Modern Information Technologies in the Sphere of Security and Defence

Сучасні інформаційні технології у сфері безпеки та оборони

2(41) 2021

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

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

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ БЕЗПЕКИ ТА ОБОРОНИ

№ 2(41)
2021

Науковий журнал

Засновник і видавець

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

Адреса редакції

Національний університет оборони України
імені Івана Черняховського
Інститут інформаційних технологій

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

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

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

Журнал видається
українською, російською та англійською мовами

Журнал виходить 3 рази на рік

Наказом Міністерства освіти і науки України №409 від 17.03.2020 р. та №886 від 02.07.2020 р. журнал включено до Переліку наукових фахових видань України категорії "Б" в галузях "технічні науки" та "військові науки", спеціальності – 122, 124, 253, 254

Рекомендовано до друку Вченою радою Національного університету оборони України імені Івана Черняховського

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

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

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

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

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

В номері:

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

MODERN INFORMATION TECHNOLOGIES IN THE SPHERE OF SECURITY AND DEFENCE

№ 2(41)
2021

Scientific journal

Founder and Publisher

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

Address:

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

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

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

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

The journal is published
in Russian, Ukrainian and English

The journal is published thrice a year

According to the orders of the Ministry of Education and Science of Ukraine № from 17.03.2020 and №886 from 02.07.2020 the journal was included in the List of scientific professional publications of Ukraine, "B" category, "technical sciences" and "military sciences" fields, specialties 122, 124, 253, 254

Recommended to publication by the Scientific Council of the National Defence University of Ukraine named after Ivan Cherniakhovskyi

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

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

Contents:

DOI:**10.33099/2311-7249/2021-41-2-5-10**

УДК: 621.396.9

Андрій Олександрович Зінченко *(доктор технічних наук, професор)*
Микола Олександрович Масесов *(кандидат технічних наук, с.н.с.)*
Іван Олегович Пантась

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ ЖИВУЧОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Розвиток телекомунікаційних технологій, в тому числі й радіорелейних та тропосферних, актуалізує проблему підвищення стійкості мереж у зв'язку з постійним підвищенням вимог до якості їх функціонування. Особливої уваги на теперішній час, враховуючи досвід ООС, потребує необхідність вдосконалення методів упередження та нейтралізації негативних впливів на телекомунікаційні мережі, які в наш час постійно вдосконалюються та відбуваються в формах, яких раніше не існувало. Збільшується кількість випадків негативних впливів на телекомунікаційні мережі, які наносять шкоду не тільки фізичній структурі мережі, а й логічній, що, в свою чергу, вимагає розглядати питання оцінки підвищення живучості не тільки в аспекті структурної живучості, а й в аспекті продуктивності програмного управління різнорідним трафіком. Додатково необхідно приділити увагу безпеці функціонування з'єднань та передачі інформації по ним.

Метою даної статті є аналіз найбільш актуальних методів та методик забезпечення та підвищення необхідного рівня живучості та звуження кола наукових досліджень для подальшої оптимізації або пошуку більш вдалої комбінації методів чи створення вдосконаленої методики для підвищення ефективності у вирішенні проблем пов'язаних з забезпеченням необхідного рівня живучості телекомунікаційних мереж та систем.

При дослідженнях живучості можливо використовувати ряд різних теоретичних підходів і, таким чином, застосування різних методів аналізу: теоретико-ігрових, імовірнісних, детермінованих, графо-аналітичних. Імовірнісний і детермінований підходи є найбільш розробленими для технічних цілей, а тому є перспективними для вдосконалення та оптимізації.

Ключові слова*: аналіз методів підвищення живучості, живучість системи зв'язку, радіорелейний та тропосферний зв'язок.*

Вступ

Постійний розвиток телекомунікаційного обладнання забезпечує збільшення кількості сервісів, які можливо реалізувати за допомогою сучасних телекомунікаційних систем та мереж. У зв'язку з цим підвищуються вимоги до якості телекомунікаційних послуг. Забезпечення належної якості телекомунікаційних послуг є динамічною задачею, складність якої пропорційна завданням та вимогам до телекомунікаційної системи й, відповідно, обладнанню на базі якого побудована система. Розвиток телекомунікаційної системи (ТКС) супроводжується постійною проблемою, яка полягає в інтеграції нового обладнання в систему, яка існує, та узгодження його для повноцінного використання та забезпечення запланованих переваг від провадження даних змін. Особливе значення для критично важливих телекомунікаційних систем та їх елементів має поняття живучості системи зв'язку: згідно ДСТУ В 3265-95 [1] п. 8.7 живучість – здатність системи військового зв'язку забезпечувати управління військами (силами) в умовах дії зброї противника; згідно військового стандарту ВСТ 01.112.001-2006 [2], є складовою стійкості, яка відноситься до основних показників якості телекомунікаційних систем.

Взаємозв'язок та залежність різних характеристик (властивостей) системи військового зв'язку, в тому числі живучості, наведено на рисунках 1 та 2.

Як видно, в різних чинних керівних документах поняття та визначення даної характеристики та її приналежність до групи характеристик дещо відрізняється. В деяких працях дана розбіжність в підходах надає можливість розглядати поняття живучості мереж та систем зв'язку більш широко, й визначити проблематику області досліджень більш точно.

В пострадянських країнах підхід до характеристик системи зв'язку аналогічний підходу в Україні.

Поняття живучості, як однієї з характеристик системи зв'язку НАТО, як такої немає. В ряді країн, які входять до даного військового блоку існують визначені вимоги до системи зв'язку – в загальному вигляді система зв'язку повинна мати зв'язну топологію, яка залежить від актуальної оперативної обстановки, характеру місцевості, завдань всіх підрозділів бойового порядку, умови виконання завдань підрозділами не повинні викликати істотних змін в організації зв'язку.

