keywords: national security; information; threat agents; public associations; think tanks; the mass media.

References

- Holovka A.A.** (2016) Civil society as subject an information security Ukraine. [*Gromadanske suspilstwo jak subject zabezpechnnja informazijnoi bezpeky Ukrainy*], Nationalnyi universytet "Lvivska politechnika", pp. 103-105.
- Holovka A.A.** (2016) Modern realities of interaction between the state and civil society in Ukraine. [*Suchasni realii vsajemodii miz derzhawoju ta gromadanskym suspilstwom v Ukraini*], "iScience", pp. 84-87.
- Martynenko V.** (2013) Interaction of public authorities and civil society in the legislative and normative dimension. [*Vsajemodija organiv derzhawnoi wladny i gromadanskogo suspilstwa u zakonodavcho-normatywnomu vymiri*], NISD, pp. 112-118.
- Saschuk H.** Information security in the national security system. [*Informazijna bezpeka v systemi zabezpechnnja nationalnoi bezpeky*], KNU im. Tarasa Shevchenka.

Отримано: 25.06.2016 року.

Иван Петрович Даценко (канд. техн. наук)

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

МЕТОДИЧЕСКИЕ ОСНОВЫ ТЕХНИКО-ЭКОНОМИЧЕСКОЙ ОЦЕНКИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ СВАРКИ ПРИ ПРОИЗВОДСТВЕ И МОДЕРНИЗАЦИИ СПЕЦИАЛЬНЫХ АВТОМОБИЛЕЙ

При производстве и модернизации специальных автомобилей важное место занимают электросварочные работы на броневых конструкциях. В настоящее время электросварочные работы являются, единственным высокопроизводительным способом надежного соединения деталей. Но при этом им присущи серьезные недостатки, обусловленные принципиальными особенностями электродуговой сварки, а именно, существенным отличием физико-механических свойств сварного соединения от свойств свариваемых деталей, в результате чего, качество сварного соединения (которое состоит из сварного шва и зоны термического влияния) существенно ниже, чем качество металла корпуса машины.

На основании анализа опыта применения бронированных специализированных машин и требований к защищенности данной группы техники предложен методический подход выбора оптимального режима сварки конструкций колесных бронированных машин. Предложенная методика может быть базовой для создания специализированного программного обеспечения в области поиска рациональных подходов в процессе модернизации и проектирование современных бронированных специализированных автомобилей.

Ключевые слова: *бронированные специализированные автомобили; броневая защита; критерий; показатель; технико-экономическая оценка; физико-механические свойства; стоимость; окружающая среда; свойства; технические характеристики; качество.*

Введение

Постановка проблемы. Опыт проведения антитеррористической операции показал, что некоторые подразделения Вооруженных Сил Украины и других военных формирований применялись для выполнения задач в большинстве случаев на небронированной технике. Это приводит к неоправданным потерям личного состава и в ряде случаев, не выполнение поставленных задач. Поэтому возникает необходимость в повышении защиты специализированных автомобилей, что может быть достигнуто за счет использования броневой защиты транспортных машин, или использованием специализированных колесных броневых машин производимых промышленностью Украины.

При производстве и модернизации специальных автомобилей важное место занимают электросварочные работы на броневых конструкциях. Сварка обеспечивает наиболее простое и быстрое изготовление прочного корпуса при наименьшей его стоимости. Следует отметить, что сварка допускает широкое внедрение автоматизации в производство броневых корпусов. Это может обеспечить массовое и наиболее дешевое производство. Поэтому очень актуальна проблема выбора рационального выбора сварки.

Анализ последних исследований и публикаций. Из публикаций [8, 9] видно, что вопросами влияния технологии изготовления

корпусов на защищенность легкобронированных боевых машин уделялось недостаточное внимание. При этом не проводилась в [8] рассмотрены образцы бронированных автомобилей ведущих стран мира. Сравнительная оценка уровня защищенности различных образцов бронетехники достаточно актуальным вопросом. В [6] определены требования к уровню бронезащищенности специальных автомобилей, но методы сравнительной оценки уровня защищенности не учитывают, как влияет на это производственный процесс, и требуют дополнительного исследования. Исходя из этого, возникает необходимость по совершенствованию существующих методических подходов, позволяющих не только оценивать бронированные автомобили по уровню защищенности, с учётом как технология производства корпуса влияет на это, а также оценивать технико-экономическую эффективность производства.

Цель статьи. Учитывая вышеизложенное, следует отметить, что статья посвящена рассмотрению технико-экономических показателей сварочного производства предприятий на которых осуществляется ремонт и модернизация специальных автомобилей. при этом оцениваются как технико-экономические показатели так и показатели качества выполнения работ, кроме этого рассматриваются и эксплуатационные свойства.

Изложение основного материала исследования.

В сфере производства, когда приходится совместно учитывать качественные и количественные факторы различной размерности, нашел применение показатель эффективности $K_{\text{Э}}$, устанавливающий связь результата, например, от применения технологического процесса, с затратами на его осуществление [2-4], наиболее общий вид которого

$$K_{\text{Э}} = \frac{P_{\text{ТП}}}{Z}, \quad (1)$$

где $P_{\text{ТП}}$ – результат (продукт), полученный от применения данного технологического процесса;

Z – затраты на создание результата.

Смысловая основа представленного показателя заключается в принципе максимизации результата на единицу затрат.

В данной работе применительно к сварке корпусов специальных автомобилей предложим более широкую трактовку понятия результата $P_{\text{К}}$ как комплексного, с учетом его проявления, и в сфере производства, и в сфере потребления:

$$P_{\text{К}} = f(\bar{R}), \quad (2)$$

где \bar{R} – совокупность показателей, характеризующих с разных сторон процесс сварки, свойства сварного соединения, как объекта, созданного сваркой, и конечный эффект от функционирования объекта по его основному назначению, в данном случае уязвимость сварного соединения от боевых средств поражения и экономические последствия его поражения.

Таким образом, речь идет о разработке методики оценки способа сварки броневых деталей на основе комплексного показателя производственно-эксплуатационной эффективности, который включает как производственные, так и потребительские (эксплуатационные, боевые) оценки процесса сварки и сварного соединения.

Группа технологических показателей достаточно разносторонне характеризует способ сварки. Для оценки дугового процесса наиболее информативным является коэффициент наплавки $\alpha_{\text{Н}}$:

$$\alpha_{\text{Н}} = \frac{P_{\text{Н}}}{I \cdot t}, \quad (3)$$

где $P_{\text{Н}}$ – масса наплавленного металла шва, г;

I – ток сварки, А;

t – время сварки, час.

Показатель наплавки $\alpha_{\text{Н}}$ одновременно учитывает производительность процесса сварки как количество металла, которым заполняется шов в единицу времени, так и эффективность использования дуги – количество металла сварного шва, приходящееся на единицу тока сварки.

Любая электродуговая сварка сопровождается потерями электродного металла на разбрызгивание и угар, что снижает производительность сварки и увеличивает её себестоимость. Величина этих

потерь существенным образом зависит от способа сварки. Например, при сварке в среде углекислого газа указанные потери достигают 12-15% от расплавленного электродного металла [2]. Для оценки потерь воспользуемся коэффициентом потерь ψ , который определяется из выражения

$$\psi = \frac{G_{\text{Р}} - G_{\text{Н}}}{G_{\text{Р}}}, \quad (4)$$

где $G_{\text{Р}}$ и $G_{\text{Н}}$ – соответственно массы расплавленного электродного металла и наплавленного металла.

Влияние способа сварки на экологию окружающей среды предлагается оценивать показателем загрязнения $K_{\text{З}}$, который определяется как сумма произведений отношения количества выделяемого загрязнения i -того вида к его предельно допустимой концентрации на обратную величину степени вредности этого загрязнения:

$$K_{\text{З}} = \sum_i \left(\frac{P_i}{P_{i\text{ДОП}}} \cdot \frac{1}{W_i} \right), \quad (5)$$

где P_i – количество выделяемого загрязнения i -того вида;

$P_{i\text{ДОП}}$ – допустимое количество загрязнения i -того вида;

W_i – степень вредности загрязнения i -того вида.

Коэффициент W_i принимает значение от 1 до 4 в зависимости от того, к какой группе отнесен i -тый вид загрязнения: “1” – чрезмерно вредные, “2” – высоко вредные, “3” – умеренно вредные, “4” – мало вредные. Допустимое количество загрязнения, а также отнесение его к определенной группе вредности, определяется согласно ГОСТ 12.1.005 – 88 [1].

Учитывая вышесказанное, предлагается следующий комплексный технологический показатель $K_{\text{Т}}$:

$$K_{\text{Т}} = \frac{\alpha_{\text{Н}}}{(1 + K_{\text{З}})(1 + \psi)}, \quad (6)$$

а после подстановки выражений (3,4,5) получим:

$$K_{\text{Т}} = \frac{P_{\text{Н}}}{I \cdot t \left[1 + \sum \left(\frac{P_i}{P_{i\text{ДОП}}} \cdot \frac{1}{W_i} \right) \right] (1 + \psi)}, \quad (7)$$

Группа технических показателей применена для оценки качества отдельных зон сварного соединения и всего соединения в целом. При этом учитывались только те показатели качества, которые отражают способность сварного соединения (и его зон) противостоять внешнему поражающему воздействию. Основными факторами, определяющими противопульную стойкость сварного соединения, являются физико-химические свойства его металла и наличие в нем дефектов [8]. Результат сварки будет наилучшим, если дефекты будут отсутствовать, а физико-

механические свойства зон сварного соединения и основного металла будут одинаковы.

Для оценки наличия дефектов в зонах металла сварного соединения применимы показатели бездефектности сварного шва $K_{БД}^{Ш}$ и бездефектности зоны термического влияния $K_{БД}^{ЗТВ}$, которым присваиваются балльные оценки:

в случае отсутствия дефектов $K_{БД}^{Ш} = 1$ и $K_{БД}^{ЗТВ} = 1$; если есть дефекты, которые могут быть устранены, $K_{БД}^{Ш} = 0,5$ и $K_{БД}^{ЗТВ} = 0,5$; при наличии дефектов, которые не могут быть устранены, $K_{БД}^{Ш} = 0$ и $K_{БД}^{ЗТВ} = 0$.

В качестве интегральной оценки физико-химических свойств металла, как указывалось выше, принята твердость металла. Степень одинаковости твердости металла сварного шва и твердости основного металла, а также твердости металла зоны термического влияния и твердости основного металла предлагается оценить соотношениями

$$K_{ОД}^{Ш} = \frac{H_{Ш}}{H_{ОМ}}, \quad (8)$$

$$K_{ОД}^{ЗТВ} = \frac{H_{ЗТВ}}{H_{ОМ}}, \quad (9)$$

где $K_{ОД}^{Ш}$ и $K_{ОД}^{ЗТВ}$ – показатели степени одинаковости сварного шва и зоны термического влияния соответственно;

$H_{Ш}$ – твердость металла сварного шва, единица твердости;

$H_{ЗТВ}$ – твердость металла зоны термического влияния, единица твердости;

$H_{ОМ}$ – твердость основного металла, единица твердости.

С учетом вышесказанного, показатели качества металла сварного шва $K_{К}^{Ш}$ и зоны термического влияния $K_{К}^{ЗТВ}$ могут быть определены по формулам:

$$K_{К}^{Ш} = K_{БД}^{Ш} \cdot K_{ОД}^{Ш}, \quad (10)$$

$$K_{К}^{ЗТВ} = K_{БД}^{ЗТВ} \cdot K_{ОД}^{ЗТВ}. \quad (11)$$

Тогда показатель качества сварного соединения $K_{К}$ определим как

$$K_{К} = K_{К}^{Ш} \cdot K_{К}^{ЗТВ}, \quad (12)$$

С учетом формул 8–12 получим следующее выражение для качества сварного соединения $K_{К}$:

$$K_{К} = \left(\frac{H_{Ш}}{H_{ОМ}} \cdot K_{БД}^{Ш} \right) \left(\frac{H_{ЗТВ}}{H_{ОМ}} \cdot K_{БД}^{ЗТВ} \right). \quad (13)$$

Следует отметить, что показатель качества сварного соединения и его составляющие отражают также и совершенство технологии сварки, т.е. этот показатель может быть отнесен к категории технических и технологических показателей.

Затраты, необходимые для получения сварочного соединения в производстве, оцениваются группой экономических показателей, отражающих единовременные затраты, необходимые для внедрения способа сварки, в виде капитальных вложений K и текущие расходы на изготовление сварного соединения в виде себестоимости сварочных работ $C_{СР}$.

Себестоимость выполнения сварочных работ $C_{СР}$ по соединению деталей корпуса при производственной оценке приведенных затрат $Z_{П}$ включает себестоимость подготовительных работ, себестоимость электросварочных работ и себестоимость последующей обработки сварных поверхностей:

$$C_{ЗР} = C_{ПР} + C_{СВ} + C_{ЗО}, \quad (14)$$

где $C_{СР}$ – себестоимость сварочных работ, грн;

$C_{ПР}$ – себестоимость подготовительных работ, грн;

$C_{ЗТВ}$ – себестоимость сварки, грн;

$C_{ЗО}$ – себестоимость заключительной обработки, грн.

При сравнении различных технологических процессов принято сравнивать только те виды затрат, входящих в себестоимость, величина которых меняется при переходе от одного технологического процесса к другому. Эти затраты составляют технологическую себестоимость $C_{Т}$ [4-7]. Для большинства исследованных способов электродуговой сварки, подготовительные работы и заключительная обработка практически одинаковы, поэтому затраты на их выполнение не подлежат включению в технологическую себестоимость. Следовательно:

$$C_{Т} = C_{СР} = C_{СВ}. \quad (15)$$

При оценке себестоимости сварки (а значит и технологической себестоимости), как правило, учитываются следующие затраты:

$$C_{Т} = C_{ЗВ} = Z_{ЗП} + Z_{М} + Z_{Э} + Z_{А}, \quad (16)$$

где $Z_{ЗП}$ – затраты на заработную плату сварщика, грн;

$Z_{М}$ – затраты на сварочные материалы, грн;

$Z_{Э}$ – затраты на электроэнергию, грн;

$Z_{А}$ – затраты на амортизационные отчисления, связанные с эксплуатацией сварочного оборудования, грн.

Расчет указанных в формуле (16) затрат, выполняется известным образом [7].

С учетом вышесказанного получим:

$$Z_{П} = C_{Т} + E_{Н} \cdot K = Z_{ЗП} + Z_{М} + Z_{Э} + Z_{А} + E_{Н} \cdot K. \quad (17)$$

Приведенные выше технологические, технические и экономические показатели относятся к группе производственных показателей. Для оценки способа сварки с точки зрения потребительских свойств сварного соединения при эксплуатации введем ограничение: оценку будем давать только применительно к боевой эксплуатации ЛБМ, когда возможно воздействие на сварное соединение средств поражения. Указанное ограничение обусловлено тем, что все

современные способы сварки обеспечивают необходимый ресурс работы сварного соединения в условиях нормальной эксплуатации без воздействия средств поражения. Как показывает опыт, повреждение сварного шва при нормальных условиях эксплуатации при отсутствии боевых повреждающих факторов маловероятно [8]. Следовательно, в дальнейшем будем вести речь об уязвимости сварного соединения в зависимости от способа сварки в условиях воздействия на машину средств боевого поражения.

В настоящих исследованиях рассматривалась уязвимость сварного соединения, обусловленная способом сварки, с учетом двух факторов: возможность попадания поражающего средства в сварное соединение и стойкость сварного соединения к воздействию поражающего средства.

Возможность попадания поражающего средства в сварное соединение при всех прочих равных условиях зависит от площади сварного соединения: чем больше площадь, тем больше возможность попадания. Площадь сварного соединения (точнее его ширина) существенно зависит от способа сварки, для оценки которого в данном случае введем показатель попадания:

$$K_{\Pi} = \frac{S_{CC}}{S_{БК}}, \quad (18)$$

где S_{CC} – площадь сварного соединения, мм²;
 $S_{БК}$ – площадь броневой конструкции, мм².

При этом учтем, что площадь сварного соединения S_{CC} складывается из площади сварного шва $S_{Ш}$ и площади зоны термического влияния $S_{ЗТВ}$:

$$S_{CC} = S_{Ш} + S_{ЗТВ}. \quad (19)$$

Как указывалось выше, наиболее достоверную оценку способов сварки с точки зрения стойкости сварного соединения к воздействию поражающего средства можно получить по результатам натурных испытаний путем обстрела. В качестве показателя стойкости примем величину приведенного импульса пробития преграды. Поскольку качество шва отличается от качества зоны термического влияния, стойкость этих участков сварного соединения к воздействию поражающего средства будет разная. Поэтому определим раздельно показатель поражаемости сварного шва:

$$K_{СТ}^{Ш} = \frac{J_{Ш}}{J_{ОМ}}, \quad (20)$$

и показатель поражаемости зоны термического влияния:

$$K_{СТ}^{ЗТВ} = \frac{J_{ЗТВ}}{J_{ОМ}}, \quad (21)$$

где $J_{ОМ}$, $J_{Ш}$ и $J_{ЗТВ}$ соответственно приведенные импульсы пробития для основного металла, сварного шва и зоны термического влияния, кг м/с.

Тогда показатель стойкости к поражению всего сварного соединения будет равен:

$$K_{СТ} = K_{СТ}^{Ш} \cdot K_{СТ}^{ЗТВ}, \quad (22)$$

С учетом показателей попадания K_{Π} и стойкости к поражению $K_{СТ}$ боевая уязвимость сварного соединения $K_{У}$ может быть оценена как:

$$K_{У} = K_{\Pi} \cdot (1 - K_{СТ}). \quad (23)$$

После подстановки выражений из формул 21, 22 и 23 получим следующую формулу для определения показателя боевой уязвимости сварного соединения:

$$K_{У} = \frac{S_{CC}}{S_{БК}} \cdot \left(\frac{J_{Ш} J_{ЗТВ}}{J_{ОМ}^2} \right). \quad (24)$$

Поврежденное в результате воздействия поражающего средства сварное соединение подлежит ремонту, для чего требуются определенные временные, материальные и трудовые затраты. Но можно утверждать, что затраты на проведение ремонта однотипных боевых повреждений сварных соединений [6] не зависят от способа сварки, с помощью которого получено это сварное соединение, а определяются принятой технологией ремонта. Поэтому, при сравнительной оценке способов сварки, предназначенных для производства сварного соединения, можно учитывать не стоимость ремонта сварного соединения, а сам факт возникновения его необходимости, т.е. факт расходования средств на ремонт. А он возникает в случае поражения сварного соединения.