Для розуміння планування та організації зв'язку у країнах – учасниках НАТО слід зазначити, що основними особливостями процесу управління військами, бойовими системами і озброєнням є:

- значна інформаційна потреба органів управління;
- підвищена мобільність підрозділів і частин;
- висока динаміка переміщень угруповань військ у цілому;
- розосереджене розгортання військ на територіях, розділених силами супротивника;
- інтеграція систем зв'язку, навігації, розвідки й автоматизації й ін.;
- єдиний інформаційний простір для всіх його учасників;
- орієнтація на безпосередніх учасників бойових дій (автоматизація рівнів батальйон – рота – взвод – окремий солдат);
- децентралізація процесів управління ресурсами мережі [3].

Постановка проблеми. В той же час, аналіз бойового застосування сучасного телекомунікаційного обладнання в ході бойових дій на сході України виявив низку проблем. Однією з критичних проблем виявилась неготовність системи забезпечити виконання покладених на неї завдань в умовах ведення бойових дій та застосування радіоелектронного подавлення та боротьби противником. Після початкового етапу оперативної заміни обладнання старого парку на обладнання, адекватне вимогам часу та ситуації, гостро постала проблема узгодження роботи даного обладнання, а також неготовність особового складу до його застосування. Під час проведення аналізу даного процесу увагу привертає проблема зниження рівня живучості телекомунікаційних систем та мереж через неврахування деяких факторів, як приклад – вирішення проблеми відновлення працездатності та обслуговування телекомунікаційного обладнання, виконання якої дасть змогу оперативного реагування на позаштатні ситуації та відновлення працездатності ланок ТКС, які того потребують; своєчасного узгодження програмного забезпечення телекомунікаційного обладнання для коректної роботи засобів зв'язку.

Виходячи з наведених прикладів, методи та методики за допомогою яких розраховувалась живучість в ТКС необхідно переглянути, та замінити на нові або удосконалити ті, які існують з врахуванням отриманого досвіду активної інтеграції різноманітного обладнання в наявну ТКС та досвіду забезпечення необхідного рівня якості зв'язку в умовах ведення бойових дій.

Рис.1 Показники якості системи військового зв'язку (згідно ДСТУ В 3265-95)

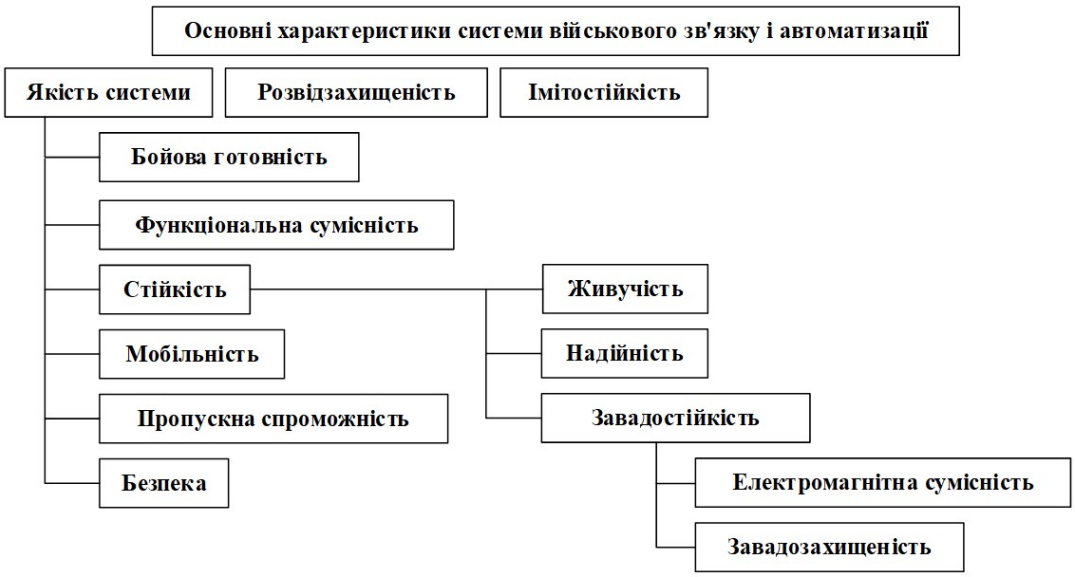

Рис.2 Основні характеристики системи військового зв'язку і автоматизації (згідно військового стандарту ВСТ 01.112.001-2006)

Аналіз останніх досліджень і публікацій. Аналіз науково-технічної літератури, інформації у відкритих джерелах та інтернеті показує, що проблематику даного питання досліджують як українські, так і іноземні вчені, а саме: А. П. Пятибратов, А.М. Юрков, Л. А. Крукиєр, Н. С. Рузанова, О. Ю. Насадкіна, В. И. КомашинськийБ. М. Стрихалюк, М. М. Климаш, М. В. Кайдан, А. Д. Іванніков, Н. О. Князєва, E. Auer, D. Helmstädt, C. Hoogendoom, G. Ohlendorf, S. V. Ahamed., V. B. Lawrence, Y. Shpungin, R. Vaisman.

Метою статті є провести аналіз методів оцінювання живучості телекомунікаційних мереж з метою подальшої їхньої оптимізації та створення вдосконаленої методики для підвищення ефективності у вирішенні проблем пов'язаних з забезпеченням необхідного рівня живучості телекомунікаційних мереж.

Виклад основного матеріалу дослідження

Г.В. Попков, В.К. Попков, В.В. Величко, А.Г. Додонов, Д.В. Ланде в своїх роботах розглянули досконально питання аналізу живучості мереж зв'язку в умовах деструктивних інформаційних впливів. В їх роботах наведена класифікація інформаційних атак в інформаційних мережах та методи їх виявлення. Широко розглянуті питання, які пов'язані з живучістю та надійністю мобільних систем зв'язку та запропоновані моделі структурної надійності в мобільних мережах передачі даних. [4,5]

В роботі І.В. Грищенко «Метод підвищення живучості інфокомунікаційної мережі» автор досяг значних результатів в удосконаленні трьох методів підвищення структурної живучості та вперше розробив кількісну оцінку живучості ТКМ, значенню якої (рівному «1») відповідає зважена за пріоритетами вимог сума пропускних спроможностей маршрутів обслуговування вимог в умовах нормального (без несприятливих впливів (НВ)) функціонування телекомунікаційної мережі (ТКМ), зміна значення якої в умовах НВ надає можливість визначити міру працездатності ТКМ. Завдяки чому отримали подальший розвиток методи реалізації системи прийняття рішень в управлінні структурною живучістю ТКМ, використання яких надає можливість керувати процесом прийняття рішень з метою безвідмовного функціонування ТКМ в умовах НВ. Також розроблено програмне забезпечення системи підтримки прийняття рішень в управлінні структурною живучістю, що реалізує удосконалені методи підвищення структурної живучості [6].

Н.А. Князева, І.В. Грищенко, С.В. Шестопалов в роботі «Метод забезпечення живучості телекомунікаційної системи на основі перерозподілу ресурсів мережі» представили метод забезпечення живучості телекомунікаційної мережі на основі перерозподілу ресурсів мережі для обслуговування потоків вимог при виникненні несприятливих впливів що дозволяє:

виконати оцінку працездатності мережі на основі запропонованого показника;

виявити «вузькі місця» мережі для можливості їх резервування;

виробити відповідні рекомендації для забезпечення працездатності мережі [7].

Суть методу полягає в послідовному виконанні десяти етапів розрахунків, починаючи з введення станів, отримання кількісних оцінок та закінчується отриманням оцінки працездатності та визначенням відповідності станів телекомунікаційної мережі гранично допустимому значенню показника працездатності. Запропонований метод може бути використаний на етапі проектування ТКС для оцінки працездатності мережі при зміні її топології.

Науковці Військового інституту телекомунікацій та інформатизації (Бондаренко Л.О., Масесов М.О., Садиков О.І.) запропонували методику оцінки стійкості системи військового зв'язку [8]. Оцінка стійкості системи в даній методиці базується в тому числі на оцінці живучості з врахуванням факторів НВ, які з'явились в наш час. При цьому було введено ряд обмежень, які були застосовані під час досліджень, для забезпечення можливості використання методики в обмежених часових умовах роботи органів військового управління зв'язком. Але, як показав аналіз оцінки стану системи зв'язку під час ведення бойових дій, факторів, які враховуються, недостатньо для повноцінної оцінки якості стану системи. Частина даних обмежень була актуальна на моменти дослідження авторами ситуації, й як показав досвід ООС, обмежень під час розрахунку живучості мережі має бути якнайменше. Необхідно намагатись врахувати якомога більше факторів та ситуацій, які можливі в системі, постійно оновлювати переліки несприятливих впливів та слідкувати за їх актуальністю.

В.В. Воротніков, О.С. Бойченко, Є.О. Гринєвич удосконалили методику підвищення живучості інформаційно-комунікаційної мережі, яка відрізняється методом енергоефективної кластеризації та методом багатошляхової маршрутизації, що дає змогу підвищити ймовірність відмови обслуговування користувачів. Підвищення живучості інформаційно-комунікаційної мережі за критерієм живучості – ймовірність відмови обслуговування користувачів, досягається за рахунок спільного використання механізмів реорганізації та реконфігурації. З метою реорганізації інформаційно-комунікаційної мережі розроблено метод енергоефективної кластеризації вузлів мережі, який дозволяє зменшити витрати енергії на передачу інформації. Для реалізації процесу реконфігурації удосконалено метод багатошляхової маршрутизації, застосування якого дозволяє підвищити час життя інформаційно-комунікаційної мережі [9].

Враховуючи реалії сьогодення в контексті збройної агресії Російської Федерації, окупації частини території країни та відповідно проведення

ООС, особливої уваги потребує аналіз досліджень які проводяться російськими вченими та дослідниками.

Н.Г. Бурменський в роботі «Живучість системи військового зв'язку: проблеми та шляхи рішення» показав, що ефективність військами та озброєнням напряму пов'язана з системою військового зв'язку виконувати свої функції в умовах впливів звичайного, ядерного та спеціального видів зброї. Приведений аналіз наявних в наш час засобів ураження, які здатні найбільш ефективно вражати радіоелектронні засоби, як найважливіші елементи системи. Сформульовані особливості системи військового зв'язку, як об'єкта озброєння, проблемні питання забезпечення необхідного рівня живучості та шляхи їх вирішення [10].

А. А. Зацарінний , Н. Г. Бурменський , А. И. Гаранін в дослідженні «Метод формування системи показників живучості інформаційно-телекомунікаційних мереж» запропонували методичні підходи до формування системи показників живучості ІТС, які основані на аналізі умов їх застосування, оцінці факторів, які впливають на живучість системи, й визначенні властивостей, які повинна мати система для виконання необхідних функцій [11].

Особливістю даної роботи є те, що поняття живучості системи зв'язку розглядається в моменті збройного протистояння двох угрупувань з відповідними цілями з кожного боку.