Следовательно, можно принять, что:

$$K_{РЗ} = 1 - K_{СТ}, \quad (25)$$

где $K_{РЗ}$ – показатель ремонтных затрат, оценивающий необходимость затрат на ремонт сварного соединения вследствие его поражения.

Подставляя соответствующие выражения из формул 24, 25 и 26 получим:

$$K_{РЗ} = 1 - \left(\frac{J_{Ш} J_{ЗТВ}}{J_{ОМ}^2} \right). \quad (26)$$

Таким образом, получены выражения для определения технологического ($K_{Т}$), технического ($K_{К}$) и экономического ($З_{\Pi}$) показателей оценки способа сварки при получении сварного соединения бронированных деталей в производственной сфере, боевой ($K_{У}$) и экономический ($K_{РЗ}$) показатели в сфере боевой эксплуатации. Показатель эффективности способа сварки, общий вид которого приведен в формуле (1), можно представить с применением указанных показателей в следующем виде:

$$K_{Э} = \frac{K_{Т} K_{К} (1 - K_{У})}{З_{\Pi} (1 + K_{РЗ})}. \quad (27)$$

Достоинство предложенной методики в том, что она позволяет выполнять сравнение способов сварки по одному критерию. При этом учитываются характеристики как самого способа сварки, так и сварочного соединения, причем как на стадии производства, так и на стадии эксплуатации. При этом, следует отметить, что большинство из указанных характеристик, которые

используются для нахождения величины показателя эффективности, определяются на основе приборометрического метода замера, являющегося самым точным и объективным. Кроме того, в дальнейшем разработанную методику можно использовать в целях оптимизации при поиске наилучших условий (например, режима или сварочных материалов) выполнения (то есть технологического процесса) конкретного способа сварки. Одним из принципов, реализуемых при этой оптимизации, может быть максимизация как всего предложенного комплексного результата, так и его отдельных составляющих на единицу затрат [7].

Литература

1. ГОСТ 12.1.005-88 (2001) Система стандартов безопасности труда. Общие санитарно-гигиенические требования к воздуху рабочей зоны. – М.: Госстандарт, 2001. 2. Даценко І. П. Аналіз екологічної безпеки зварювальних робіт на бронетанкових ремонтних заводах / І. П. Даценко, В. В. Яблоков // Збірник наукових праць – К.: КІСВ, 1999. – С. 88-93. 3. Даценко І. П. Екологічні аспекти зварювальних робіт в ремонтному виробництві / І. П. Даценко // Збірник “Технології ремонту машин, механізмів, обладнання”. – К., АТМУ 2000. – С. 26-27. 4. Демидов В. А. Методы военно-экономического анализа. Часть 1. – М.: Военная инженерная радиотехническая академия

Выводы и перспективы дальнейших исследований

Основной задачей статьи было выработка методических подходов к повышению качества изготовления корпусов специальных автомобилей. Используя приведенные зависимости, можно вычислить технологическую себестоимость выполнения сварочных работ по соединению броневых деталей по существующей и предлагаемой технологиям и по результатам их сопоставления сделать вывод об экономической целесообразности внедрения предлагаемой технологии в сфере производства специальных бронированных автомобилей.

противовоздушной обороны. – 1985. – 619 с. 5. Каменев В. Д. Опыт организации и проведения технико-экономических исследований модернизации ВВТ при ремонте. – М.: изд-во ВА БТВ, 1983. – 87 с. 6. Маслов Н. Н. Эффективность и качество ремонта автомобилей. – М.: Транспорт, 1981. – 304 с. 7. Экономика производства, эксплуатации и ремонта вооружения и техники. Под ред. Марютина М. И. – М.: ВА БТВ. – 1989. – 188 с. 8. Средства защиты – НИИ Стали / Официальный сайт НИИ Стали. – Режим доступа до матеріалів: <http://www.niistali.ru>. 9. Ф. Лапшин. Броневахтовики / Авторевю – Украина. – К.: Авторевю, 2013. – С. 55 – 60.

МЕТОДИЧНІ ОСНОВИ ТЕХНІКО-ЕКОНОМІЧНОЇ ОЦІНКИ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ ЗВАРЮВАННЯ ПІД ЧАС ВИРОБНИЦТВА ТА МОДЕРНІЗАЦІЇ СПЕЦІАЛЬНИХ АВТОМОБІЛІВ

Іван Петрович Даценко (канд. техн. наук)

Національний університет оборони України імені Івана Черняхівського, Київ, Україна

При виробництві та модернізації спеціальних автомобілів важливе місце займають електрозварювальні роботи на броньових конструкціях. В даний час електрозварювальні роботи є, єдиним високопродуктивним способом надійного з'єднання деталей. Але при цьому їм притаманні серйозні недоліки, зумовлені принциповими особливостями зварювання, а саме, істотною відмінністю фізико-механічних властивостей зварного з'єднання від властивостей деталей, що зварюються, в результаті чого, якість зварного з'єднання (яке складається з зварного шва і зони термічного впливу) істотно нижче, ніж якість металу корпусу машини.

На підставі аналізу досвіду застосування броньованих спеціалізованих машин і вимог до захищеності даної групи техніки запропоновано методичний підхід вибору оптимального режиму зварювання конструкцій колісних броньованих машин. Запропонована методика може бути базовою для створення спеціалізованого програмного забезпечення в області пошуку раціональних підходів у процесі модернізації та проектування сучасних броньованих спеціалізованих автомобілів.

Ключові слова: броньовані спеціалізовані автомобілі; броньовий захист; критерій; показник; техніко-економічна оцінка; фізико-механічні властивості; вартість; навколишнє середовище; властивості; технічні характеристики; якість.

METHODICAL BASES FEASIBILITY ASSESSMENT WELDING PROCESS IN PRODUCTION OF MODERNIZATION OF SPECIAL VEHICLES

Ivan P. Datsenko (Candidate of Technical Sciences)

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

In the production and modernization of special vehicles occupy an important place electric welding work on the armor designs. Currently, electric welding works are the only high-way secure connections details. But in doing so, they have serious drawbacks due to fundamental features arc welding, namely, a significant difference of physical and mechanical properties of a welded joint on the properties of welded parts, whereby the quality of

the welded joint (which includes the weld and heat-affected zone) significantly lower than the quality of metal machine frame.

Based on the analysis of experience with specialized armored vehicles and requirements for this group of security appliances methodical approach of choosing the optimal mode of welding structures of wheeled armored vehicles. The proposed method can be the base for the creation of specialized software in the field of search of rational approaches in the process of modernization and the design of modern armored special vehicles.

Keywords: specialized armored vehicles; armor protection; criteria; indicators; technical and economic evaluation; physical and mechanical properties; cost; environment; features; specifications; quality.

References

1. GOST 12.1.005-88 (2001) Occupational safety standards system. [Sistema standartov bezopasnosti truda. Obshhie sanitarno-gigienicheskie trebovaniya k vozduhu rabochej zony]. General hygiene requirements for working zone air. - Moscow: State Standard.
2. Datsenko I.P. (1999), Analysis of ecological safety in welding armored repair plant. [Analiz ekolohichnoi bezpeky zvarivvalnykh robot na bronetankovykh remontnykh zavodakh], V.V. Yablokov, Collection Naukova Prace, Kyiv: KISV, pp. 88-93.
3. Datsenko I.P. (2000), Environmental aspects of welding to repair production. [Ekolohichni aspekty zvarivvalnykh robot v remontnomu vyrobnytstvi], Collection "Tehnologii repair machines mehanizmiv, obladnannya", Kyiv: Atma, pp. 26-27.
4. Demidov V.A. (1985), Methods of military-economic analysis. Part 1. [Metody voenno-jekonomicheskogo analiza. Chast' I], Moscow: Military Academy of Radio Engineering Air Defense, 619 p.
5. Kamenev V.D. (1983), Experience in organizing and carrying out feasibility studies modernization of weapons and military equipment for the repair. [Opyt organizacii i provedenija tehniko-jekonomicheskikh issledovanij modernizacii VVT pri remonte], Moscow: Publishing House VA BTV, 87 p.
6. Maslov N.N. (1981), Efficiency and quality car repair. [Jeffektivnost' i kachestvo remonta avtomobilej], Moscow: Transport, 304 p.
7. The economy of production, operation and maintenance of weapons and equipment. (1989), Ed. Maryutina M.I., Moscow: VA BTV, 188 p.
8. Remedies - Research Institute of Steel, Steel Research Institute official website. Access mode to materialiv: <http://www.niistali.ru>.
9. Lapshin F., (2013), Bronevahtoviki, Autoreview, Ukraine, Kyiv: Auto Review, pp. 55-60.

Отримано: 25.07.2016 року.

УДК 355.6

*Володимир Олександрович Дачковський (канд. техн. наук)**Ігор Володимирович Овчаренко (канд. військ. наук, доцент)**Національний університет оборони України імені Івана Черняховського, Київ, Україна*

АНАЛІЗ РОЗВИТКУ БОЙОВИХ БРОНЬОВАНИХ МАШИН

Проведено аналіз бойових броньованих машин, які запропоновані вітчизняним оборонно-промисловим комплексом України. На його основі визначені основні тенденції щодо їх розвитку. Визначено, що в основі формування бойових броньованих машин з урахуванням задач, які на них покладаються, в рамках яких будуть отримані оціночні чисельні значення показників і критеріїв якості бойових броньованих машин, повинні лежати три основних принципи:

базовий, який полягає в розробці базової платформи бойових броньованих машин;

агрегатно-вузловий, який полягає в створенні агрегатів і вузлів різного функціонального призначення на основі розмірної і функціональної взаємозамінності їх складових частин;

блочно-модульний, який полягає у визначенні можливостей уніфікації функціональних і технічних властивостей модулів, призначених для вирішення широкого спектра завдань різними військовими підрозділами.

Ключові слова: бойові броньовані машини; засоби ураження; тенденції розвитку; базовий агрегатно-вузловий і блочно-модульний принципи.

Вступ

Постановка проблеми. Бойові дії на Сході України обумовлені новими умови ведення збройної боротьби та широким застосуванням нових та модернізованих систем озброєння. З початком агресії Російської Федерації проти України на озброєнні ЗС України знаходились усі зразки озброєння та військової техніки (ОВТ), які за своїми термінами служби морально та фізично застаріли.

У зв'язку з цим провідні українські компанії вітчизняного оборонно-промислового комплексу і приватний бізнес запропонували для прийняття на озброєння великий асортимент бойових броньованих машин (ББМ) які на думку фахівців оборонно-промислового комплексу відповідають сучасним умовам.

Аналіз останніх досліджень і публікацій. В роботі [1] пропонується створення ББМ з використання броньованої капсули, яка встановлена всередині корпусу ББМ для розміщення та підвищення захищеності особового складу, але в даній роботі не розглядаються інші не менш важливі функціональні задачі які покладаються на ББМ. В [2-4] розглянуті зразки ББМ провідних країн світу, але в даній роботі не розглядаються основні напрямки розвитку ББМ. У [5] визначені основні заходи щодо планування розвитку ББМ.

Мета статті Враховуючи вищезазначене, стаття присвячена проведенню аналізу розвитку ББМ які запропоновані вітчизняним оборонно-промисловим комплексом, визначення їх недоліків та переваг та формулювання раціонального напрямку розвитку ББМ.

Виклад основного матеріалу дослідження

Для оновлення парку озброєння та військової техніки ЗС України за останні два роки оборонно-промисловий комплекс України запропонував велике різноманіття ББМ, які б могли замінити фізично застарілі та втрачені, під час виконання завдань за призначенням.

Отже, ПАТ “АвтоКрАЗ” розробив “лінійку” броньованих автомобілів: Kraz Shrek з колісною формулою 4x4, Kraz Fiona з колісною формулою 6x6, які здатні витримувати підривання на фугасах і обстріл з автоматичної зброї. Також, КрАЗ розробив 4-вісне шасі КрАЗ-7634НЕ для монтажу ракетних систем залпового вогню та інших систем озброєння замість старих МАЗів, БАЗів та інших багатовісних тягачів. З класу автомобілів підвищеної прохідності, розроблено Спартан (базове шасі Ford), Когуар (базове шасі Toyota) [6].

Корпорація “Богдан” розпочала в Україні складання армійських версій МАЗ-5316 (4x4), МАЗ-6317 (6x6), а також тягачів МАЗ-6425 (6x6) а з класу автомобілів підвищеної прохідності – 8-тонний бронеавтомобіль Барс-8, який розрахований на екіпаж 2 + 8 осіб. Барс-8 (платформа пікапа Dodge Ram) має захист рівня Stanag 4569 Level 2, оснащений 6,7-літровим дизелем Cummins потужністю 385 к.с та має критичну для нього масу 8 т. Модель – Барс-6 (виконана на шасі KIA Military), укомплектована 3,9-літровим дизелем Hyundai потужністю 139 к.с., механічною КПП і має масу 5,6 т [7].

В якості ще однієї альтернативи пропонуються автомобілі підвищеної прохідності “Козак” (Land Rover Defender). “Козак-2”, виконаний на шасі IVECO Cargo 4x4, бронеавтомобіль досить великий і високий, при цьому він має захист за

стандартом STANAG II та протимінне днище. Крім патрульних машин, НВО “Практика” пропонує і медичні броньовані автомобілі [8].

Також державні підприємства військово-промислового комплексу пропонують вітчизняний броньований транспортний засіб “Дозор-Б”, який комплектується силовим агрегатом німецької фірми Deutz BF 4M1013FC потужністю 190 к.с. При повній масі в 8,5 т, він здатний взяти на борт 10 осіб екіпажу і вести бойові дії [9].

Київський завод “Ленінська кузня” пропонує легко-броньовану плаваючу платформу “Тритон” – яка може взяти на борт до 11 чоловік і долати як бездоріжжя, так і водні перешкоди. “Тритон” укомплектований 5,7-літровим дизелем Volvo потужністю 211 к.с., автоматичною КПП Allison, бойовим модулем з дистанційним управлінням, до складу якого входить 12,7-мм кулемет та гранатомет. Також працюють над створенням БТР з колісною формулою 6х6. Платформа “Арбалет” теж буде плаваючою і матиме збільшений бронезахист (Level 3) [8].

Компанія “Техімпекс” представляє свою версію сучасного БТР. Її “Варан” з колісною формулою 8х8 представляє глибоку модернізацією БТР-70. Від колишнього БТР-70 залишилися тільки мости і деякі агрегати, а також нижня частина бронекорпусу.

Також пропонується створення броньовика на шасі ГАЗ-66, та модернізацію БРДМ-2, БМП [8].

Отже із аналізу основних тактико-технічних характеристик ББМ виникає ряд запитань, а саме:

для виконання яких бойових завдань призначені дані ББМ і чи дані завдання притаманні ЗС України;

чи відповідає запропонований ряд ББМ головним завданням “Державної цільової програми розвитку озброєння та військової техніки” щодо уніфікації ОВТ, тобто взаємозамінності запасних частин, вузлів та агрегатів;

який термін поставки запасних частин виробником та чи планується комплектування даних ББМ груповими комплектами запасних частин;

які в ЗС України є рухомі засоби технічного обслуговування та ремонту для технічного обслуговування та ремонту даного ряду ББМ в польових умовах.

Вирішення зазначених питань на сучасному етапі розвитку ОВТ має розглядатися в рамках системи національної безпеки держави і її головного компонента – Збройних Сил. При цьому обов'язково повинні враховуватися економічні можливості, науково-технічний потенціал та можливості по військово-технічній співпраці держави.

Напрямки розвитку конкретних зразків ОВТ визначаються ступенем залучення до вирішення однієї або декількох певних тактичних, технічних або функціональних задач.

При обґрунтуванні напрямів розвитку

(модернізації) ББМ слід враховувати існуючі світові тенденції розвитку засобів ураження і розвитку ББМ. Це дозволить виробити науково обґрунтовані підходи до формування вимог до сучасних ББМ.

При формуванні вимог до ББМ необхідно проаналізувати які засоби використовується для їх ураження. На даний час їх можна розподілити на звичайні та високоточні.

До звичайних засобів ураження ББМ відносяться ручні і реактивні протитанкові гранати, протитанкові міни, бронебійні, кумулятивні і кінетичні боєприпаси танків, ствольної артилерії і реактивні системи залпового вогню та стрілецька зброя.

Високоточними засобами ураження є крилаті ракети, авіаційні керовані ракети, керовані авіаційні бомби, касетні бомби, безпілотні літальні апарати, протитанкові керовані ракети, високоточні боєприпаси ствольної і реактивної артилерії.

В сучасних умовах найбільш пильна увага приділяється розвитку високоточної зброї, так як її застосування дозволяє забезпечити необхідну ефективність і розширити можливості по вогневому ураженню ББМ.

Серед основних тенденцій розвитку засобів ураження ББМ виділяють:

збільшення дальності вогневого ураження;
підвищення точності доставки засобів ураження до цілі;

автоматизацію процесів підготовки до бойового застосування, розширення області використання електронно-обчислювальної техніки і засобів автоматизації управління зброєю;
комплексування і уніфікацію озброєнь на всіх рівнях.

Поряд з цим серед тенденцій розвитку ББМ можна виділити наступні:

підвищення вогневої потужності;
підвищення захищеності;
підвищення рухливості;
поліпшення компонування;
впровадження систем командної керованості;
підвищення надійності;
продовження терміну служби.