В своєму інтерв'ю 27.04.2021 єдиному національному інформаційному агентству України УКРІНФОРМ, командувач Військ зв'язку та кібербезпеки ЗСУ Євген Степаненко, звернув увагу на реформування і створення нових структурних підрозділів військ зв'язку, яке відбувається згідно натівських принципів. Відмінністю від структури військ зв'язку НАТО є те, що у складі командування Військ зв'язку та кібербезпеки є таке поняття, як «військовий провайдер» – постійно діюча система зв'язку (стаціонарна компонента), яка функціонує постійно в Збройних Силах України у стаціонарному вигляді: це стаціонарні вузли зв'язку, волокно-оптичні, радіорелейні та тропосферні лінії зв'язку, лінії прямого зв'язку, лінії прив'язки тощо, мережі й напрямки радіозв'язку. Це якраз та постійно діюча система зв'язку, яку треба утримувати та розвивати. Також він наголосив про те що розвиток та підтримка даної компоненти є однією з ключових задач Військ зв'язку та кібербезпеки.[12]

За останні роки, у зв'язку з проведенням комплексу заходів по відновленню територіальної цілісності держави, Збройні Сили України зазнали колосальної модернізації в усіх напрямках, а система зв'язку Збройних Сил України (ЗСУ) також кардинально змінились. Розроблено, отримано від стратегічних партнерів та прийнято на озброєння (постачання) ряд новітніх засобів зв'язку, які відповідають вимогам часу, змінились деякі підходи до організації та забезпечення безпеки зв'язку в сучасній армії. Це в свою чергу створює ряд нових завдань забезпеченню необхідного рівня зв'язності та живучості ТКМ з врахуванням варіантів інтеграції сучасного обладнання з тим, яке вже існує.

Деякі зразки засобів зв'язку, які використовують ЗСУ в даний час, не було можливості перевірити в умовах наближених до бойових, робилась ставка на його технологічність та надійність складових. На відміну, Російська Федерація тестує свої розробки та новітні зразки озброєння та військової техніки в реальних збройних конфліктах в різних куточках світу й Україна не виняток. Дана ситуація висвітлила нову проблему – відсутність можливості оперативного усунення бойових пошкоджень – а це один з складників живучості, який необхідно активно досліджувати для ефективної оптимізації системи прийняття рішень щодо забезпечення необхідного рідня живучості ТКМ ЗСУ в цілому.

Проаналізована література та дослідження, які проводяться в даній області, висвітлюють таку недосліджену проблематику:

- рішення задачі комплексної оцінки живучості системи військового зв'язку з врахуванням більшої множини факторів в різних умовах бойових дій;
- необхідність розширення вимог до живучості в тактико-технічних (технічних) завданнях на розробку засобів зв'язку;
- необхідність розробки методики підвищення живучості ТКМ з врахуванням того, що це динамічна система, яка постійно розвивається та змінюється.

Особливу увагу необхідно звернути на дослідження ситуації в сегменті радіорелейного та тропосферного зв'язку. Ця необхідність випливає з універсальності та мобільності даного виду обладнання, за допомогою якого є можливість оперативно будувати багатоканальні лінії зв'язку відносно великої дальності, які можуть забезпечити мультисервісність мережі та необхідний рівень стійкості мережі, однією з складових якої і є живучість. Особливу увагу цей рід зв'язку привертає тому що під час АТО та ООС він зарекомендував себе як один з найбільш оперативних та ефективних родів зв'язку, який забезпечує виконання поставлених завдань підрозділами.

Перспективним для поглибленого дослідження та вдосконалення є система прийняття рішень в управлінні структурною живучістю ТКМ. Досягти більшої ефективності даної системи можливо за рахунок включення в базові складові методів для обчислень живучості додаткових параметрів, які враховують специфіку застосування ТКМ у сфері існування військового зв'язку.

Висновки і перспективи подальших досліджень

Подальша оптимізація методів та створення вдосконаленої методики для підвищення ефективності у вирішенні проблем пов'язаних з

забезпеченням необхідного рівня живучості телекомунікаційних мереж та систем є перспективним напрямком наукових досліджень. Вирішення поставленої проблематики однозначно підвищить ефективність оцінки живучості що, в свою чергу, підвищить якість обслуговування в ТКС в цілому. Для системи військового зв'язку поняття живучості є одним з ключових, тому що від забезпечення високих показників даної характеристики пропорційно залежить можливість військових підрозділів виконувати завдання за призначенням на високому професійному рівні при якісній роботі системи управління.

Література

1. ДСТУ В3265–95 "Зв'язок військовий. Терміни та визначення". **2.** ВСТ 01.112.001-2006. "Військовий звязок. Терміни та визначення". **3. Думітраш В., Бондаренко О., Думітраш О., Гетьман А.** Аналіз напрямків розвитку систем радіозв'язку НАТО URL: https://www.ukrmilitary.com/2020/08/signal.html. **4. Величко В. В., Попков Г. В., Попков В. К..** Модели и методы повышения живучести современных систем связи — М.: Горячая линия-Телеком, 2017. — 270 с. **5. Додонов А.Г.** Живучесть информационных систем / А.Г. Додонов, Д.В. Ландэ. – К.: Наук. думка, 2011. – 256 с. **6. Грищенко И. В.** Метод повышения живучести инфокоммуникационной сети / И. В. Грищенко // Холодильна техніка і технологія. - Одеса, НХІХКтаЕ, 2013. - №6. (146). – С. 66–70. **7. Князева Н. О.** Метод обеспечения живучести телекоммуникационной сети на основе перераспределения ресурсов сети [Текст] / Н. О. Князева, И. В. Грищенко, С. В. Шестопалов // Холодильная техника и технология. Одеса, НХІХКтаЕ, 2014. - №4. (150). – С. 65–71. **8. Масесов М.О., Бондаренко Л.О., Садиков О.І., Макарчук В.І.** Методика оцінки стійкості системи військового зв'язку. Збірник наукових праць ВІТІ. – 2016. – 5 С. 94-102. **9. Воротніков В.В., Бойченко О.С., Гринєвич Є.О.** Методика підвищення живучості інформаційно-комунікаційної мережі. Системи обробки інформації. — 2017. — № 5(151). С. 69-75. **10. Буроменский Н.Г.** Живучесть системы военной связи: проблемы и пути решения. Вооружение и экономика. -2014 № 4 (29) С. 54-59. **11. Зацаринный А. А., Буроменский Н. Г., Гаранин А. И.** Системы и средства информ., 23:2 (2013), 154–169. **12. Степаненко Є.О.** Інтерв'ю інформагенству Укрінформ 27.04.2021 URL: https://armyinform.com.ua/2021/04/systemy-zvyazku-yaki-my-zakupovuyemo-suttyevo-krashhi-anizh-ti-yaki-rosiyany-vyroblyayut-u-sebe/.

АНАЛИЗ МЕТОДОВ ПОВЫШЕНИЯ ЖИВУЧЕСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

***Андрей Александрович Зинченко** (доктор технических наук, профессор)*
***Николай Александрович Масесов** (кандидат технических наук, с.н.с.)*
Иван Олегович Пантась

Военный институт телекоммуникаций и информатизации имени Героев Крут, Киев, Украина

Развитие телекоммуникационных технологий, в том числе радиорелейных и тропосферных, актуализирует проблему повышения устойчивости сетей в связи с постоянным повышением требований к качеству их функционирования. Особого внимания в наше время, учитывая опыт ООС, требует необходимость совершенствования методов предупреждения и нейтрализации негативных воздействий на телекоммуникационные сети, которые в наше время постоянно совершенствуются и происходят в формах, которых ранее не существовало. Увеличивается количество случаев негативных воздействий на телекоммуникационные сети, которые наносят вред не только физической структуре сети, но и логической, что, в свою очередь, требует рассматривать вопрос оценки живучести не только в аспекте структурной живучести, но и в аспекте производительности программного управления разнородным трафиком. Дополнительно необходимо уделить внимание безопасности функционирования соединений и передачи информации по ним.

Целью данной статьи является анализ наиболее актуальных методов и методик обеспечения и повышения необходимого уровня живучести и сужение круга научных исследований для дальнейшей оптимизации или поиска более удачной комбинации методов или создания усовершенствованной методики для повышения эффективности в решении проблем, связанных с обеспечением необходимого уровня живучести телекоммуникационных сетей и систем.

При исследованиях живучести можно использовать ряд различных теоретических подходов и, таким образом, применение различных методов анализа: теоретико-игровых, вероятностных, детерминированных, графо-аналитических. Вероятностный и детерминированный подходы являются наиболее разработанными для технических целей, а потому являются перспективными для совершенствования и оптимизации.

***Ключевые слова:** анализ методов повышения живучести, живучесть системы связи, радиорелейная и тропосферный связь.*

ANALYSIS OF METHODS OF INCREASING VISIBILITY TELECOMMUNICATIONS NETWORKS

***Andrii Zinchenko** (Doctor of technical sciences, professor)*
***Mykola Masesov** (Candidate of Technical Science, Senior Research Scientist)*
Ivan Pantas

Military Institute of Telecommunications and Informatization named after Heroes Krut, Kiev, Ukraine

The development of telecommunication technologies, including radio relay and tropospheric technologies, raises the problem of increasing the stability of networks in connection with the constant increase in requirements for the quality of their operation. Particular attention in our time, given the experience of environmental protection, is growing need to improve methods of prevention and neutralization of negative impacts on telecommunications networks, which in our time are constantly improving and occur in forms that previously did not exist. The number of cases of negative effects on telecommunications networks that harm not only the physical structure of the network, but also logical, which, in turn, requires consideration of assessing the increase in survivability not only in terms of structural survivability, but also in terms of software performance of heterogeneous traffic management. Additionally, you need to pay attention to the security of connections and the transmission of information on them.

The purpose of this article is to analyze the most relevant methods and techniques to ensure and increase the required level of survivability and narrow the scope of research to further optimize or find a better combination of methods or create improved methods to improve efficiency in solving problems related to ensuring the required level of telecommunications networks. and systems.

In the study of survivability, it is possible to use a number of different theoretical approaches and, thus, the use of different methods of analysis: game-theoretic, probabilistic, deterministic, graph-analytical. Probabilistic and deterministic approaches are the most developed for technical purposes, and therefore are promising for improvement and optimization.

Keywords*: analysis of methods to increase survivability, survivability of the communication system, radio relay and tropospheric communication.*

References

1. DSTU V3265–95 “Zviazok viiskovyi. Terminy ta vyznachennia”. **2.** VST 01.112.001-2006. “Viiskovyi zviazok. Terminy ta vyznachennia”. **3. Dumitrash V.**, Bondarenko O., Dumitrash O., Hetman A. Analiz napriamkiv rozvytku system radiozviazku NATO URL: https://www.ukrmilitary.com/2020/08/signal.html.