Підвищення вогневої потужності ББМ направлено на збільшення показників ефективності ураження броньованих і укріплених цілей в будь-яких умовах обстановки і на максимальній дальності, а також на кардинальне розширення можливостей систем пошуку, виявлення, ідентифікації цілей різних класів.

Найбільш економічно прийнятним вважається напрямок вдосконалення показників вогневої потужності, заснований на використанні уніфікованих бойових модулів. Сутністю прийнятих конструкторських, технічних та технологічних рішень є реалізація можливостей військово-промислового потенціалу по самостійній розробці або закупівлі комплексів озброєння і систем управління ними, виконаних за

модульним принципом.

Підвищення захищеності бойової броньованої машини досягається за рахунок застосування нових броньових матеріалів, збільшення товщини броні, застосування спеціальних форм корпусів, використання спеціальних маскувальних радіопоглинаючих покриттів і масок, застосування спеціальних маскувальних фарб для зниження помітності.

Підвищення рівня захищеності ББМ може бути реалізовано шляхом:

застосування модульних конструкцій для підвищення захищеності корпусу та бойового модуля. Модульна конструкція дозволяє без зміни товщини броні підвищити захищеність і забезпечити можливість вдосконалення захищеності протягом життєвого циклу зразка. Застосування модульної конструкції дозволяє оперативно змінювати ступінь захищеності ББМ в залежності від поставлених бойових завдань. Зручність монтажу дозволяє швидко замінювати пошкоджені модулі в польових умовах.

Відповідно, комплект динамічного захисту дозволяє забезпечити круговий захист ББМ від ураження гранатами ручних протитанкових гранатометів і деякими типами кумулятивних снарядів.

Підвищення ефективності протимінного захисту досягається як за рахунок підвищення товщини броні (установка додаткових броньових листів з композиційних матеріалів, так і за рахунок спеціальної форми днища.

Застосування комплексу активного захисту підвищує захищеність ББМ від протитанкових засобів ураження незалежно від систем наведення і типу бойової частини.

Застосування електромагнітного і електротермічного захисту принцип дії якого полягає у впливі потужним імпульсом електричного струму на засіб ураження (за своєю суттю аналогічний динамічному захисту). Суть його полягає у використанні потужних електричних імпульсів для створення газоподібного робочого тіла, яке штовхає металеві пластини в сторону засобу ураження.

Застосування комплексів оптико-електронної протидії забезпечує попередження екіпажу про лазерне опромінювання ББМ в спектральному діапазоні 0,7–2,5 мкм і забезпечує постановку активних перешкод протитанковим комплексам з напівавтоматичною системою наведення шляхом постановки багатоспектральних аерозольних завіс, які гасять лазерне випромінювання.

Також повинні застосовуватись сучасні засоби і заходи забезпечення живучості та пожежовибухобезпеки.

Застосування засобів зниження помітності впровадженням маскувальних конструкцій дозволить знизити дальність виявлення.

В свою чергу підвищуючи захищеність бойової машини, необхідно приймати рішення по недопущенню перевищення масогабаритних вимог

і забезпечити збереження плавучості.

Підвищення рухливості забезпечується переходом на більш потужні багатопаливні дизельні двигуни; використанням досконаліших гідромеханічних трансмісій; поліпшенням конструкції і характеристик ходової частини.

Поліпшення компоновання ББМ полягає в формуванні вимог до розміщення вузлів і агрегатів, в першу чергу в інтересах забезпечення високої живучості екіпажу і десанту.

Основною складовою частиною функціонального призначення бойової машини є її корпус. Конструкційні рішення якого визначають архітектуру ББМ.

Впровадження систем командної керованості відбувається за рахунок забезпечення цифрового інформаційного та мовного обміну, використання сучасних систем навігації, що функціонують в реальному масштабі часу.

Для забезпечення безперервного управління підрозділами, бойовими групами, екіпажами ББМ і іншими взаємодіючими підрозділами повинен бути стійкий радіозв'язок в складних умовах радіоподавляючої обстановки. Забезпечення інформаційно-керуючою системою окремих бойових машин в єдину автоматизовану систему управління боєм і зброєю надає можливість створення єдиного "інформаційного простору", який забезпечує обмін інформацією як між ББМ (включаючи машини розвідки та БПЛА), так і засобами підтримки (системи залпового вогню, розвідувально-ударні ракетні комплекси.

Тобто, в основі формування зразка ББМ з урахуванням задач, які на неї покладаються, в рамках яких будуть отримані оцінки чисельних значень показників і критеріїв якості ББМ, в основі яких повинні лежати три основних принципи: базовий, агрегатно-вузловий і блочно-модульний.

Базовий принцип полягає в розробці основного зразка ББМ на "платформі" уніфікованої базової несучої конструкції відповідно з концептуальними підходами і передбачає модернізаційний потенціал виробу.

На даній "платформі" може бути змонтована бойова машина вогневої підтримки, самохідний міномет, бойова розвідувальна машина, командно-штабна машина, медична машина, ремонтно-евакуаційна машина, машина РХБ розвідки, машина артилерійської розвідки, машина інженерної розвідки та інші.

Агрегатно-вузловий принцип полягає в створенні агрегатів і вузлів різного функціонального призначення на основі розмірної і функціональної взаємозамінності їх складових частин.

Блочно-модульний принцип визначає можливість уніфікації властивостей функціональних і технічних модулів, призначених для вирішення широкого спектра завдань різними військовими підрозділами.

Висновки й перспективи подальших досліджень

Таким чином, існуюча тенденція застосування високоточних засобів ураження, вимагає вдосконалення як всього комплексу зразків ББМ, так і підвищення їх захищеності. Вирішуючи

завдання в усіх напрямках одночасно, необхідно враховувати як економічні можливості, так і пріоритети в завданнях, які виконуються із застосуванням ББМ на основі яких запропоновано підхід до формування перспективного зразка ББМ.

Література

1. Пат. 89968 Україна, МПК^С (2009) F 41 H 7/02. Легка броньована колісна машина / Купрієнко О.М., Лапицький С.В., Голуб В.А., Бісик С.П., Ларін О.Ю., Чеченкова О.Л.; заявник і володар патенту, Купрієнко О.М. – № u201312968; заяв. 8.11.2013; опубл. 12.05.2014, Бюл. № 9. 2. **Ф. Лапшин**. Броневахтовики / Авторевю – Україна. – К.: Авторевю, 2013. – С. 55-60.
3. **Холявський Г. Л.** Энциклопедия бронетехники. Боевые гусеничные машины 1919-2000 г. – Мн.: ООО “Харвест” 2001. – 656 с. 4. **Капранов М. Ю.** Современная бронетанковая техника армий иностранных государств / Капранов М. Ю., Шевченко А. В., Лукиянов А. В., Соколенко В. Н. и др. – Кубинка: ЗАО “Компания ИМАДЖВЕЙН”, 2010. – 394 с. 5. **Тарасов В. М.** Военно-технічна політика: навч. посіб. / Тарасов В. М., Терещенко А. М., Смірнов В. О., Копашинський С. А. та ін. – К.: НУОУ імені Івана Черняхівського, 2013. – 312 с.
6. **Автомобили КраЗ** спеціального призначення – Режим доступу: <http://www.autokraz.com.ua/index.php/ru/fabrication/automobile/military>.
7. **Звіт за результатами проведення XII міжнародної спеціалізованої виставки зброя та безпека – 2015** – Режим доступу: <http://www.iec-expo.com.ua/uk/zbroya-ta-bezpeka-2015.html>.
8. **Чем будем давать по зубам: Обзор новинок выставки “Зброя и безпека 2015”** – Режим доступу: <http://www.autoconsulting.com.ua/article.php?sid=34353>.
9. **Українська бронетехніка на виставці Eurosatory 2016** – Режим доступу: <https://www.autocentre.ua/ua/kommercheskie/voennaia-texnika/ukrayinska-bronetexnika-na-vistavtsi-eurosatory-2016-297824>

АНАЛІЗ РАЗВИТИЯ БОЕВЫХ БРОНИРОВАННЫХ МАШИН

Владимир Александрович Дачковский (канд. техн. наук)

Игорь Владимирович Овчаренко (канд. воен. наук, доцент)

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Проведен анализ боевых бронированных машин, которые предложены отечественным оборонно-промышленным комплексом Украины. На его основе определены основные тенденции их развития. Определено, что в основе формирования боевых бронированных машин с учетом задач, которые на них возлагаются, в рамках которых будут получены оценочные численные значения показателей и критериев качества боевых бронированных машин, должны лежать три основных принципа:

базовый, который заключается в разработке базовой платформы боевых бронированных машин;

агрегатно-узловой, который заключается в создании агрегатов и узлов различного функционального назначения на основе размерной и функциональной взаимозаменяемости их составных частей;

блочно-модульный, который заключается в определении возможностей унификации функциональных и технических свойств модулей, предназначенных для решения широкого спектра задач различными военными подразделениями.

Ключевые слова: *боевые бронированные машины; средства поражения; тенденции развития; базовый, агрегатно-узловой и блочно-модульный принципы.*

ANALYSIS OF ARMoured COMBAT VEHICLES

Volodymyr O. Dachkovskiy (Candidate of Technical Sciences)

Ihor V. Ovcharenko (Candidate of Military Sciences, Associate Professor)

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

Analysis of armored combat vehicles, proposed domestic military-industrial complex of Ukraine. On the basis of the basic trends of development. Determined that the basis for the formation of armored combat vehicles based tasks that rely on them, in which will the estimated numerical values of quality criteria and armored combat vehicles, should be based on three basic principles:

basic, which is to develop a base platform armored combat vehicles;

aggregate-node, which is to build units and units of different functions based on the dimensional and functional interchangeability of their components;

modular, which is to identify opportunities to unify functional and technical features modules designed for a wide range of tasks in different military units.

Keywords: *armored combat vehicles; equipment damage; trends; basic, aggregate-node and block-modular principles.*

References

1. **Pat. 89968** Ukraine, IPC (2009) F 41 H 02/07. Light armored wheeled vehicles, Kupriyenko O.M., Lapytskyy S.V. Golub V.A., Bisyk S.P., Larin O., Chechenkova O.L. [*Legka bronovana kolisna mashina*], The applicant and the owner of the patent Kupriyenko A.M. - № u201312968; statements. 08/11/2013; publ. 05.12.2014, Bull. Number 9.
2. **Lapshin F.** (2013), Bronevohovyyky, Autorevue, Ukraine, Kyiv: Auto Review, pp. 55-60.
3. **Holyavskiy G.** (2001), Encyclopedia Armoured Fighting Vehicle. [*Encyklopedia Bronetehniky. Boyovye husenychnie mashiny*], Mn.: profile "Harvest", 656 p.
4. **Kapranov M.** (2010), Modern technics bronetankovaya Army Foreign states. [*Sovremennay bronetankovaya tehnika armiy inostrannih gosudarstv*], Shevchenko A.V., Lukyanov A.V., Sokolenko V.N., ZAO "Company YMADZHVEYN", 394 p.
5. **Tarasov V.** (2013), Military-technical policy: [*Voennotekhnichna politika*] teach. posib, Tarasov V.N., Tereschenko A., Smirnov V.A., Kopashynskyy S.A. etc. Kyiv: NUOU Ivan Chernyakhovsky, - 312 p.
6. **Special purpose** KrAZ vehicles. [*Avtomobili Kraz specialnogo naznacheniy*], Access: <http://www.autokraz.com.ua/index.php/ru/fabrication/automobile/military>.
7. **Report on** the results of the XII international exhibition Arms and Security. [*Zvit za rezultatami prjvedenia XII miznarodnoi specializovanoi vistavki zbroa ta bezpeka – 2015*], Access: <http://www.iec-expo.com.ua/uk/zbroya-ta-bezpeka-2015.html>.
8. **Replace** we should give to the teeth: Browse new exhibition "Arms and Security 2015" [*Chem budim davit po zubam: Obzor novinok vistavki "Zbroa ta bezpeka – 2015"*], Access: <http://www.autoconsulting.com.ua/article.php?Sid = 34353>.
9. **Ukrainian armored** vehicles at the exhibition Eurosatory 2016. [*Ukrainskaa bronetehnika na vistavke Eurosatory 2016*], Access: <https://www.autocentre.ua/ua/kommercheskie/voennaya-tehnika/ukrayinska-bronetehnika-na-vistavtsi-eurosatory-2016-297824>

Отримано: 03.08.2016 року.

Микола Петрович Думенко (канд. військ. наук)

Генеральний штаб Збройних Сил України, Київ, Україна

АНАЛІЗ ФУНКЦІОНУВАННЯ СИСТЕМИ КАДРОВОГО ЗАБЕЗПЕЧЕННЯ ПІД ЧАС ДІЇ ОСОБЛИВОГО ПЕРІОДУ У 2014-2015 РОКАХ

У статті відображено основні результати діяльності кадрових органів щодо кадрового забезпечення у 2014-2015 рр. під час переходу на функціонування в умовах особливого періоду. Здійснено аналіз основних проблем в системі кадрового забезпечення та висвітлено шляхи їх вирішення. Аналіз діяльності кадрових органів Збройних Сил України під час дії особливого періоду у 2014-2015 роках свідчить, що основні зусилля спрямовувались на підтримання належного рівня укомплектованості військових частин бойового складу, збереження кадрового потенціалу, удосконалення порядку комплектування військ (сил) навченим особовим складом з метою забезпечення виконання військовими частинами (підрозділами) бойових завдань в районі проведення Антитерористичної операції на території Донецької та Луганської областей. У порівнянні з періодом функціонування військових організаційних структур на штатах мирного часу, вдалося значно збільшити обсяги залучення громадян на військову службу, у першу чергу завдяки спрощенню процедури укладання контрактів, упорядкуванню термінів проходження військової служби, налагодженню дієвої взаємодії з органами державної влади.

Ключові слова: особливий період; кадрове забезпечення; комплектування; особовий склад.

Вступ

Постановка проблеми. Збройна агресія Російської Федерації проти України стала основною причиною оголошення в державі часткової мобілізації, з моменту якої настав особливий період, який триває і зараз. Згідно з керівними документами [1, 2] під час дії особливого періоду набирають чинності особливості проходження громадянами України військової служби у Збройних Силах України, а, відповідним чином, діяльність органів військового управління і, зокрема, кадрових органів повинна бути спрямована на забезпечення швидкого та оперативного виконання завдань за призначенням.

Аналіз останніх публікацій і досліджень. Колишній радник з безпеки при ООН і НАТО, генерал-майор у відставці Франк ван Каппен, у своєму інтерв'ю заявив, що Росія веде проти України гібридну війну.

На думку доктора К. Вуйціцького з Центру студій Східної Європи Варшавського університету, те, що відбувається в Україні, можна назвати гібридною війною, яка полягає в тому, що сильна держава не може напасти на слабшу, тому намагається розділити її. Москва робить це, висилаючи диверсантів, мобілізуючи злочинців і проводячи інформаційну війну.

Подібну думку висловив і український політолог Сергій Таран. Якщо говорити про гібридну війну, то в Україні слово "гібридна" вживається у тому сенсі, що немає оголошеної повномасштабної війни. А є неоголошена, за допомогою малих диверсійних груп, які вчиняють провокації на території України, хоча вони прийшли з Росії, і дуже багато найманців-росіян. У цьому є сенс гібридної війни [3, с. 10].

Підполковник корпусу морської піхоти США Білл Немет, чия дисертація базується на досвіді обох чеченських війн, характеризує ведення гібридної війни, як сучасну форму партизанської війни, що використовує як сучасні технології, так і сучасні методи мобілізації [4, с. 23].

Однак, заходи, які використала Росія для здійснення агресії проти України, у всій їх повноті, так і не були до кінця концептуалізовані ні вітчизняними, ні західними науковцями. Сама генеза формування російської концепції "гібридної війни", етапи її розгортання, складники, стан реалізації "гібридного" протистояння в Україні та можливі напрямки протидії планам Російської Федерації у цій сфері мають бути додатково досліджені й опрацьовані.

Тим паче, до цього часу недослідженим залишається питання функціонування Збройних Сил нашої держави і, зокрема, діяльність кадрових органів у обстановці, що склалася. Саме тому розгляд даної теми стає актуальним у контексті відображення спроможності кадрових органів виконувати завдання в умовах гібридної війни, яка досі називається "особливим періодом".

Стаття має **на меті** проведення аналізу функціонування системи кадрового забезпечення під час дії особливого періоду, а саме відображення основних результатів діяльності та визначення подальших перспектив кадрової роботи.

Викладення основного матеріалу дослідження

Виходячи з досвіду ведення бойових дій під час Великої Вітчизняної війни стає очевидним, що система, яка ефективно функціонує в мирний час,

нездатна ефективно відповідати на всі виклики і загрози, які постають перед державою та її збройними силами з початком війни.

З перших днів війни перед кадровими органами радянської армії постали складні і відповідальні завдання. Виснажлива збройна боротьба, пов'язана із великими втратами особового складу, викликала гостру необхідність у кадрах офіцерського складу. Необхідно було віднайти кадри для поповнення втрат в діючій армії і забезпечення ними нових формувань, організувати підготовку досвідчених кадрів для створення відповідних резервів, виконувати роботу з комплектування, обліку кадрів, присвоєнню військових звань і нагороджень.

Кадровим органам довелося в умовах бойових дій переходити на організацію воєнного часу, формувати нові частини і з'єднання, формувати ряд нових кадрових органів і одночасно перелаштовуватися на методи роботи воєнного часу до яких у мирний час вони були не підготовані.

Крім труднощів, які створювалися складною обстановкою на фронтах, робота кадрових органів на початкових етапах війни ускладнювалася рядом інших важливих причин:

1. Крайня нестача численності особового складу кадрових органів, особливо в період відмобілізування військ. Так, відділи кадрів фронтів у своєму складі мали по 36 офіцерів і 4 службовці, а відділи кадрів армій – по 12 офіцерів і 2 службовці.

2. Надмірна централізація роботи з офіцерським складом з питань присвоєння військових звань і присвоєння офіцерів на посади. Військові кадрові органи змушені були направляти в центр велику кількість подань і тривалий час очікувати рішень.