4. Velichko V. V., Popkov G. V., Popkov V. K.. Modeli i metodyi povyisheniya zhivuchesti sovremennyih sistem svyazi — M.: Goryachaya liniya-Telekom, 2017. – 270 s. **5. Dodonov** A.G. Zhivuchest informatsionnyih sistem / A.G. Dodonov, D.V. Lande. – K.: Nauk. dumka, 2011. – 256 s. **6. Grischenko** I. V. Metod povyisheniya zhivuchesti infokommunikatsionnoy seti / I. V. Grischenko // Holodilna tehnIka I tehnologIya. - Odesa, NNIHKtaE, 2013. - № 6. (146). – S. 66–70. **7. Knyazeva** N. O. Metod obespecheniya zhivuchesti telekommunikatsionnoy seti na osnove pereraspredeleniya resursov seti [Tekst] / N. O. Knyazeva, I. V. Grischenko, S. V. Shestopalov // Holodilnaya tehnika i tehnologiya. Odesa, NNIHKtaE, 2014. - №4. (150). 65–71. **8. Masesov M.O**., Bondarenko L.O., Sadykov O.I., Makarchuk V.I. Metodyka otsinky stiikosti systemy viiskovoho zviazku. Zbirnyk naukovykh prats VITI. – 2016. – 5 S. 94-102. **9. Vorotnikov V.V**., Boichenko O.S., Hrynievych Ye.O. Metodyka pidvyshchennia zhyvuchosti informatsiino-komunikatsiinoi merezhi. Systemy obrobky informatsii. – 2017. – № 5(151). S. 69-75. **10. Buromenskiy** N.G. Zhivuchest sistemyi voennoy svyazi: problemyi i puti resheniya. Vooruzhenie i ekonomika. -2014 № 4 (29). 54-59. **11. Zatsarinnyiy** A. A., Buromenskiy N. G., Garanin A. I. Sistemyi i sredstva inform., 23:2 (2013), 154–169. **12. Stepanenko** Ye.O. Interviu informahenstvu Ukrinform 27.04.2021 URL: https://armyinform.com.ua/2021/04/systemy-zvyazku-yaki-my-zakupovuyemo-suttyevo-krashhi-anizh-ti-yaki-rosiyany-vyroblyayut-u-sebe/.

DOI:**10.33099/2311-7249/2021-41-2-11-16**

УДК: 621.391.825

Григорій Митрофанович Тіхонов (кандидат військових наук, с.н.с.)[1]
Сергій Миколайович Шолохов (кандидат технічних наук, доцент)[2]
Богдан Анатолійович Ніколаєнко (кандидат технічних наук)[2]
Валерій Миколайович Тютюнник [1]

[1]Національний університет оборони України імені Івана Черняховського, Київ, Україна
[2]Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Україна

ПОСТАНОВКА ЗАДАЧІ ОПТИМАЛЬНОГО РОЗПОДІЛУ РЕСУРСУ НЕОДНОРІДНИХ ЗАСОБІВ ДИСТРУКТИВНОГО ВПЛИВУ НА ЕЛЕМЕНТИ ПЛАТФОРМИ НАЦІОНАЛЬНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ В ОСОБЛИВИЙ ПЕРІОД

Завадозахист системи зв'язку є актуальним та важливим напрямом дослідження, методологія оцінки впливу на нього засобів радіо та електромагнітного подавлення, на сьогоднішній день, досить розвинута та відома. Національна телекомунікаційної мережа, як сукупність систем і мереж зв'язку, в умовах ведення гібридної війни проти України потребує вдосконалення способів її захисту від деструктивного впливу противника, що має на озброєнні новітні засоби радіо подавлення та електромагнітного впливу. Незахищена Національна телекомунікаційної мережа не зможе виконати основну свою функцію, а саме обіг (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам. Якісна розробка способів та методів забезпечення завадостійкості елементів Національної телекомунікаційної мережі неможлива без прогнозування можливих сценаріїв дій противника та завадової обстановки, що може скластися.

Теперішній момент часу характеризується принциповими змінами у умовах застосування транспортної платформи Національної телекомунікаційної мережі в умовах ведення гібридної війни Російської Федерації проти України. Проведений аналіз показав, що у випадку загострення ситуації на фронті, переходу противника до широкомасштабної збройної агресії або терористичних дій ресурс транспортної платформи Національної телекомунікаційної мережі є одним з першочергових об'єктів впливу новітніх засобів радіоелектронного та електромагнітного подавлення частин (підрозділів) РЕБ російсько-терористичних військ.

Проведено постановку задачі раціонального розподілу ресурсу неоднорідних засобів радіоелектронної боротьби противника по елементах транспортної платформи Національної телекомунікаційної мережі для подальшої розробки методики визначення способів її радіоелектронного подавлення та створення моделі радіоелектронної обстановки в умовах ведення гібридних, бойових та терористичних дій противником проти України.

***Ключові слова**: багатокритеріальна оптимізація, деструктивний вплив, радіоелектронна боротьба, електромагнітний вплив, транспортна платформа, сценарій дій, завадова обстановка, терористичні дії, гібридна війна.*

Вступ

В умовах особливого періоду в країні, коли російські окупаційні війська продовжують порушувати Мінські домовленості і практично ведуть бойові дії на сході України, особлива увага повинна приділятися розробці і розвитку засобів радіоелектронної боротьби. Це пояснюється тим, що сучасне озброєння і військова техніка (ОВТ) швидко розвивається, все більше радіоелектронних засобів з'являється на озброєнні противника, а старі способи і засоби боротьби з ними малоефективні.

Постановка проблеми. Дослідження та аналіз досвіду ведення антитерористичної операції (АТО) та операції об'єднаних сил (ООС) показав, що для дезорганізації державного управління російсько-терористичні війська можуть комплексно та узгоджено за місцем і часом впливати на елементи транспортної платформи (ТП) Національної телекомунікаційної мережі засобами радіо (РП) та електромагнітного подавлення (ЕМП) [2, 3, 4].

В таких умовах транспортна платформа Національної телекомунікаційної мережі повинна забезпечувати виконання завдань за призначенням умовах складної завадової обстановки, що обумовлена масованим застосуванням навмисних подібних, структурних, широкосмугових шумових, вузькосмугових перешкод противника для радіоподавлення приймальних пристроїв радіозасобів транспортної платформи Національної телекомунікаційної мережі. Це вимагає розробки нових методів та засобів завадозахисту для застосування у складі транспортної платформи Національної телекомунікаційної мережі.