3. Відсутність основоположних документів, які б визначали особливості проходження військової служби офіцерським складом у воєнний час.

4. Наявність серйозних недоліків у веденні облікових документів на кадрових офіцерів та офіцерів запасу. Значна частина офіцерів не мали особових справ, послужних карток та інших облікових документів [5].

Основними недоліками в роботі кадрових органів радянської армії були: недостатня оперативність, поверхневий підхід в розстановці кадрів, механічний розподіл їх по військових частинах і з'єднаннях. Офіцери відділів кадрів тільки й встигали складати списки на офіцерів, які поступали і формувати команди для їх відправки на фронт.

Не дивлячись на існуючий досвід, аналіз роботи кадрових органів Збройних Сил України показав, що сучасна система кадрового забезпечення також є далеко недосконалою. Нормативно-правова база, яка розроблялася в мирний час виявилася неадекватною в особливий період. Кадрові органи зіткнулися з низкою складних задач, таких як:

1. Організація прибуття до материкової частини України військовослужбовців військових частин, дислокованих на території Автономної Республіки Крим та міста Севастополя, та членів їх сімей;

2. Залучення офіцерського складу на військову службу за контрактом;

3. Унормування питання звільнення з військової служби військовослужбовців, які були призвані на військову службу під час мобілізації, на особливий період;

4. Збільшення обсягів залучення громадян на військову службу за контрактом для доукомплектування бойових частин мотивованим особовим складом;

5. Призов на строкову військову службу та комплектування ЗС України та інших військових формувань військовослужбовцями строкової військової служби, а також визначення порядку звільнення даної категорії;

6. Удосконалення системи військової освіти;

7. Забезпечення якісної підготовки військових фахівців відповідно до потреб Збройних Сил України у підготовленому особовому складі, з урахуванням втрат військ (сил) під час виконання бойових завдань на сході країни.

8. Здійснення кадрового забезпечення програм міжнародного співробітництва;

9. Удосконалення законодавства щодо запровадження короткострокових контрактів, розширення переліку підстав для звільнення військовослужбовців з військової служби за етапами особливого періоду, забезпечення врегулювання проблем у гуманітарній та соціальних сферах;

10. Спрощення механізму підготовки документів до прийняття кадрових рішень для забезпечення оперативності при їх підготовці і прийнятті;

11. Запровадження персонального обліку втрат особового складу;

12. Автоматизація процесів прийняття кадрових рішень;

13. Прискорення отримання статусу учасника бойових дій військовослужбовцями.

Умови, що склалися вимагали швидкого та оперативного реагування для вирішення зазначених проблем з використанням наявних сил і засобів. Саме тому, у 2014-2015 роках кадрові органи основні зусилля у своїй діяльності спрямовували на вирішення завдань направлених на виконання заходів мобілізаційного розгортання Збройних Сил України, а саме:

продовження прийняття на військову службу за контрактом осіб офіцерського та рядового, сержантського складу;

організацію підготовки до призову та призов громадян України на строкову військову службу, на службу за призовом осіб офіцерського складу;

доукомплектування визначених військових частин до штатів воєнного часу та формуванні підрозділів територіальної оборони;

опрацювання змін та доповнень до діючих нормативно-правових актів стосовно удосконалення порядку проходження військової служби, організації призову громадян України на строкову військову службу в особливий період та призову на військову службу за призовом осіб офіцерського складу, звільнення з військової служби;

супроводження звільнення визначених категорій військовослужбовців;

організацію зустрічі та розміщенні військовослужбовців військових частин та членів їх сімей, дислокованих на території АР Крим;

підготовку навчальних центрів, навчальних підрозділів, загальновійськових полігонів та їх матеріально-технічної бази до зустрічі молодого поповнення та організація їх підготовки;

реалізацію заходів, передбачених замислами застосування, перегрупування, заміни та нарощування бойових спроможностей угруповань військ (сил).

Стосовно організації зустрічі, обліку та розміщення на материковій частині України військовослужбовців військових частин, дислокованих на території Автономної Республіки Крим та міста Севастополя, і членів їх сімей було розгорнуто та функціонувало 5 збірних пунктів на фондах військових частин.

У результаті діяльності кадрових органів стосовно даного питання було досягнуто наступних показників.

1. Створено необхідні умови для переміщення військовослужбовців Збройних Сил України з АР Крим, як у складі підрозділів, військових частин, установ та організацій Збройних Сил України так і методом поодинокого переміщення через створені збірно-пересильні та збірні пункти.

2. У встановлені терміни організовано роботу щодо організації передислокації військових частин Збройних Сил України з Автономної Республіки Крим та міста Севастополь [6].

3. Заведено облік військовослужбовців, переміщених з АР Крим, який здійснюється у Кадровому центрі Збройних Сил України за результатами узагальнення інформації, переданої зі штабів військових частин та збірних пунктів. При цьому перепрізначення до інших військових частин Збройних Сил України дозволялося тільки тих військовослужбовців, які вийшли з АР Крим методом поодинокого переміщення і були зареєстровані на збірних пунктах.

4. Призначення військовослужбовців Збройних Сил України до інших військових частин після їх переміщення з АР Крим було суттєво обмежено. Крім того, рішенням начальника Генерального штабу – Головнокомандувача Збройних Сил України особовий склад Військово-Морських Сил Збройних Сил України утримувався на своїх посадах у існуючих штатах до прийняття рішення щодо подальшого функціонування або розформування (переформування) військових частин. Визначення подальшого службового

використання військовослужбовців військових частин інших видів Збройних Сил, які прибули до материкової частини України, проводилося кадровими органами також з урахуванням рішень щодо подальшого функціонування військових частин, в яких вони перебували на посадах .

5. Виведення (переміщення) військ (сил) з анексованого півострова Крим та досвід, який отриманий при цьому, надав можливість подальшого функціонування Військово-Морських Сил Збройних Сил України, військових частин інших видів Збройних Сил України, передислокованих з Автономної Республіки Крим та міста Севастополь в нових організаційно-штатних структурах та пунктах постійної дислокації.

Що стосується питання запровадження військової служби за призовом осіб офіцерського складу на виконання Указу Президента України [7] кадровими органами:

визначено обсяги ресурсу офіцерського складу, який перебуває на військовому обліку у військових комісаріатах та задовольняє вимогам до призову на військову службу;

підготовлено доповнення до проекту закону щодо унормування питань запровадження військової служби за призовом осіб офіцерського складу [8];

для остаточного унормування питань призову осіб офіцерського складу опрацьовано пропозиції щодо удосконалення порядку проходження військової служби;

відпрацьовано розпорядження щодо визначення переліку первинних вакантних посад для комплектування офіцерами військової служби за призовом;

відпрацьовано План заходів щодо організації призову громадян України на військову службу за призовом осіб офіцерського складу до Збройних Сил України, який уточнює порядок і терміни опрацювання нормативно-правових актів та практичних заходів для впровадження призову офіцерів на військову службу.

Таким чином, заходи, які вживались особовим складом управління кадрового забезпечення стосовно запровадження військової служби за призовом осіб офіцерського складу дозволили виконати завдання щодо забезпечення проведення часткової мобілізації.

Питання мобілізації тягло за собою визначення порядку роботи органів військового управління та командирів та усіх рівнів щодо звільнення військовослужбовців, призваних на військову службу під час мобілізації, на особливий період. Відповідним чином, було підготовлено директиву [9], а також доведено до органів військового управління, військових частин та установ Методичні рекомендації щодо порядку звільнення військовослужбовців, призваних на військову службу під час мобілізації, на особливий період [10].

Крім того, було опрацьовано зміни до трьох Указів Президента України стосовно унормування питання звільнення з військової служби військовослужбовців, які були призвані на військову службу під час мобілізації, на особливий період [11, 12, 13], а також проведено погодження постанови Кабінету Міністрів України щодо затвердження переліку сімейних обставин та інших поважних причин, що можуть бути підставою для звільнення громадян з військової служби та служби осіб рядового і начальницького складу [14].

У результаті проведеної роботи, кадровими органами ефективно планується, організується та здійснюється планове звільнення військовослужбовців, призваних на військову службу під час мобілізації, на особливий період. Створена нормативно-правова та методична база звільнення військовослужбовців, призваних на військову службу під час мобілізації, на особливий період, а також дотримання соціальних прав та гарантій звільнених військовослужбовців. Ведеться постійний моніторинг кількості звільнених військовослужбовців та потреби щодо їх заміни.

У ході проведення антитерористичної операції на сході України виникло проблемне питання щодо необхідності збільшення у військових частинах частки військовослужбовців за контрактом, як найбільш мотивованої та професійної категорії військовослужбовців.

У зв'язку з зазначеним, перед кадровими органами постало завдання збільшення обсягів залучення громадян на військову службу за контрактом для доукомплектування бойових частин мотивованим особовим складом.

З цією метою, протягом 2014 – 2015 років за участю офіцерів кадрових органів було ініційовано зміни до законодавства щодо спрощення порядку відбору, оформлення документів кандидатів та розширено коло осіб, яких можливо приймати на військову службу за контрактом, а саме:

внесено зміни до законів, якими впроваджено соціальні гарантії для військовослужбовців за контрактом [15, 16, 8];

з червня 2015 року впроваджено грошову винагороду при вступі на військову службу за контрактом;

розроблено Методичні рекомендації щодо особливостей укладання контрактів з громадянами та військовослужбовцями, які приймаються на військову службу за контрактом рядового, сержантського та старшинського складу Збройних Сил України [17].

Задля максимального залучення на військову службу за контрактом протягом 2014 – 2015 років внесено зміни до законодавства щодо укладення контракту до отримання результатів спеціальної перевірки, що дозволило скоротити процедуру укладання контракту. Впроваджено короткостроковий контракт. Розширено коло осіб, яких можливо приймати на військову службу за

контрактом. Спрощено процедуру проходження військово-лікарської комісії.

Важливими мотиваційними чинниками для вступу на військову службу за контрактом стало впровадження норм щодо збереження:

місяця роботи та середнього заробітку на строк до завершення особливого періоду для осіб, яких прийнято на військову службу за контрактом під час кризової ситуації;

місяця роботи та середнього заробітку понад рік для осіб, яких призвано під час мобілізації та які підлягають звільненню, але продовжують військову службу та укладають короткостроковий контракт;

пенсії на строк до завершення особливого періоду для осіб, яких прийнято на військову службу за контрактом під час кризової ситуації.

Постановою КМУ з червня 2015 року впроваджено грошову винагороду при вступі на військову службу за контрактом

Таким чином, виконання зазначених заходів дозволило за час проведення АТО в Донецькій та Луганській областях (у період пріоритетності виконання військоматами завдань мобілізації) частково вирішити проблему комплектування військ професійним особовим складом.

Проте, комплектування Збройних Сил на професійній основі не зменшувало необхідності комплектування військових частин (підрозділів) забезпечення військовослужбовцями строкової військової служби, що було необхідним для максимального вивільнення військовослужбовців інших категорій для залучення в АТО.

Крім того, необхідно було вирішити проблему звільнення військовослужбовців строкової військової служби, які вислужили встановлені строки військової служби, не залучались в АТО та обумовили соціальну напругу у військових колективах і в сім'ях військовослужбовців.

З метою, вирішення даної проблеми протягом 2014–2015 років кадровими органами було внесено зміни до законодавства щодо можливості здійснювати призов громадян на строкову військову службу під час дії особливого періоду та звільнення військовослужбовців строкової військової служби, які вислужили до 2 років (два терміни) строкової військової служби.

Внесення змін у законодавство та проведення заходів щодо можливості призову громадян на строкову військову службу під час особливого періоду дозволило:

у квітні – червні 2015 року призвати на строкову військову службу близько 20 тис. осіб;

отримати додаткове джерело комплектування особовим складом під час особливого періоду;

залучити до участі в АТО додаткову кількість військовослужбовців за контрактом (військовослужбовців призваних під час мобілізації), які раніше виконували завдання у військових частинах забезпечення, базах, арсеналах, складах, на аеродромах тощо, на заміну яким прибули військовослужбовці строкової військової служби.

Ще одним джерелом доукомплектування бойових частин та підрозділів забезпечення повинні стати випускники вищих військових навчальних закладів, військових навчальних підрозділів вищих навчальних закладів та навчальних центрів. Саме тому у системі військової освіти продовжувалась робота щодо вдосконалення змісту підготовки військових фахівців, інтеграції навчального процесу з підготовкою та завданнями військ (сил) з урахуванням бойового досвіду, отриманого у ході проведення АТО та оптимізації мережі ВВНЗ та ВВП ВНЗ та навчальних центрів.

Особливість системи військової освіти обумовлена участю військ у проведенні АТО та складним процесом заходів, які проводились і продовжують проводитись з одночасним виконанням завдань навчально-виховного процесу у вищих військових навчальних закладах, військових навчальних підрозділах вищих навчальних закладів навчальних центрів та залученням викладацького складу та курсантів до виконання бойових завдань за призначенням.

Продовжено практику залучення керівного складу Генерального штабу Збройних Сил України, інших органів військового управління Збройних Сил України до занять зі слухачами та науково-педагогічними працівниками Національного університету оборони України, забезпечено залучення представників замовників до проведення занять з курсантами (студентами) вищих військових навчальних закладів.

Впроваджено практику залучення в якості керівників занять, командирів відділень (взводів) навчальних підрозділів навчальних центрів курсантів вищих військових навчальних закладів та військових коледжів, які безпосередньо приймали участь у виконанні бойових завдань в АТО.

Проведено заходи щодо створення факультету військово-морських сил Одеської національної морської академії та відділення військової підготовки Морського коледжу технічного флоту Одеської національної морської академії.

Протягом 2014–2015 років постійно проводилося уточнення показників потреб у підготовці офіцерського складу відповідно до змін чисельності Збройних Сил України.

У результаті, заходи, які проводились стосовно підготовки персоналу та визначення потреби у фахівцях у зазначений період були спрямовані на якісну їх підготовку до виконання завдань за призначенням у обсягах, необхідних для виконання завдань за призначенням.

Додатково було проведено часткове розгортання мережі та структури курсів підвищення кваліфікації при ВВНЗ (ВВП ВНЗ) та навчальних центрів Збройних Сил України, що дозволило:

організувати підготовку військовозобов'язаних, призваних по мобілізації, на особливий період та призваних на військову

службу за контрактом з числа офіцерського, сержантського та рядового складу;

зосередити підготовку військових фахівців рядового, сержантського (старшинського) і офіцерського складу на єдиній навчальній матеріально-технічній базі вищих військових навчальних закладів;

досягти сумісності навчального процесу у навчальних центрах з заходами підготовки військ (сил) з урахуванням досвіду виконання військами завдань за призначенням у ході проведення АТО.

Підвищення кваліфікації офіцерського складу здійснювалася на 12 курсах перепідготовки та підвищення кваліфікації офіцерів призваних із запасу за відповідними переліками військово-облікових спеціальностей з терміном навчання 1 місяць та загальним обсягом одночасної підготовки близько 6 тис. осіб.

Протягом 2014-2015 років пройшли навчання на курсах підвищення кваліфікації близько 9 тис. офіцерів, призваних на військову службу під час мобілізації.

Таким чином, призов офіцерського складу до курсів перепідготовки та підвищення кваліфікації при ВВНЗ, ВВП ВНЗ надав можливість забезпечити необхідний рівень їх підготовки до виконання завдань за призначенням.

Якщо підготовка офіцерського складу постійно вдосконалювалася і у вирішенні даного питання було досягнуто значних результатів, то особливістю підготовки рядового та сержантського (старшинського) складу у періоду проведення АТО була організація одночасного навчання військовослужбовців призваних під час мобілізації та військовослужбовців за контрактом, що в свою чергу створювало додаткові труднощі під час планування періодів навчання та впливало на організований їх початок і завершення.

Так, основним завданням у зазначений період для кадрових органів стало забезпечення якісної підготовки військових фахівців відповідно до потреб Збройних Сил України у підготовленому особовому складі, з урахуванням втрат військ (сил) під час виконання бойових завдань на сході країни.

За результатами діяльності кадрових органів з початку проведення заходів АТО було підготовлено та направлено до військ (сил) понад 90 тис. осіб.

Що стосується напрямку кадрового забезпечення програм міжнародного співробітництва, було надано роз'яснення щодо порядку повернення до України (відкликання) національних контингентів, національного персоналу, окремих військовослужбовців та працівників, які перебувають на навчанні за кордоном.

Крім того, відповідно до Плану кадрового забезпечення міжнародних програм навчання військовослужбовців Збройних Сил України та працівників Збройних Сил України у навчальних

закладах іноземних держав з початку 2014 року підготовлено 160 осіб.

Враховуючи відсутність нормативно-правового врегулювання питання щодо визначення чіткого порядку утримання (обліку) та подальшого використання військовослужбовців, які перебувають у складі національних контингентів за кордоном та на посади, яких, призиваються громадяни України із запасу під час оголошеної мобілізації, з метою упорядкування питання щодо доукомплектування військових частин (підрозділів), які формують національні контингенти в умовах особливого періоду було підготовлено відповідні розпорядчі документи.

Суттєві недоліки та упущення в законодавстві України у перші дні проведення часткової мобілізації було виявлено стосовно запровадження короткострокових контрактів на проходження військової служби в особливий період (до завершення особливого періоду), розширення переліку підстав для звільнення військовослужбовців з військової служби за етапами особливого періоду, забезпечення врегулювання проблем, які мали місце на той час у гуманітарній та соціальних сферах.

З метою усунення зазначених проблем офіцерами кадрових органів опрацьовувались пропозиції щодо внесення змін до керівних документів щодо удосконалення оборонно-мобілізаційних питань під час проведення мобілізації та соціального захисту військовослужбовців. Зміни, які були внесені до законодавства України, забезпечили врегулювання основних проблем, що виникли під час проведення часткової мобілізації та дозволили провести перші черги часткової мобілізації.