На першому етапі розробки методів та засобів завадозахисту транспортної платформи Національної телекомунікаційної мережі виникає завдання визначення можливих способів радіо- та електромагнітного подавлення з урахуванням реальних бойових можливостей новітніх засобів РЕБ противника та можливостей наших військ щодо їх знищення з подальшою розробкою моделі реальної завадової обстановки що може скластися під час ведення бойових або диверсійних дій [5].

Зауважимо що під способом радіо-електронного подавлення транспортної платформи Національної телекомунікаційної мережі будемо розуміти порядок і прийоми застосування засобів радіо- та електромагнітного подавлення з метою радіоелектронного подавлення ліній зв'язку ТП в умовах ведення гібридних бойових та терористичних дій.

Аналіз останніх досліджень і публікацій. Питання обґрунтування способів РЕБ розглянуті в [5]. Однак, у відомій літературі можливі сценарії та способи радіо та електромагнітного подавлення ТП Національної телекомунікаційної мережі не досліджені. Сутність та вимоги до етапу математичної постановки задачі оптимізації (раціоналізації) складних організаційних систем розглядались в роботі [6,7], в тому числі військового призначення. Однак, отримані результати не конкретизовані до формування оптимальних способів за економічними показниками та показниками складності виконання бойового завдання новітніми засобами радіоподавлення та ЕМП в операціях.

Метою статті є проведення постановки задачі раціонального розподілу ресурсу неоднорідних засобів радіоелектронної боротьби противника по елементах ТП транспортної платформи Національної телекомунікаційної мережі для подальшого розробки методики визначення способів її радіоелектронного подавлення в умовах ведення гібридних бойових та терористичних дій.

Виклад основного матеріалу дослідження

В методичному плані будь-яка задача оптимізації включає два етапи: постановку задачі і її рішення. Постановка задачі передбачає змістовний опис і формальне представлення. Метою змістовного опису є відображення фізичного змісту задачі формальне представлення необхідно для приведення змістовного опису до вигляду, зручного для рішення.

Задача вважається коректно поставленою, якщо вибрані критерії оптимальності, визначені основні змінні задачі, здійснюючі суттєвий вплив на вибраний критерій, враховані обмеження на змінні і створена модель, установлюючи взаємозв'язок між критерієм, змінними і обмеженнями [5, 6]. Постановка задачі в основному визначає і методи її вирішення, які можуть грунтуватись або на виборі варіантів, або на спеціальних алгоритмах [8].

Нехай, за результатами ведення попередньої радіорозвідки ліній зв'язку ТП транспортної платформи Національної телекомунікаційної мережі противником визначено, що способи застосування засобів РП можуть бути розроблені на основі k типів засобів радіоподавлення та ЕМП.

Противник під час підготовки та ведення гібридних дій (терористичної діяльності) ставить завдання зірвати державне управління у певному територіальному районі України, що залежить від масштабів та завдань операції. При цьому, в залежності від масштабів гібридних дій, противник вирішує j часткових завдань $Z_1, Z_2, ..., Z_m$, $j = 1,2,...,m$. Зокрема, під час ведення гібридних бойових дій завданнями можуть полягати в наступному:

Наприклад, здійснення за єдиним замислом та планом радіоподавлення та ЕМП засобів ТП транспортної платформи Національної телекомунікаційної мережі в наступних просторових масштабах (рис.1):

($j = 1$) – до 100 км від лінії розмежування;

($j = 2$) – до 250 км від лінії розмежування;

($j = 3$) – до 500 км від лінії розмежування

($j = 4$) – на всю глибину території України.

При цьому вважається, що завдання з подавлення інших видів зв'язку в інтересах державного управління виконані.

В рамках вирішення кожного j-го завдання за результатами попередньої радіорозвідки противником викрито n_j типів функціонально незалежних елементів ТП транспортної платформи Національної телекомунікаційної мережі – об'єктів радіоподавлення та ЕМП. Q_{jz} – загальна кількість об'єктів z-го типу (терміналів ТП), $z = 1,2,...,n_j$. Кожен об'єкт організовує одну радіолінію ТП, яка за ТТХ термінала є багатоканальною і в залежності від ланки управління включає в себе від одиниць до десятків радіоканалів.

На рис.1 пунктиром показані радіолінії, які організовані об'єктами РЕБ на глибину завдання Z_j, j = 1, 2, 3 та 4 відповідно.

За результатами оцінки радіоелектронної обстановки (РЕО) визначена загальна кількість

радіоканалів U_j, яка організована на всіх об'єктах z типів, що можуть бути об'єктами РП та ЕМП противника при виконанні j-го завдання. $U_j = \sum_{z=1}^{n_j} Q_{jz} \cdot A_{jz}$, де A_{jz} – кількість радіоканалів, організованих однією радіолінією об'єкта z-го типу при виконанні противником j-го завдання.

За результатами воєнно-економічного аналізу необхідно сформувати матрицю $\|C_{jzk}\|$ економічних витрат РП та ЕМП однієї лінії ТП транспортної платформи Національної телекомунікаційної мережі об'єкта z-го типу при виконанні j-го завдання засобами РЕБ k-го типу (див. рис. 1).