Верховною Радою України опрацьовано Закон України щодо удосконалення оборонно-мобілізаційних питань під час проведення мобілізації. Вищезазначеним Законом України, зокрема, внесені зміни до нормативних документів стосовно звільнення військовослужбовців з військової служби під час дії особливого періоду [18, 11].

З метою забезпечення організації та своєчасного виконання заходів щодо звільнення військовослужбовців було підготовлено відповідні рекомендації щодо порядку застосування деяких положень Закону України "Про військовий обов'язок і військову службу". Таким чином, було проведено своєчасне звільнення військовослужбовців Збройних Сил України в порядку реалізації зазначених законів. Досвід організації вищезазначеного звільнення військовослужбовців Збройних Сил України використаний під час проведення звільнення військовослужбовців, призваних на військову службу під час мобілізації, на особливий період під час першої, другої та третьої черг мобілізації [19, 20].

Під час виконання заходів щодо внесення змін до існуючого законодавства постало питання

розробки нових нормативних документів стосовно удосконалення роботи кадрових органів та надання їм можливості прийняття кадрових рішень у стислі терміни. Так з метою забезпечення оперативності при підготовці і прийнятті кадрових рішень, на підставі Методичних рекомендацій з порядку організації підготовки документів до прийняття кадрових рішень кадровими органами Збройних Сил України, був розроблений та доведений до командирів (начальників) усіх рівнів спрощений механізм підготовки документів до прийняття кадрових рішень, застосування якого дозволяє:

уникнути тривалої підготовки значної кількості документів для перепризначення військовослужбовців при проведенні організаційних заходів;

забезпечити оперативне переміщення військовослужбовців до визначених військових частин для їх негайного доукомплектування особовим складом;

запобігти випадкам зволікання при призначенні військовослужбовців та проявам корупції у роботі кадрових органів.

Як результат, завдяки запровадженню вищезазначеного спрощеного механізму підготовка документів щодо призначення на посади, прийняття кадрових рішень та їх доведення до військ (сил) здійснюється за 3-4 доби.

Всі роз'яснення з основних питань кадрової роботи у військових частинах з урахуванням вимог положень діючого законодавства, керівних документів Міністерства оборони України та Генерального штабу Збройних Сил України, а також окремих рішень керівного складу Збройних Сил України закладено в Пам'ятку командира бригади (полку) з кадрових питань під час дії особливого періоду. З метою належної організації кадрової роботи та обліку особового складу її було доведено до кожної окремої військової частини для вивчення і застосування у повсякденній діяльності.

Належний облік особового складу передбачав запровадження персонального обліку втрат особового складу. Задля вирішення даного питання у Кадровому центрі Збройних Сил України створено окремий структурний підрозділ – відділення персонального обліку втрат особового складу.

На підставі чинного законодавства підготовлені Схема обліку загиблих (померлих) у Збройних Сил України та Схема обліку поранених у Збройних Сил України [21, 22].

Підготовлено ряд розпорядчих документів відповідно до яких:

організовано роботу щодо ведення персонального обліку загиблих та поранених військовослужбовців у військових частинах (підрозділах), оперативного збору та надання інформації;

здійснюється узагальнення інформації (чисельності, списків та персональних даних) за визначеними формами та готуються інформаційні матеріали для надання до органів державної влади, засобів масової інформації офіційних даних щодо втрат особового складу Збройних Сил України.

На підставі рішень керівництва Міністерства оборони України та Генерального штабу, заведений та ведеться окремих облік військовослужбовців Збройних Сил України, які загинули, отримали поранення та зникли безвісти.

Разом з тим, для оперативного інформування керівництва Міністерства оборони України та Генерального штабу Збройних Сил України про кількісні та якісні показники укомплектованості Збройних Сил України персоналом, автоматизації процесів прийняття кадрових рішень на всіх рівнях управління у 2015 році розпочата робота з розгортання та впровадження інформаційно-аналітичної системи "Персонал".

І нарешті, не менш вагомими є результати діяльності кадрових органів стосовно визнання військовослужбовців учасниками бойових дій. Так, відповідно до наказу Міністерства оборони України було утворено спеціальні комісії з розгляду матеріалів, що значно прискорило отримання статусу учасника бойових дій особами, які захищали суверенітет та територіальну цілісність держави, приймали участь у антитерористичній операції [23].

Висновки й перспективи подальших досліджень

Отже, досвід ведення бойових дій у роки війни, а також досвід проведення АТО в Україні показав, що Збройні Сили, а відповідно їх кадрові органи

Література

1. Закон України "Про мобілізаційну підготовку та мобілізацію" від 21.10.1993 № 3543/ХІІ (зі змінами) – К., 1993. 2. Закон України "Про оборону України від 06.12.1991 № 1932/ХІІ (зі змінами) – К., 1991. 3. Гібридна війна в Україні, думки експертів/ Polonews, 2014. 4. Armed Forces Journal: Hybrid vs. compound war, 2009. 5. Военные кадры в ВОВ/ под ред. Дукачева М.П., 1963. 6. Наказ Міністра оборони України від 05.04.2013 № 230 "Про організацію передислокації військових частин Збройних Сил України з Автономної Республіки Крим та міста Севастополь". 7. Указ Президента України від 01.05.2014 № 447/2014 "Про заходи щодо підвищення обороноздатності держави". 8. Закон України "Про соціальний і правовий захист військовослужбовців та членів їх сімей"/ ВВР від 20.12.1991 № 2012-ХІІ (зі змінами). 9. Спільна директива Міністерства оборони та Генерального штабу Збройних Сил України від 2 березня 2015 року № Д-1 "Про звільнення військовослужбовців, які були призвані на військову службу під час мобілізації, на особливий період". 10. Методичні рекомендації щодо порядку звільнення військовослужбовців, призваних на військову службу під час мобілізації, на особливий період, затверджені начальником Генерального штабу – Головнокомандувачем Збройних Сил України 1 березня 2015 року. 11. Указ Президента України від 6 травня 2015 року № 254 "Про звільнення з військової служби

змушені миттєво реагувати на всі виклики і загрози, які перед ними постають. Аналіз роботи кадрових органів показав, що нормативно-правова база, яка відповідає умовам мирного часу є неадекватною в умовах особливого періоду та виявив ряд недоліків, які негативно впливають на рівень боєздатності Збройних Сил, а саме:

необхідність обов'язкового проходження військовозобов'язаними фахової та бойової підготовки (так, з числа призваних по мобілізації понад 90 тис. осіб направлено на підготовку до курсів перепідготовки та підвищення кваліфікації, навчальних центрів та полігонів);

короткий термін військової служби;

додаткові витрати з бюджету (проходження підготовки, виплата грошового забезпечення за попереднім місцем служби, виплата пенсії, витрати на забезпечення соціальних пільг та ін.);

необхідність внесення змін до існуючої нормативно-правової бази;

низький рівень підготовленості, морально-психологічного стану, відношення до військової служби.

Ураховуючи всі помилки, кадровими органами Збройних Сил України під час переходу на функціонування в особливий період протягом 2014-2015 рр. було досягнуто значних результатів. У розрізі того, що Україна перебуває у стані неоголошеної війни, а також тому, що особливий період досі триває, актуальним залишається питання удосконалення системи кадрового забезпечення та надання їй універсального характеру, що дасть змогу однаково ефективно вирішувати кадрові питання, як у мирний час так і в особливий період.

військовослужбовців, які були призвані на військову службу під час мобілізації, на особливий період відповідно до Указу Президента України від 6 травня 2014 року № 454 "Про часткову мобілізацію". 12. Указ Президента України від 12 червня 2015 року № 328 "Про звільнення з військової служби військовослужбовців, які були призвані на військову службу під час мобілізації, на особливий період. 13. Указ Президента України від 21 липня 2014 року № 607 "Про часткову мобілізацію". 14. Постанова Кабінету Міністрів України "Про внесення змін до постанови Кабінету Міністрів України від 12 червня 2013 року № 413 "Про затвердження переліку сімейних обставин та інших поважних причин, що можуть бути підставою для звільнення громадян з військової служби та служби осіб рядового і начальницького складу". 15. Закон України "Про військовий обов'язок та військову службу"/ Постанова ВР від 25.03.1992 № 2233-ХІІ (зі змінами). 16. Закон України "Про Кодекс законів про працю України" від 10.12.1971 № 322-VIII (зі змінами). 17. Методичні рекомендації щодо особливостей укладання контрактів з громадянами та військовослужбовцями, які приймаються на військову службу за контрактом рядового, сержантського та старшинського складу Збройних Сил України, затверджені начальником Генерального штабу – Головнокомандувачем Збройних сил України від

12.09.2014 № 19563/С. **18. Закон України № 1275-ІV** “Про внесення змін до деяких законодавчих актів України щодо удосконалення оборонно-мобілізаційних питань під час проведення мобілізації”, який набрав чинності 8 червня 2014 року. **19. Рекомендації** щодо порядку застосування деяких положень Закону України “Про військовий обов’язок і військову службу”. **20. Закон України** від 20.05.14 № 1275-VII “Про внесення змін до деяких законодавчих актів України щодо удосконалення оборонно-мобілізаційних питань під час проведення мобілізації” (зі змінами). **21. Наказ Міністерства** оборони України від 26.05.2014 № 333

“Про затвердження Інструкції з організації обліку особового складу Збройних Сил України”. **22. Спільна директива** Міністерства оборони та Генерального штабу Збройних Сил України від 08.10.2014 № Д-4 “Про порядок зарахування в розпорядження окремих категорій військовослужбовців Міністерства оборони України та Збройних Сил України”. **23. Наказ Міністерства** оборони України від 07.05.2015 № 200 “Положення про комісії Міністерства оборони України з питань розгляду матеріалів про визнання учасниками бойових дій”.

АНАЛИЗ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ КАДРОВОГО ОБЕСПЕЧЕНИЯ ВО ВРЕМЯ ОСОБОГО ПЕРИОДА В 2014-2015 ГГ.

Николай Петрович Думенко (канд. воен. наук)

Генеральный штаб Вооруженных Сил Украины, Киев, Украина

В статье отображены основные результаты работы кадровых органов касательно кадрового обеспечения в 2014-2015 гг. во время перехода на функционирование в условиях особого периода. Проведен анализ основных проблем в системе кадрового обеспечения и отображены пути их решения. Анализ деятельности кадровых органов Вооруженных Сил Украины во время действия особого периода в 2014-2015 годах показывает, что основные усилия направлялись на поддержание надлежащего уровня укомплектованности воинских частей боевого состава, сохранение кадрового потенциала, совершенствование порядка комплектования войск (сил) обученным личным составом с целью обеспечения выполнения воинскими частями (подразделениями) боевых задач в районе проведения антитеррористической операции на территории Донецкой и Луганской областей. По сравнению с периодом функционирования военных организационных структур на штатах мирного времени, удалось значительно увеличить объемы привлечения граждан на воинскую службу, в первую очередь благодаря упрощению процедуры заключения контрактов, упорядочению сроков прохождения воинской службы, налаживанию действенного взаимодействия с органами государственной власти.

Ключевые слова: *особый период; кадровое обеспечение; комплектование; личный состав.*

ANALYSIS OF THE FUNCTIONING OF PERSONNEL PROVIDING SYSTEM DURING THE SPECIAL PERIOD IN 2014-2015

Mykola P. Dumenko (Candidate of Military Sciences)

General Staff of the Armed Forces of Ukraine, Kyiv, Ukraine

Article shows the main results of personnel bodies of personnel providing in 2014-2015 during transition to the special period. The author analyzed the main problems in a personnel providing system and highlighted the main ways of their solution. Analysis of the personnel of the Armed Forces of Ukraine during the special period in 2014-2015, shows that the main efforts were directed at maintaining an adequate level of staffing of combat units, saving human resources, improvement of the procedure of recruitment of troops (forces) trained personnel to ensure execution units combat missions in the area of the antiterrorist operation in the Donetsk and Lugansk regions. Compared with the period of the military organizations in peacetime states, could significantly increase the involvement of citizens for military service, primarily by simplifying contracting procedures, streamlining terms of military service, establish effective interaction with state authorities.

Keywords: *the special period; personnel providing; recruitment; personnel.*

References

1. The Law of Ukraine “On mobilization preparation and mobilization” of 21.10.1993 number 3543 / XII (amended), Kyiv, (1993). **2. The Law of Ukraine** “On Defense of Ukraine from 06.12.1991 number 1932” / XII (amended), Kuiv, (1991). **3. Hybrid war** in Ukraine, experts' opinions. [Hibrydna viina v Ukraini, dumky ekspertiv], (2014), Polonews. **4. Armed Forces Journal: Hybrid vs. compound war**, (2009). **5. Military people** in WWII. [Voennyie kadry v VOI], (1963), pod red. Dukacheva M.P. **6. Order** of the Minister of Defense of Ukraine of 05.04.2013 number 230 “On organization of the redeployment of military units of the Armed Forces of Ukraine in the Autonomous Republic of Crimea and Sevastopol”. **7. Order of the President of**

Ukraine of 01.05.2014 № 447/2014 “On measures to improve the defense of the State”. **8. The Law of Ukraine** “On social and legal protection of servicemen and their families”, VVR vid 20.12.1991 # 2012-XII (zi zminamy). **9. The joint directive** Defense Ministry and the General Staff of the Armed Forces of Ukraine from March 2, 2015 № D-1 “On the dismissal of soldiers who were called up for military service during the mobilization in times of crisis”. **10. Guidelines** on the order of dismissal of soldiers called up for military service during the mobilization in times of crisis, approved by the Chief of General Staff - Chief of the Armed Forces of Ukraine March 1, 2015. **11. Decree** of the President of Ukraine on May 6, 2015 № 254 “On discharge

from military service soldiers who were called up for military service during the mobilization, the special period in accordance with the Decree of the President of Ukraine on May 6, 2014 № 454” On partial mobilization”. **12. Decree of the President** of Ukraine on June 12, 2015 № 328 “On discharge from military service soldiers who were called up for military service during the mobilization in times of crisis”. **13. Decree of the President** of Ukraine on July 21, 2014 № 607 “On partial mobilization”. **14. Cabinet of Ministers of Ukraine** “On Amendments to the Cabinet of Ministers of Ukraine on June 12, 2013 № 413” “On approving the list of family circumstances or other valid reasons which may be the reason for the release from military service and servicemen of composition”. **15. The Law of Ukraine** “On Military Duty and Military Service” / BP Decision of 25.03.1992 number 2233-XII (as amended). **16. Law of Ukraine** “On the Labor Code of Ukraine” dated 10.12.1971 number 322-VIII (as amended). **17. Guidelines** on the specifics of contracts with citizens and military personnel taken for military service contract privates, sergeants and petty officers of the Armed Forces of Ukraine approved by the Chief of General Staff - Chief of

the Armed Forces of Ukraine of 12.09.2014 number 19563 / C. **18. Law of Ukraine** № 1275-IIV “On amendments to some legislative acts of Ukraine concerning improvement of defense mobilization during mobilization”, which came into force on 8 June 2014. **19. Recommendations** on the application of certain provisions of the Law of Ukraine “On Military Duty and Military Service”. **20. Law of Ukraine** of 20.05.14 number 1275-VII “On amendments to some legislative acts of Ukraine concerning improvement of defense mobilization during mobilization” (as amended). **21. Order of the Ministry of Defense** of Ukraine of 26.05.2014 number 333 “On approval of instructions of keeping the Armed Forces of Ukraine”. **22. The joint directive** Defense Ministry and the General Staff of the Armed Forces of Ukraine of 08.10.2014 number D-4 “On the order of admission to the disposal of certain categories of servicemen of Defense Ministry of Ukraine and the Armed Forces of Ukraine”. **23. Order of the Ministry of Defense** of Ukraine of 07.05.2015 number 200 “Regulations of the Ministry of Defense of Ukraine for consideration of materials on the recognition combatants”.

Отримано: 31.05.2016 року.

ПОРЯДОК ВИЗНАЧЕННЯ ОПТИМАЛЬНОГО КАЛЕНДАРНОГО СТРОКУ СЛУЖБИ ПЕРСПЕКТИВНИХ ЗРАЗКІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ З УРАХУВАННЯМ МОРАЛЬНОГО СТАРІННЯ

Життєвий цикл зразків озброєння та військової техніки (ОВТ) тісно пов'язаний з воєнно-технічною політикою (ВТП) держави щодо забезпечення військ необхідною кількістю сучасних зразків ОВТ. Напрями ВТП України, які пов'язані з показниками експлуатації та планового ремонту ОВТ, на сьогоднішній день є найбільш складними і найменш методично відпрацьованими. Складність проблеми проявляється насамперед у тому, що формування ВТП відбувається в умовах значних невизначеностей, які пов'язані, зокрема, з міжремонтними строками експлуатації, кількістю ремонтів, календарним строком служби зразків ОВТ з урахуванням морального старіння. В умовах прискореного розвитку ОВТ, зростання витрат на виготовлення, експлуатацію й ремонт більш сучасних зразків ОВТ, скорочення строків їх морального старіння все більш актуальним стає завдання обґрунтування строку служби зразків ОВТ, які перебувають на озброєнні Збройних Сил України. Вирішення цього завдання дозволить проводити своєчасне оновлення ОВТ у військах для підтримання їх боєздатності. Теоретичні напрацювання попередників щодо обґрунтування основних показників життєвого циклу зразків ОВТ не мали комплексного вирішення. У статті пропонується варіант проведення розрахунку оптимального календарного строку служби зразків ОВТ з урахуванням їх морального старіння.

Ключові слова: вартість; експлуатація; зразок; календарний строк служби; плановий ремонт.

Вступ

Постановка проблеми. Календарний строк служби T є основним показником, який характеризує довговічність зразка озброєння та військової техніки (ОВТ). Використання цього показника створює можливості щодо планування своєчасного забезпечення Збройних Сил сучасним озброєнням шляхом оновлення ОВТ, яке знаходиться у військах. На сьогоднішній день для багатьох зразків ОВТ календарний строк служби взагалі не призначається. Момент проведення планових ремонтів, списання при цьому визначається певною величиною пробігу (напрацювання) зразка ОВТ. Як засвідчили дослідження, доцільно для кожного із зразків призначати календарний строк служби (або одночасно і календарний строк служби, і вихід у плановий ремонт чи списання – за пробігом чи напрацюванням зразка) [1]. Календарний строк служби тісно пов'язаний з іншими показниками, які характеризують експлуатацію та планові ремонти зразка ОВТ, зокрема з такими, як міжремонтний строк експлуатації, тривалість планового ремонту, кількість планових ремонтів. Від названих показників залежить тривалість календарного строку служби зразка ОВТ, що очевидно.

Призначений календарний строк служби зразків ОВТ дозволяє планувати ремонт та оновлення ОВТ, розрахувати необхідні можливості ремонтних органів, кошти для проведення планових ремонтів і оновлення ОВТ.

Таким чином, визначення календарного строку служби зразків ОВТ є питанням актуальним.

Також важливим питанням, яке визначає боєздатність ОВТ військ, є узгодження календарного та морального строку служби зразків ОВТ.

Аналіз останніх досліджень і публікацій. Аналіз літератури, присвяченої розглядуваній галузі, свідчить про те, що питання щодо показників життєвого циклу зразків ОВТ досліджувалися і раніше [2-4].

Автори у [2] розглянули основні положення методичного апарату вирішення завдання розрахунку тривалості експлуатації (міжремонтних строків служби) технічних систем до виходу їх у плановий ремонт на прикладі радіоелектронних засобів (РЕЗ). Як показав проведений аналіз, наведений в [2] методичний апарат має певні недоліки:

велика кількість припущень, зокрема щодо лінійної залежності параметра потоку відмов від тривалості експлуатації на міжремонтному інтервалі;

для отримання значень деяких величин (параметрів) необхідні статистичні дані щодо виробництва, експлуатації та планових ремонтів РЕЗ. Зокрема, порядок визначення коефіцієнтів, які характеризують вплив профілактичних заходів на надійність РЕЗ, не пояснюється, що створює суттєві труднощі для практичного використання методичного апарату;

стосовно проведення планового ремонту РЕЗ як критерій прийняття рішення застосовується припустиме значення параметра потоку відмов РЕЗ, що викликає певні сумніви щодо коректності цього рішення, оскільки потік відмов може

залежати не тільки від технічного стану зразка ОВТ, а й від навченості обслуг тощо;

не враховується моральне старіння РЕЗ.

Питання довговічності зразків ОВТ досліджувалося в роботі [3] на прикладі озброєння військ ППО Сухопутних військ. Досліджувалися технічна довговічність, моральне старіння та економічні фактори. Недоліком наведеного у дослідженні методичного апарату є те, що його використання потребує наявності великого масиву статистичної інформації.

Як видно з наведеного, методичний апарат щодо визначення календарного строку служби зразків ОВТ потребує подальшого розвитку.

Тому метою статті є розгляд порядку розрахунку оптимального календарного строку служби зразка ОВТ з урахуванням його морального старіння та обмежень у коштах на розроблення, виробництво, експлуатацію та планові ремонти зразка ОВТ.

Виклад основного матеріалу дослідження

Коректне визначення календарного строку служби зразків ОВТ сприяє підвищенню боєздатності військ (сил), оскільки дає змогу провести планування оновлення ОВТ у військах, чим забезпечує укомплектування частин, підрозділів сучасними зразками ОВТ. У [4] запропоновано метод обґрунтування оптимальних значень календарного строку служби зразків ОВТ. Значення цього показника повинне бути розраховане ще до розроблення перспективних зразків ОВТ і виступати як вимога до зразка, який розробляється.

Розглянемо порядок проведення розрахунку оптимальних значень календарного строку служби перспективного зразка ОВТ. Як показано в [4], визначення календарного строку служби зразка ОВТ проводиться з використанням формули:

$$\alpha_e \cdot T^\alpha + \alpha_p \cdot T^\delta = \alpha_0, \quad (1)$$

$$\text{де } \alpha_e = \frac{C_e}{C_0}, \quad \alpha_p = \frac{C_p}{C_0} \leq 1;$$

$$C_{\text{відп}} \cdot T \cdot C' = Z_{\text{відп}} \cdot C' = C_{\text{відп}} \cdot T \cdot (C_0 - C_{\text{зал}}) = \alpha_0 \cdot C_0,$$

$$\text{звідки } \alpha_0 = \frac{C_{\text{відп}} \cdot T - C_0 + C_{\text{зал}}}{C_0} -$$

коефіцієнт, який враховує перебільшення над початковою вартістю зразка ОВТ C_0 сумарних коштів $Z_{\text{відп}} = C_{\text{відп}} \cdot T$, відпущених на виробництво, експлуатацію й ремонти зразка ОВТ протягом календарного строку служби;

$Z_{\text{відп}}$ – сумарні кошти, які відпускаються (плануються) на виробництво (закупівлю), експлуатацію, планові ремонти упродовж усього календарного строку служби T зразка ОВТ;

$C_{\text{відп}}$ – величина питомих (наприклад, середньорічних) коштів, які відпускаються (плануються) на виробництво (проекування, розробку, випробування), експлуатацію й плановий ремонт зразка ОВТ;

$C_{\text{зал}}$ – залишкова вартість зразка ОВТ у момент зняття його з експлуатації;

$C' = C_0 - C_{\text{зал}}$ – затрати, які можна назвати “корисними” з погляду використання зразка ОВТ за призначенням (безпосередні затрати на придбання зразка ОВТ за винятком його залишкової вартості $C_{\text{зал}}$);

C_0 – початкова вартість зразка ОВТ; $C_e = \alpha_e \cdot C_0$ – величина питомих (наприклад, середньорічних) затрат на утримання й експлуатацію зразка ОВТ за досвідом виробництва та експлуатації відповідних зразків ОВТ;

α_e – коефіцієнт середньорічних затрат на утримання й експлуатацію зразка ОВТ (розраховується відносно початкової вартості зразка ОВТ);

α – показник експлуатаційних затрат, обумовлений величиною відпрацьованого ресурсу, тривалістю експлуатації, інтенсивністю використання, умовами експлуатації зразка ОВТ.

За досвідом виробництва та експлуатації відповідних зразків ОВТ $\alpha \geq 1 - 2$; $C_p = \alpha_p \cdot C_0$ – величина питомих (наприклад, середньорічних) затрат (відрахувань) на плановий ремонт; α_p – коефіцієнт середньорічних затрат на плановий ремонт (розраховується відносно початкової вартості зразка ОВТ); $C_{\text{ві}i}$ – вартість i -го планового ремонту; $C_i = C_i(\Delta R_{i-1}) = C_{\text{зал}i}$ – залишкова вартість зразка ОВТ перед i -м плановим ремонтом; δ – показник, установлений дослідним шляхом у галузі ремонтно-відновлювальних робіт стосовно певного виду (групи, типу) ОВТ. За досвідом експлуатації та планових ремонтів відповідних зразків ОВТ $\delta > 1 - 3$, при цьому $\delta \geq \alpha$.

Рівняння (1) розв’язується чисельним способом відносно T .

Розраховані строки служби (в роках) зразків ОВТ без урахування морального старіння ($\gamma=1$) показані в табл. 1–3 залежно від відпущених коштів $Z_{\text{відп}} = C_{\text{відп}} \cdot T$ на придбання, експлуатацію та плановий ремонт зразка ОВТ – показника α_0 , показника $\alpha = 1,1$ експлуатаційних затрат, який визначається величиною відпрацьованого ресурсу, тривалістю експлуатації, інтенсивністю використання, умовами експлуатації зразка ОВТ та показника $\delta=1,4$ для ремонтно-відновлювальних робіт на зразках ОВТ (звичайно $\delta \geq \alpha$) [6] при

$$\alpha_0 = \frac{C_{\text{відп}} \cdot T - C_0 + C_{\text{зал}}}{C_0} = 6 \div 8.$$

Таблиця 1

Значення T (років) для ОВТ при $\alpha_0=6$; $\alpha=1,1$; $\delta=1,4$; ($\gamma=1$)

$\alpha_p \backslash \alpha_e$	0,1	0,2	0,3	0,4	0,5
0,1	14,3	11,5	9,6	8,3	7,2
0,2	9,7	8,4	7,4	6,6	6
0,3	7,5	6,8	6,1	5,6	5,1
0,4	6,3	5,8	5,3	4,9	4,6
0,5	5,4	5	4,7	4,4	4,1

Таблиця 2

Значення T (1) для ОВТ при $\alpha_0=7; \alpha=1,1; \delta=1,4;$
($\gamma=1$)

$\alpha_p \backslash \alpha_c$	0,1	0,2	0,3	0,4	0,5
0,1	16,1	13	10,9	9,4	8,2
0,2	10,8	9,4	8,3	7,5	6,8
0,3	8,5	7,6	6,9	6,3	5,8
0,4	7	6,5	6	5,5	5,1
0,5	6,1	5,7	5,3	4,9	4,6

Таблиця 3

Значення T (1) для ОВТ при $\alpha_0=8; \alpha=1,1; \delta=1,4;$
($\gamma=1$)

$\alpha_p \backslash \alpha_c$	0,1	0,2	0,3	0,4	0,5
0,1	17,8	14,5	12,2	10,5	9,2
0,2	12	10,5	9,3	8,3	7,5
0,3	9,3	8,4	7,7	7	6,5
0,4	7,8	7,1	6,6	6,1	5,7
0,5	6,7	6,2	5,8	5,5	5,2

Моральне старіння зразка ОВТ враховується завдяки формулі [4]:

$$\frac{K_{Vi} + K_{Ci} + K_{Pi}}{K_{Oi}} \leq \gamma \leq 1, \quad (2)$$

де $K_{Ci} = \frac{C_i}{C_0} = \frac{C_{зал i}}{C_0}$ – коефіцієнт залишкової

вартості перед і-м плановим ремонтом зразка ОВТ;

$$K_{Oi} = \frac{R(t_{pi})}{R_0} \text{ – коефіцієнт відновлення}$$

технічного ресурсу (коефіцієнт вартості відновленого технічного ресурсу) за рахунок (після) проведення на ньому і-го планового ремонту (дорівнює 0,4÷0,6);

$$K_{Vi} = \frac{C_{Vi}}{C_0} \text{ – коефіцієнт вартості і-го}$$

планового ремонту зразка ОВТ;

$$K_{Pi} = \frac{t_{pi} \cdot (K_{Ci} + K_{Vi})}{t_{ei} + t_{pi}} \text{ – коефіцієнт}$$

врат за час простою зразка ОВТ упродовж перебування його в і-му плановому ремонті; $R(t_{pi})$ – величина ресурсу зразка ОВТ після проведення і-го планового ремонту; R_0 – початкова величина ресурсу зразка ОВТ; t_{pi} – час підготовки й проведення (тривалість) і-го планового ремонту; t_{ei} – міжремонтний строк експлуатації після і-го планового ремонту.

Наприклад, при $K_{Pi}=0,03, K_{Oi}=0,9$ та різних K_{Ci}, K_{Vi} з урахуванням, що $K_{Vi} \leq K_{Oi} - K_{Ci}$ при $K_{Oi} \geq K_{Ci}$ [5], значення коефіцієнта

$$\gamma = \frac{K_{Vi} + K_{Ci} + K_{Pi}}{K_{Oi}} \text{ морального } T_m \text{ і календарного}$$

T строків служби зразка ОВТ наведені в табл. 4

Таблиця 4

Значення γ для ОВТ при $K_{Pi}=0,03, K_{Oi}=0,8$ (за умови, що $K_{Vi} \leq K_{Oi} \cdot \gamma - (K_{Ci} + K_{Pi}), K_{Oi} \cdot \gamma \geq K_{Ci} + K_{Pi}$)

$K_{Ci} \backslash K_{Vi}$	0,1	0,15	0,20	0,25	0,30
0,1	0,26	0,31	0,37	0,42	0,48
0,2	0,37	0,42	0,48	0,53	0,59
0,3	0,48	0,53	0,59	0,64	0,70
0,4	0,59	0,64	0,70	0,76	0,81

Прийmemo, що моральний строк служби зразка ОВТ (в роках) з урахуванням табл. 1-3 обчислюється таким чином:

$$T_M = T \cdot \frac{R_M}{R_0} = T \cdot \gamma, \quad (3)$$

де R_M – технічний ресурс, що може бути витрачений протягом морального строку служби зразка ОВТ.

Запишемо рівняння (1) у вигляді:

$$\alpha_e \cdot T^\alpha + \alpha_p \cdot T^\delta - \alpha_0 = 0. \quad (4)$$

Знайдемо з цього рівняння значення T.

Для прикладу візьмемо такі значення вихідних даних:

$\alpha = 1,1; \delta = 1,4; C_0 = 7,2$ млн грн;

$C_e = 0,72$ млн грн;

$C_p = 1,846$ млн грн;

$\alpha_0 = 5,$

$\gamma = 0,8.$

Проведемо розрахунки:

$$\alpha_e = \frac{C_e}{C_0} = 0,1; \alpha_p = \frac{C_p}{C_0} = 0,26.$$

Підставляючи у формулу (4) вихідні дані та значення α_e, α_p проводимо розрахунки.

У розглядуваному випадку $T = 7,2$ роки.

З урахуванням морального старіння:

$$T_M = T \cdot \gamma = 5,76 \text{ року.}$$

Висновки й перспективи подальших досліджень

1. Календарний строк служби зразка ОВТ, як показують дослідження, пов'язаний із кількістю виділених коштів на його експлуатацію та планові ремонти.

2. Наведені розрахунки свідчать, що зі збільшенням (зменшенням) α_0 , тобто коштів, що відпускаються на експлуатацію й планові ремонти зразка ОВТ, можлива тривалість календарного строку служби T цього зразка зростає (зменшується). З другого боку, за заданого значення α_0 зі збільшенням (зменшенням) C_e, C_p календарний строк служби T зразка ОВТ зменшується (збільшується).

3. Коректність розрахованих величин календарного строку служби зразків ОВТ значною мірою залежить від правильного вибору вихідних даних для проведення розрахунків.

Перспективами подальших досліджень є проведення розрахунків оптимальних значень інших показників життєвого циклу зразка ОВТ.

Література

1. Костенко Ю. П. Танки (тактика, техніка, економіка) [Текст] / Ю. П. Костенко. – М.: НТЦ “Інформтехніка”, 1992, – 68 с. 2. Ковтуненко А. П. Основы анализа сложных технических систем. Теория и приложения [Текст] : монография / А. П. Ковтуненко, В. В. Зубарев. – К.: ЦНД ОВТ ЗСУ, СПД Богданов В.О., 2009. – 496 с. 3. Крыжний А. В. Основы решения проблемы долговечности вооружения войск ПВО Сухопутных войск [Текст] : дис. докт. техн. наук : 20.02.14 / Крыжний Аркадий Владимирович. – К., 1994. – 310 с. 4. Закусило П. С. Метод обгрунтування календарного строку служби зразків озброєння та військової техніки з урахуванням їхнього морального старіння [Текст] / П. С. Закусило, В. П. Харченко // Зб. наук. пр. ЦНД ЗС України. – К., 2014. – №3 (69). – С. 110-119. 5. Шуенкин В. А. Обоснование показателей безотказности, долговечности, эксплуатации и целесообразности проведения планового ремонта и модернизации образцов вооружения и военной техники [Текст] : учебное пособие. / В. А. Шуенкин. – К.: ЦНИИ ВС Украины, 2012. – 432 с.

ПОРЯДОК ОПРЕДЕЛЕНИЯ ОПТИМАЛЬНОГО КАЛЕНДАРНОГО СРОКА СЛУЖБЫ ПЕРСПЕКТИВНЫХ ОБРАЗЦОВ ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ С УЧЕТОМ МОРАЛЬНОГО СТАРЕНИЯ

Петр Степанович Закусило (канд. воен. наук, с.н.с.)

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

Жизненный цикл образцов вооружения и военной техники (ВВТ) тесно связан с военно-технической политикой (ВТП) государства касательно обеспечения войск необходимым количеством современных образцов ВВТ. Направления ВТП Украины, которые связаны с показателями эксплуатации и планового ремонта ВВТ, на сегодняшний день есть наиболее сложным и наименее методично отработанными. Сложность проблемы проявляется прежде всего в том, что формирование ВТП осуществляется в условиях значительных неопределенностей, которые связаны, в частности, с межремонтными сроками эксплуатации, количеством ремонтов, календарным сроком службы образца ВВТ с учетом морального старения. В условиях ускоренного развития ВВТ, роста расходов на изготовление, эксплуатацию и ремонт более современных образцов ВВТ, сокращения сроков их морального старения все более актуальным становится задание обоснования срока службы образцов ВВТ, которые находятся на вооружении Вооруженных Сил Украины. Решение этого задания позволит проводить своевременное обновление ВВТ у войсках для поддержания их боеспособности. Теоретические наработки предшественников касательно обоснования основных показателей жизненного цикла образцов ВВТ не имели комплексного решения. В статье предлагается вариант проведения расчета оптимального календарного срока службы образцов ВВТ с учетом их морального старения.

Ключевые слова: стоимость; эксплуатация; образец; календарный срок службы; плановый ремонт.

PROCEDURE FOR DETERMINING OPTIMAL POLICY CALENDAR LIFETIME OF WEAPONS AND MILITARY EQUIPMENT WITH OBSOLESCENCE

Petro S. Zakusylo (Candidate of Military Sciences, Senior Research Fellow)

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

The life cycle of weapons and military equipment (WME) is closely associated with the military-technical policy (MTP) on state support for the troops necessary number of modern WME samples. Directions MTP of Ukraine, which are associated with indicators of operation and scheduled maintenance WME is the most complicated and least methodically exhaust today. The complexity of the problem manifests itself primarily in the fact that the formation of the MTP carried out in conditions of considerable uncertainty, which are connected, in particular, with the turnaround time of operation, the number of repairs, the calendar service life of WME sample taking into account obsolescence. In the context of the accelerated development of WME, increasing costs for manufacturing, maintenance and repair of more modern WME samples, shortening their obsolescence is becoming increasingly important task substantiate lifetime WME models that are in service with the Armed Forces of Ukraine. The solution of this task will allow for the timely WME do updates from the troops to maintain their combat capability.

Theoretical developments predecessors regarding justification main indicators WME samples lifecycle solutions were not integrated.

The article offers an option of calculating the optimal calendar life of WME models with regard to their obsolescence.

Keywords: cost; maintenance; sample; calendar service life; routine repairs.

References

1. Костенко Ю. П. (1992), Tanks (tactics, technique, economy). [Tanki (taktika, tekhnika, ekonomika)], Moscow: "Informtehnika" 68 p. 2. Kovtunen A.P., Zubarev V.V. (2009), Fundamentals of analysis of complex technical systems. Theory and applications. [Osnovy analiza slozhnykh tekhnicheskikh sistem]: monograph, Kyiv: CRI WME AFU, SPD Bogdanov V.O., 496 p. 3. Kryzhny A.V. (1994), Basics weapons durability problems of air defense troops of the Land Forces. [Osnovy reshenia problemy dolgovechnosti vooruzhenia voisk PVO Sukhoputnykh voisk]: dis. Doctor. tehn. Sciences: 20.02.14, Kyiv, 310 p. 4. Zakusylo P.S., Kharchenko V.P. (2014), Method of substantiate calendar lifetime service sample weapons and military equipment with obsolescence. [Metod obgruntuвання kalendarного строку sluzhby zrazkiv ozbroєnnia ta viiskovoi tekhniki z urakhuvanniam yikhnoho moralnoho starinnia], CRI Armed Forces of Ukraine, Kyiv, No.3 (69), pp. 110-119. 5. Shuenkin V.A. (2012), Substantiation of reliability indicators, durability, operation and feasibility of carrying out scheduled maintenance and modernization of weapons and military technology. [Obosnovanie pokazatelei bezotkaznosti, dolgovechnosti, ekspluatatsii i tselesoobraznosti provedeniia planovogo remonta i modernizatsii obratstov vooruzheniia i voennoi tekhniki]: a tutorial, Kyiv: CRI Armed Forces of Ukraine, 432 p.

Отримано: 24.05.2016 року.

Олександр Васильович Майстренко (канд. військ. наук)

Національний університет оборони України імені Івана Черняхівського, Київ, Україна

ОБҐРУНТУВАННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗОНАЛЬНОГО РОЗПОДІЛУ ЗАСОБІВ ВОГНЕВОГО ВПЛИВУ ТА ОБ'ЄКТІВ ДЛЯ УРАЖЕННЯ

У статті обґрунтовано рекомендації щодо зонального розподілу засобів вогневого впливу та об'єктів для ураження, що спираються на визначення кількості засобів вогневого ураження противника, приведені до кількості уражених об'єктів за віддаленням від лінії бойового зіткнення, та проведено подальшу їх градацію за допомогою правила золотого зрізу за ознакою дальності стрільби (пусків ракет).

Впровадження означених рекомендацій у практику організації бойового застосування військових формувань під час вогневого ураження противника дасть змогу поліпшити управління військовими формуваннями ракетних військ і артилерії, планувати означене застосування відповідно до функціональних можливостей військового формування, скоротити час для розроблення та віддачі розпоряджень у разі необхідності застосування військового формування не відповідно до плану, забезпечити достатню інтенсивність обробки інформації та віддання розпоряджень у неklasичних способах застосування військового формування, що в цілому може підвищити ступінь реалізації можливостей військового формування.

Ключові слова: *вогневе ураження; військові формування; можливості; зональний розподіл.*

Вступ

Постановка проблеми. Загальна тенденція до збільшення кількості високотехнологічних засобів так званого дальнього вогневого ураження противника (ВУП), застосовуваних у воєнному конфлікті [1], зумовлює необхідність зміни підходів до їх застосування. Звичайно, певні удосконалення є і досить широко застосовуються під час організації ВУП, наприклад зонально-об'єктовий та вибірково-об'єктовий методи ВУП [2]. Однак у цілому, як свідчить аналіз результатів бойового застосування військових формувань (ВФ) в останніх воєнних конфліктах [3], зокрема в зоні проведення Антитерористичної операції на сході України (АТО) [4], досить часто можливості сил і засобів дальнього ВУП, у тому числі ракетних військ і артилерії (РВіА) залишаються реалізованими не повною мірою або їх виявилось недостатньо.

Результати аналізу бойового застосування ВФ РВіА як одного з основних елементів дальнього ВУП в останніх воєнних конфліктах показують, що можливості РВіА визначають відповідно до організаційної належності та організаційного рівня підпорядкованості певного ВФ РВіА [2-4]. Означене обумовлене тим, що за існуючими методиками [2-4] бойовий потенціал мають лише ВФ механізованих і танкових військ, а ВФ РВіА розподіляються відповідно до їх потреби. Такий підхід певним чином відображає рівень можливостей ВФ, однак інколи їх можливості на організаційному рівні не відповідають функціональним, тобто рівень реальних можливостей відрізняється від спланованого або визначеного рівня.

У цілому проблема визначення можливостей ВФ РВіА полягає у відсутності достатньо простої і точної ознаки, за якою можна розподілити можливості ВФ РВіА та спланувати їх реалізацію. У цьому разі планування пропонується здійснювати залежно від функціональних можливостей ВФ, а не відповідно до організаційного об'єднання.

До того ж під час управління ВФ у ході бойового застосування доволі часто витрачається значний час для розроблення та віддання розпоряджень у разі необхідності застосування ВФ не відповідно до плану, що в цілому призводить до зниження можливостей ВФ через їх нереалізованість [3-4]. Інтенсивність видачі розпоряджень підсистемою управління зменшується і призводить до зниження інтенсивності виконання завдань підсистемою вогневого впливу, що в цілому знижує продуктивність вогневого впливу за сталих потенційних можливостей підсистеми вогневого впливу.

Аналіз останніх досліджень і публікацій [5-7] показує, що основні зусилля дослідників були спрямовані на пошук досконаліших методів визначення величин показників можливостей ВФ, причому визначення можливостей проводилося для організаційних структур (штатних підрозділів, частин або угруповань) а обсягу завдань – відповідно до фактичних можливостей противника. До того ж під час розподілу обсягу завдань між штатними підрозділами недостатньо враховуються їх місцезположення, що спричиняє істотні розбіжності між результатами планування реалізації можливостей РВіА щодо ВУП і

фактичним результатом ВУП. Також означена проблема істотно впливає на управління ВФ під час бойового застосування, особливо якщо ВФ потрібно застосовувати не за планом.

Також існуючі дослідження переважно базуються на дослідженні так званих класичних способів застосування ВФ: оборонного, наступального бою, рейдових дій тощо [5-7], а у разі застосування неklasичних способів – із поправочними коефіцієнтами, точність і достовірність яких без проведення статистичного дослідження набору натурних даних є сумнівною. Як показує аналіз останніх збройних конфліктів, частка класичних способів застосування ВФ значно зменшується [3-4].

У дослідженнях доволі часто співвідношення можливостей сторін визначають без урахування особливостей засобів вогневого впливу (наприклад дальності стрільби), що не дає змоги повною мірою реалізувати можливості ВФ щодо ВУП [3-4].

На думку автора, однією з ознак за якими можна визначити і розподілити можливості ВФ щодо ВУП, є віддалення засобів вогневого впливу та об'єктів для ураження від лінії бойового зіткнення, що через урахування максимальної дальності стрільби артилерії (пусків ракет) дасть змогу враховувати особливості засобів ВУП під час управління ВФ РВіА, особливо в екстремальних умовах. Звичайно, визначення можливостей ВФ РВіА залежно від дальності стрільби і пусків ракет потребує відповідного зонального розподілу засобів вогневого впливу та об'єктів для ураження.

Мета статті. Отже, метою статті є обґрунтування рекомендацій щодо зонального розподілу засобів вогневого впливу та об'єктів для ураження з метою поліпшення управління ВФ РВіА, особливо в екстремальних умовах.

Викладення основного матеріалу дослідження

Відстань від засобу вогневого впливу до об'єкта ураження відіграє ключову роль під час ВУП. Так, чим більша відстань досяжності засобів вогневого впливу, тим більші похибки внаслідок розсіювання та підготовки стрільби [5-7], відповідно менша імовірність ураження об'єкта і, як наслідок, менша продуктивність, а у разі недосяжності засобів вогневого впливу продуктивність дорівнює 0.

В існуючих підходах [5-7] відстань від засобу вогневого впливу до об'єкта ураження враховується, однак, як правило, під час оцінювання ефективності виконання одного вогневого завдання, а інколи – детального планування вогню артилерії. Причому основний акцент зроблено на організаційній належності засобу вогневого впливу і його потенційній спроможності уразити деяку кількість об'єктів противника. Однак практика бойового застосування ВФ РВіА показує, що потенційні спроможності засобів вогневого впливу досить

часто залишаються недостатньо реалізованими через недосяжність або досить велику відстань до об'єктів ураження.

Таким чином, дальність стрільби (пусків ракет) може слугувати ознакою, за якою можливо визначити та розподіляти можливості ВФ, у тому числі РВіА. Звичайно, використання дальності без певного градування, зумовлене значними змінами у можливостях ВФ, є достатньо складним процесом і може призвести до великої кількості помилок. Отже, градування відстаней від засобу вогневого впливу до об'єкта ураження пропонується проводити врахуванням параметрів, які визначатимуть можливості РВіА, а також вибрати критерій (критерії) поділу означених відстаней.

Як додаткові параметри, які визначатимуть можливості РВіА на певній відстані, пропонується використати кількість вогневих засобів, які досягають цілі стрільбою (пуском), та їх питому потужність (з урахуванням потужності одного снаряда (ракети), інтенсивності та імовірності виконання завдань).

За критерій поділу означених відстаней пропонується обрати правило золотого зрізу, отримане з послідовності Фібоначчі [8], яке певним чином підтверджене використанням у відомих дослідженнях та практиці бойового застосування ВФ РВіА.

Для подальшого дослідження пропонується розглянути певну сукупність існуючих на озброєнні ЗС України засобів вогневого впливу табл.1 та рис.1.

Таблиця 1

Таблиця максимальної дальності стрільби та кількості засобів РВіА (приклад)

Система, індекс, шифр	Макс. дальність стрільби, км	Кількість засобів РВіА, од.
9К79М1 "Точка-У"	120	1
9К51 "Град"	20,4	22
9К57 "Ураган"	35,8	10
9К58 "Смерч"	70	2
122-мм гаубиця Д-30	15,3 (ОФ-24)	8
152-мм гаубиця 2А65 "Мста-Б"	28 (ОФ-61)	18
152-мм гармата 2А3 "Гіацинт-Б"	32,8 (ОФ-30)	1
122-мм гаубиця 2С1 "Гвоздика"	15,2 (ОФ-24)	27
152-мм самохідна гаубиця 2С3 "Акація"	17,3 (ОФ-25); 20,3(ОФ-22)	15
152-мм самохідна гаубиця 2С19 Мста-С"	24 (ОФ-45); 28,5 (ОФ-61)	4
152-мм самохідна гармата 2С5 "Гіацинт-С"	28,3 (ОФ-29); 32,8 (ОФ-30)	3
82-мм БМ-37	3	6
82-мм АМ 2Б9 Васильок"	4,3	7
120-мм ПМ38	5,7	3
120-мм 2С12 "Сані"	7,1 (ОФ-34)	24
100-мм протитанкова гармата МТ 12	8,2	13
ПТРК "Конкурс"	4(9М113)	4
ПТРК "Штурм-С"	5	2

На підставі даних табл. 1 пропонується розглянути графічне відображення дальності стрільби систем РВіА та щільність розподілу типів засобів РВіА за дальністю стрільби (пусків) (рис.1).

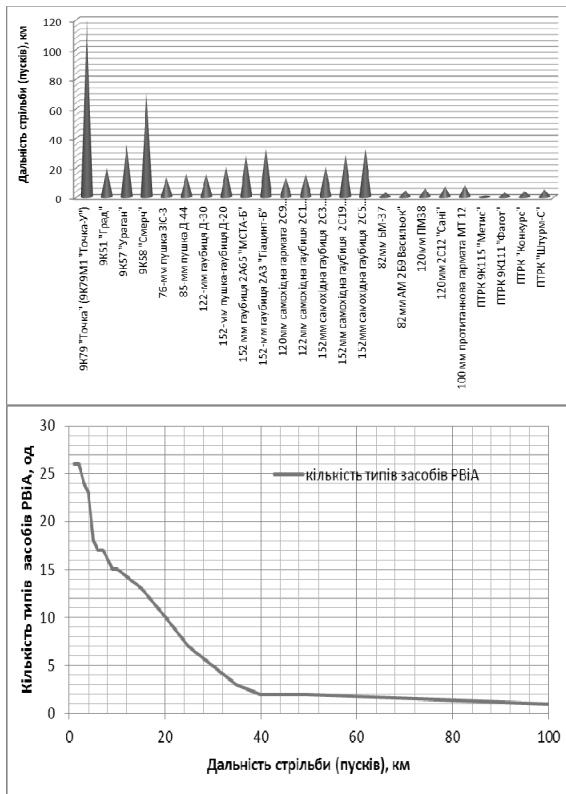


Рис. 1. Діаграма дальності стрільби пусків та графік щільності розподілу типів засобів РВіА за дальністю стрільби (пусків)

Результати аналізу табл. 1 та рис. 1 показують, що за дальністю стрільби артилерії (пусків ракет) можна виділити три характерні ділянки – 0...5 км, 5...35 км та 35...120 км. Однак для точнішого градування можливостей пропонується ураховувати відносну кількість засобів вогневого впливу (табл. 1, рис. 2), наприклад відносно ракетного комплексу 9К79.

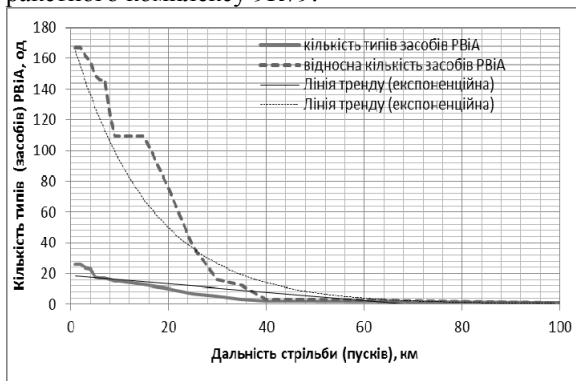


Рис. 2. Графік щільності розподілу типів засобів РВіА та їх кількості за дальністю стрільби (пусків)

Результати аналізу рис. 2 показують, що графік залежності дещо змінює форму, причому виявити яскраво виражені ділянки достатньо важко. Звичайно із застосуванням певних правил (критеріїв), зокрема золотого зрізу, можна градувати дальність стрільби. Однак доцільнішим є використання такого параметру, як віддалення від лінії бойового зіткнення, що дасть

зможу враховувати за допомогою одного показника можливості і своїх засобів вогневого впливу, і противника. Для цього пропонується застосувати такий показник, як кількість об'єктів для ураження. Так, відповідно до узагальнених результатів аналізу останніх збройних конфліктів [3-4] було проведено розподіл об'єктів для ураження залежно від їх віддалення від лінії бойового зіткнення (табл. 2), щільність розподілу ураження зазначено на рис. 3.

Таблиця 2

Кількість об'єктів для ураження та щільність їх розподілу разом із засобами РВіА за віддаленням від лінії бойового зіткнення (Приклад)

Відстань від лінії бойового зіткнення, км	Кількість об'єктів для ураження, од	Щільність розподілу об'єктів для ураження та засобів РВіА (табл. 1), од
До 1	120	287,25
Від 1 до 2	30	197,25
Від 2 до 3	20	181,75
Від 3 до 4	15	172,75
Від 4 до 5	11	160
Від 5 до 6	10	156
Від 6 до 7	9	155
Від 7 до 8	8	130,25
Від 8 до 9	7	116,5
Від 9 до 10	5	114,5
Від 10 до 15	4	113,5
Від 15 до 20	4	78,75
Від 20 до 25	3	41
Від 25 до 30	3	19,25
Від 30 до 35	2	14,5
Від 35 до 40	2	5
Від 40 до 50	1	4
Від 50 до 100	1	2

Аналіз табл. 2 та рис. 3 показує, що урахування дальності стрільби (пусків) дасть змогу точніше визначати зони розподілу можливостей засобів ВУП. Під час урахування дальності стрільби (пусків) обов'язково потрібно зважати на віддалення засобів ВУП від лінії бойового зіткнення.

Таким чином, використовуючи кількість засобів ВУП, приведену до кількості уражених об'єктів за віддаленням від лінії бойового зіткнення можна провести градацію за допомогою правила золотого зрізу [8]:

$$L_{зони} = L(N_{поч}^{(пр)} \cdot 0,63), \quad (1)$$

де $L_{зони}$ – межа зони реалізації можливостей засобів ВУП, км;

$N_{поч}^{(пр)}$ – кількість засобів ВУП, приведена до кількості уражених об'єктів за віддаленням від лінії бойового зіткнення, од.;

0,63 – значення золотого зрізу, отримане з послідовності Фібоначчі.

Загалом порядок визначення межі зони можна описати таким чином: від початкового значення кількості засобів ВУП, приведеної до кількості об'єктів для ураження за віддаленням від лінії бойового зіткнення (0 км), визначити наступне його значення множенням на значення золотого зрізу з послідовності Фібоначчі. Далі через

визначення відповідної точки на графіку залежності пропонується обчислювати відповідне значення дальності та приймати його як межу відповідної зони (рис. 3).



Рис. 3. Графік залежності кількості об'єктів для ураження та засобів РВіА від дальності їх розташування від лінії бойового зіткнення та порядку визначення зони за допомогою послідовності Фібоначчі (правила золотого зрізу)

Застосування означеного підходу (1), (рис. 3) дає змогу визначити відповідні межі зон реалізації можливостей засобів ВУП для прийнятих у межах дослідження умов (рис. 4). До того ж для якіснішого сприйняття отриманих результатів пропонується візуально зони розподіляти за кольорами, адже в деяких арміях світу [3], а також деяких ВФ ЗС України в зоні АТО [4] існує градація без визначення точних меж означених зон, що ускладнює їх застосування. Пропонується використовувати таке позначення зон: від 0 до 2 км – червона, від 2 до 8 км – жовта, від 8 до 20 км – зелена та від 20 до 100 км – сіра (рис. 4).

На рис. 4 зображені різні варіанти визначення зон, що в цілому можуть використовуватися комплексно. Так, на рис. 4а зображено зони реалізації можливостей засобів вогневого ураження наших військ, на рис. 4б – зони реалізації можливостей засобів ВУП.

Висновки й перспективи подальших досліджень

Отже, у статті обґрунтовано рекомендації щодо зонального розподілу засобів вогневого впливу та об'єктів для ураження, що спираються на визначення кількості засобів ВУП, приведеної до кількості уражених об'єктів за віддаленням від лінії бойового зіткнення, та проведено подальшу їх градацію за допомогою правила золотого зрізу за ознакою дальності стрільби (пусків ракет). Впровадження означених рекомендацій у практику організації бойового застосування ВФ під час ВУП може сприяти поліпшенню управління ВФ РВіА, плануванню означеного застосування відповідно до функціональних можливостей ВФ, скороченню часу для розроблення та віддання розпоряджень у разі необхідності застосування ВФ не відповідно

до плану, забезпеченню достатньої інтенсивності обробки інформації та відданню розпоряджень у неklasичних способах застосування ВФ, що в цілому може підвищити ступінь реалізації можливостей ВФ.

Подальші дослідження пропонується присвятити розробленню та обґрунтуванню рекомендацій щодо визначення необхідних та достатніх віддалень розміщення засобів вогневого ураження від лінії бойового зіткнення і доцільного цілерозподілу об'єктів для ураження між засобами вогневого впливу.

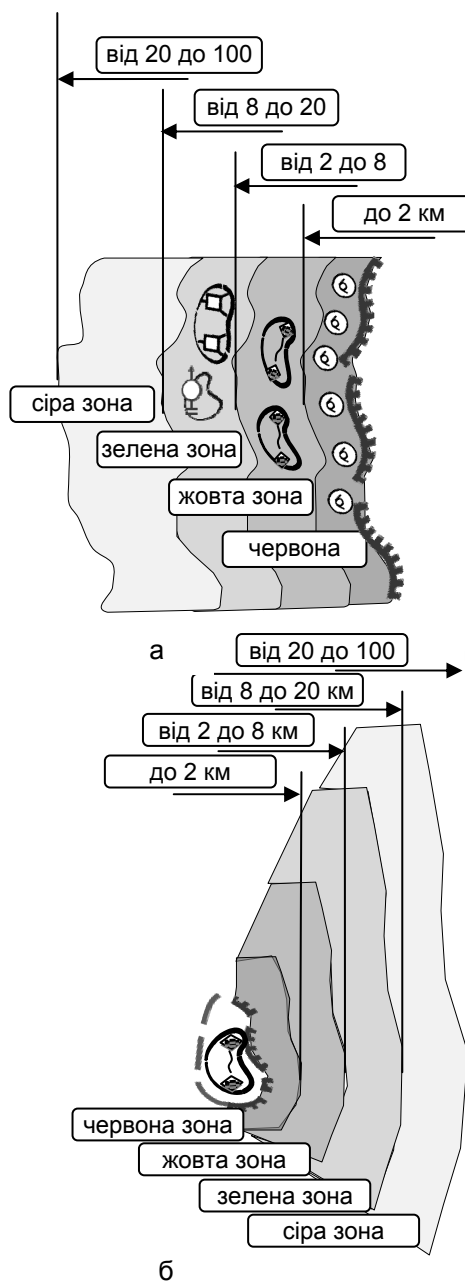


Рис. 4. Зони та їх межі для реалізації можливостей засобів ВУП із відповідною кольоровою візуалізацією

Література

1. **Матеріали** доповідей науково-практичного семінару кафедри РВіА “Перспективи бойового застосування ракетних військ і артилерії ЗС України” (Львів, АСВ, 17 грудня 2015 р.) 112 с. 2. **Матеріали** доповідей науково-технічної конференції “Перспективи розвитку ракетних військ і артилерії ЗС України” (Львів, АСВ, 5–6 листопада 2014 р.) 204 с. 3. **Розвиток** тактики родів військ Сухопутних військ за досвідом локальних війн і збройних конфліктів сучасності: матеріали наук.-практ. конф. (Київ 17 грудня 2009 р.) / Каф. СВ НАОУ. – К.: НАОУ, 2009. – С. 80-86. 4. **Збірник** матеріалів доповідей науково-практичного семінару “Сучасний стан сил спеціальних операцій,

проблемні питання та шляхи вирішення”. (Київ, НУОУ, 22 грудня 2015 р.) К.: НУОУ, 2015. – 167 с. 5. **Бобриков А.** Оценка эффективности огневого поражения ударами ракет и огнем артиллерии / А. Бобриков – СПб.: Галея Принт, 2006. – 424 с. 6. **Ефимов Н. Е.** Системный подход к решению проблемы планирования огневого поражения противника в операциях / Н.Е. Ефимов // Военная мысль. – 1995. – № 6. – С. 51–54. 7. **Фесенко Ю. Н.** Об особенностях огневого поражения группировок войск / Ю. Н. Фесенко // Военная мысль. – 2000. – № 5. – С. 57-65. 8. **Кеплер И. О.** шестиугольных снежинках / И. Кеплер – М.: Наука, 1982. – 194 с.

ОБОСНОВАНИЕ РЕКОМЕНДАЦИЙ ОТНОСИТЕЛЬНО ЗОНАЛЬНОГО РАСПРЕДЕЛЕНИЯ СРЕДСТВ ОГНЕВОГО ПОРАЖЕНИЯ ПРОТИВНИКА И ОБЪЕКТОВ ДЛЯ ПОРАЖЕНИЯ

Александр Васильевич Майстренко (канд. воен. наук)

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье обоснованы рекомендации относительно зонального распределения средств огневого поражения и объектов для поражения. Отмеченные рекомендации основываются на определении количества средств огневого поражения противника, приведенного к количеству пораженных объектов по расстоянию от линии боевого столкновения, и последующей их градации с помощью правила золотого среза по признаку дальности стрельбы (пусков ракет).

Внедрение отмеченных рекомендаций в практику организации боевого применения воинских формирований во время огневого поражения противника позволит осуществлять планирование огневого поражения в соответствии с функциональными возможностями воинского формирования, сократить время для разработки и отдачи распоряжений в случае необходимости применения воинского формирования не в соответствии с планом, обеспечить достаточную интенсивность обработки информации и отдачи распоряжений в неклассических способах применения воинского формирования, что в целом повысит степень реализации возможностей воинского формирования.

Ключевые слова: огневое поражение; воинское формирование; возможности; зональное распределение.

GROUND OF RECOMMENDATIONS IN RELATION TO ZONALITY OF FACILITIES OF FIRE DEFEAT OF OPPONENT AND OBJECTS FOR DEFEAT

Oleksandr V. Maistrenko (Candidate of Military Sciences)

National Defense University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine

In the article proved recommendations for the zonal distribution fire weapons and sites for defeating. Reported guidelines are based on the determination of number of funds destruction by fire, reduced to the number of infected objects by the distance from the line of clash and the their further gradation by using regulations of the gold cutting on the basis effective range (missile launch).

Implementation of the selected recommendations at practice of providing combat use of military units during the fire destruction of the enemy will allow for the planning of fire damage in accordance with the functionality of the military unit, reduce the time to develop and the impact of orders in case of the need for military formation not according to plan provide sufficient intensity and efficiency of information processing orders at non-classical methods of using military unit, which generally increase the degree of realization of military formation opportunities.

Keywords: fire defeat; military forming; possibilities; zonality.

References

1. **Materials** of lectures of scien.-pract. seminar of department of RTaA of “Prospect of battle application of rocket troops and artillery of Army of Ukraine” (2015). [Materiali dopovidei naukovopractichnogo seminaru kafedri RViA “Perspektivi boivogo zastosuvannia raketnih viisk I artilerii ZS Ukraini”], Lviv: ASV, 112 p. 2. **Materials** of lectures of scientific and technical conference of “Prospect of development of rocket troops and artillery of Army of Ukraine”. (2014). [Materiali dopovidei naukovotekhnichnoi konferencii “Perspektivi rozvitku raketnih viisk I artilerii ZS Ukraini”], Lviv: ASV, 204 p. 3. **Development** of tactic of births of troops of Ground forces after experience of local wars and armed conflicts of contemporaneity materials of scien.-pract. conferences (2009) [Rozvitok taktiki rodiv viisk Suhoputnih viisk za dosvidom lokalnih viin I zbroynih kofliktiv suchasnosti], Materiali naukovopractichnoi konferencii, Kiev: NAOU, 213 p. 4. **Collection** of materials of lectures of scien.-pract. seminar is the “Modern state of forces of the special operations, problem

questions and ways of decision”. (2015) [Zbirnik materialiv dopovidei naukovopractichnogo seminaru “Suchasni stan sil specialnih operacii, problemni pitannia ta shliahi ih virishinnia”], Kiev: NUOU, 22.12., 167 p. 5. **Bobrikov A.** (2006) Estimation to efficiency of fire defeat the shots of rockets and fire of artillery. [Ocenka effektivnosti ogneвого porazhenia udarami raket I ognem artilerii], Saint Petersburg: Galeya Print, 424 p. 6. **Efimov N.E.** (1995) Approach of Systems to the decision of problem of planning of fire defeat of opponent in operations. [Sistemni podhod k resheniyu problemi planirovania ogneвого porazhenia protivnika v operaciah] The Military Idea, No.6, pp. 51-54. 7. **Fesenko Yu.N.** (2000) About the features of fire defeat of groupments of troops. [Ob osobenostiah ogneвого porazhenia grupirovok voisk], The Military Idea, No.5, pp. 57-65. 8. **Kepler Iogan** (1982) About hexagonal snowflakes, [O shestiuholnih snezhinkah], Moscow: Science, 194 p.

Отримано: 24.05.2016 року.

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.

На сторінках журналу розглядаються такі питання:

1. Теоретичні основи та інструментальні засоби створення і використання інформаційних технологій у сфері безпеки та оборони.

2. Критерії оцінювання і методи забезпечення якості, надійності, живучості інформаційних технологій і систем.

3. Принципи оптимізації, моделі та методи прийняття рішень при створенні автоматизованих систем різноманітного призначення у сфері безпеки і оборони.

4. Дослідження закономірностей побудови інформаційних комунікацій та розроблення теоретичних засад побудови і впровадження інтелектуальних інформаційних технологій для створення новітніх систем накопичування, переробки, збереження інформації та систем управління у сфері безпеки та оборони.

5. Інтерактивні моделі розвитку науково-освітнього простору у сфері безпеки та оборони.

6. Збереження, розвиток і трансформація культурно-мовної спадщини в інтерактивному дискурсі у контексті інформаційної безпеки держави.

7. Глобалізація, полілогічність та інтерактивність як філософське підґрунтя розвитку інформаційних технологій у сфері безпеки та оборони.

8. Інтелектуальні освітні інформаційні технології у сфері безпеки та оборони. Проблеми сумісності і взаємодії технологій навчання.

9. Сучасні підходи до проектування розподілених інтелектуальних систем для освіти і науки.

10. Військово-теоретичні проблеми.

Схема оформлення статей

УДК (*Arial*, кегль – 11 пт.)

Анатолій Анатолійович Іванов (д-р техн. наук, професор)¹

Іван Іванович Петров (канд. техн. наук, доцент)²

¹Університет..., Київ, Україна

²Інститут..., Київ, Україна

← (кегль – 11 пт.)

← 1 пустий рядок – 10 пт.

← (кегль – 11 та 8 пт.)

← 1 пустий рядок – 6 пт.

← 1 пустий рядок – 10 пт.

НАЗВА СТАТТІ (*Arial*, кегль – 14 пт.; накреслення – “напівжирне”, по правому краю)

← 1 пустий рядок – 10 пт.

Текст анотації мовою тексту статті (в даному випадку – українською). Зміст анотації має стисло і достатньо інформативно підсумовувати основні ідеї та отримані результати дослідження. Розмір анотації повинен становити 100–250 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.

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.

Шриффт 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 колонітилли. Між значенням величини та одиницею її вимірювання ставте нерозривний пропуск (Ctrl + Shift + пропуск).

УВАГА! Остання сторінка статті заповнюється

не менш, ніж на 3/4.

Набір формул: редактор формул MS Equation. **Забороняється** використовувати для набору формул графічні об'єкти, кадри й таблиці.

В меню “Размер → *Определить*” ввести такі розміри: Обычный – 10 пт.; Крупный индекс – 8 пт.; Мелкий индекс – 7 пт.; Крупный символ – 15 пт.; Мелкий символ – 9 пт.

Стиль формул – “прямий”, тобто в меню “Стиль → *Определить*” поля “Формат символів” – пусті.

Табличний заголовок (10 пт.) – **обов'язковий**.

Рисунки **обов'язково** супроводжуються центрованими підписаними підписами (кегль – 10).

Не допускаються кольорові та фонові рисунки.

Допускається розташування великих рисунків, формул та таблиць в одну колонку (до 16 см.).

Список літератури виділяється підзаголовком “**Література**” та оформлюється згідно з міждержавним стандартом ДСТУ ГОСТ 7.1:2006” (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), міжрядковий інтервал – 1,0, вирівнювання – по центру). Обсяг анотації – 100-250 слів, англійською – 150-250 слів.

НАЗВАННЯ СТАТТІ

¹Анатолій Анатолієвич Іванов (д-р техн. наук, професор)

²Іван Іванович Петров (канд. техн. наук, доцент)

¹Університет..., Київ, Україна

²Інститут..., Київ, Україна

Перевод текста аннотации и ключевых слов

ARTICLE TITLE

¹Anatolii A. Ivanov (Doctor of Technical Sciences, Professor, Professor of a Department)¹

²Ivan I. Petrov (Candidate of Technical Sciences, Associate Professor, Associate Professor of a Department)²

¹University..., Kyiv, Ukraine

²Institute..., Kyiv, Ukraine

Translation of the abstract and keywords

Після цього наводиться список літератури англійською мовою за зразком (9 кегль):

References

1. Pukhov G.E. (1990), Differential spectrums and models. [Dyferentsiini spektry ta modeli], Kyiv, Naukova Dumka, 184 p. 2. Mikheenko L.A., Nechiporuk S.A. (2011), Energy model of digital camcorder. [Enerhetichna model tsyfrovoyi videokamery], Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh, No. 1. pp. 150–157. 3. Voskresenskaya E.V. (2003), Legal regulation of valuation activities: dissertation. [Pravovoe regulirovanie otsenочноi deyatel'nosti: dis. kand. yurid. nauk], St. Petersburg, 187 p. 4. Bezrodnaya V.F. (2004), Features of

civil society development in the process of political modernization of Ukraine: Author's thesis. [Osobennosti formirovaniya grazhdanskogo obshchestva v protsesse politicheskoi modernizatsii Ukrainy: avtoref. dis. kand. polit. nauk], Odessa, 16 p. 5. Serdyuk T.V., Self-regulation in Ukraine: advantages and disadvantages in the current economic conditions. [Samoregulirovanie v Ukraine: preimushchestva i nedostatki v sovremennykh ekonomicheskikh usloviyakh], available at: <http://economy.kpi.ua/ru/node/343>.

A.A. Ivanov: iv@u.ua I.I. Petrov: petr@u.ua

Після цього наводяться відомості про рецензента та контактна інформація авторів.

Рецензент: д-р техн. наук, професор О. Ю. Пермяков, начальник інституту, Національний університет оборони України імені Івана Черняхівського, Київ.

Автор: Анатолій Анатолійович Іванов
Роб. тел. – 333-33-33, дом. тел. – 777-77-77, E-mail – kim@ic.ua.

Подання матеріалів

Обсяг рукопису – від 3 до 10 аркушів українською, російською або англійською мовами.

Для публікації необхідно представити статтю у електронній формі з роздрукованим екземпляром,

підписаним всіма авторами статті. Рукопис супроводжується **експертним висновком, рецензією доктора наук (професора), витягом з протоколу засідання кафедри (відділу)**. Подані матеріали автору не повертаються.

Матеріали просимо подавати до інституту інформаційних технологій Національного університету оборони України імені Івана Черняхівського за адресою: 03049, м. Київ, Повітрофлотський пр., 28, тел.: (044) 271-09-44, Тищенку Максиму Георгійовичу, каб. 2/305, тел.: +38-066-713-20-22, e-mail: sitnuou@ukr.net.

З питань оплати звертатись до редакції.

Редколегія залишає за собою право відмови у публікації статей, що не відповідають проблематиці журналу й умовам оформлення матеріалів.

Корисні посилання:

<http://translit.kh.ua/?passport> – автоматична транслітерація з української мови

<http://ru.translit.net/> – автоматична транслітерація з російської мови

<http://vak.in.ua/do.php> – оформлення списку літератури по вимогам ВАК України

Комп'ютерна верстка: *М.Г. Тищенко, М.О. Масесов, Є.О. Судніков*

Оформлення обкладинки: *Є.О. Судніков*

Засновник і видавець Національний університет оборони України імені Івана Черняховського.
Св-во КВ № 20490-10290ПР. Адреса редакції: 03049, м. Київ, Повітрофлотський пр-т, 28. Тел. (044) 271-09-44.

Підписано до друку 31.08.2016. Формат 60×84 1/8. Ум. друк. а. 19. Тираж 100 прим.

Надруковано у друкарні Національного університету оборони України імені Івана Черняховського.