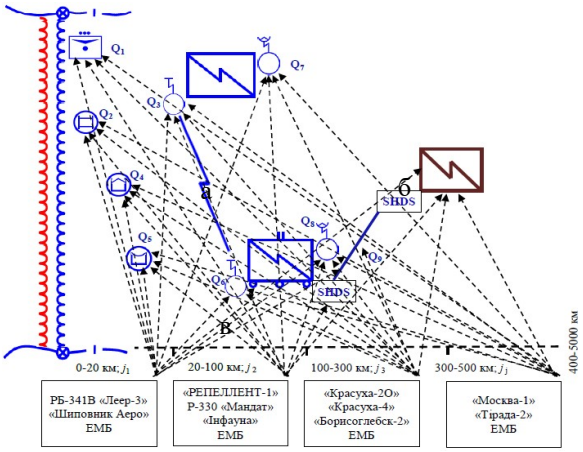

Рисунок 1. Вихідні дані щодо постановки задачі оптимального розподілу неоднорідних засобів РП та ЕМП транспортної платформи Національної телекомунікаційної мережі для ведення гібридних дій (терористичної діяльності) противником

Ефективність виконання противником завдань $Z_1, Z_2, ..., Z_m$ відповідно оцінимо за показником $U_j^{\text{п}}$ – загальна кількість каналів транспортної платформи Національної телекомунікаційної мережі, яку необхідно подавити під час виконання j-го завдання, де $U_j^{\text{п}} = \sum_{z=1}^{n_j} Q_{jz}^{\text{п}} \cdot A_{jz}$, $Q_{jz}^{\text{п}}$ – кількість подавлених противником ліній (об'єктів) транспортної платформи Національної телекомунікаційної мережі z-го типу при вирішенні j-го завдання.

Тоді, критерій для оцінки ефективності порушення інформаційного обміну в транспортної платформи Національної телекомунікаційної мережі шляхом РП та ЕМП противником її елементів при виконанні часткового завдання Z_j має вигляд:

$$U_j^{\text{п}} \geq U_j^{\text{кр}}, \qquad (1)$$

де $U_j^{\text{кр}}$ – критична кількість подавлених каналів ТП НТМ, при якій досягається потрібний рівень порушення інформаційного обміну у транспортної платформи Національної телекомунікаційної мережі.

Для вирішення завдань $Z_1, Z_2, \ldots Z_m$ під час ведення гібридних дій (терористичної діяльності) необхідно сформувати оптимальний набір $S_{\text{опт}} = \|Q_{jzk}^{\text{п}}\|$ об'єктів ТП НТМ z-го типу, що подавляються відповідними засобами РЕП противника k-го типу при вирішенні j-го завдання, який забезпечує для противника мінімізацію економічних витрат реалізації способу бойового застосування засобів РЕП транспортної платформи Національної телекомунікаційної мережі під час ведення гібридних дій (терористичної діяльності) при одночасному виконанні вимог до ефективності процесу РЕП (оптимізація за критерієм "вартість – ефективність"). Критерій ефективність вартість не є єдиним можливим підходом та обраний для прикладу як найбільш розповсюджений. Також на практиці поставники задачі доцільно також застосовувати критерії "складність виконання бойового завдання – ефективність" [6], або "вартість – складність виконання бойового завдання – ефективність" [5]. Формалізація постановки задачі оптимізації для цих критеріїв виходить за рамки роботи та буде вирішена авторами в окремій публікації.

Математична трактовка задачі оптимального розподілу неоднорідних засобів РП та ЕМП елементів транспортної платформи Національної телекомунікаційної мережі противником в гібридних діях (терористичній діяльності) за критерієм "ефективність-вартість" може бути конкретизована до вигляду:

$$S_{\text{опт}}(Q_{jzk}^{\text{п}}) = min\left\{\sum_{j=1}^{m}\sum_{z=1}^{n_j}\sum_{k=1}^{\nu} C_{jzk} \cdot Q_{jzk}^{\text{п}}\right\} \qquad (2)$$

при обмеженнях на параметри цільової функції:

$$\sum_{z=1}^{n_j}\sum_{k=1}^{\nu} A_{jz} \cdot Q_{jzk}^{\text{п}} \geq U_j^{\text{кр}},\ j = 1, 2, ..., m,\ z = 1, 2, ..., n_j, \qquad (3)$$

$$Q_{jzk}^{\text{п}} = 1, 2, ..., Q_{jzk}, \qquad (4)$$

$$C_{jzk} \geq 0,\ k = 1, 2, ... \nu. \qquad (5)$$

Аналіз (2)–(5) дозволяє зробити висновок, що задачі оптимального розподілу неоднорідних засобів РП та ЕМП по елементах транспортної платформи Національної телекомунікаційної мережі в гібридних діях (терористичній діяльності) за критерієм "вартість – ефективність" відноситься до багатоіндексної двоякої цілочисельної зворотної задачі лінійного програмування [8]. Метод мінімізації (2) суттєво визначається її мірністю та характером сукупності обмежень типу (3)–(5). Підходи до вирішення зворотних двоякої задач досліджені в [8]. Однак результати отримані або в умовах розподілу однорідного ресурсу або невисокої індексності (не більше 2) цільової функції та їх використання для отримання однозначного розв'язання задачі типу (2)–(5) утруднено.

Одним із підходів до зняття виникаючих протиріч є пониження мірності цільової функції (2). В результаті чого, формується матриця економічних витрат, яка приводиться до матриці-строки C_z шляхом згортання за правилом, згідно з яким, з елементів кожного z-го стовпця матриці $\|C_{jzk}\|$ обирається мінімальний та його значення присвоюється відповідному елементу матриці-строки C_z^k зі збереженням індексу z, де верхній індекс k є типом засобу РП, ЕМП, що чисельно дорівнює номеру рядка в якому знаходився мінімальний для z-го стовпця елемент матриці $\|C_{jzk}\|$.

В результаті запропонованого підходу задача (2)–(5) спрощується до вигляду:

$$S_{\text{опт}}(Q_z^{\text{п}}) = min\left\{\sum_{z=1}^{n_j} C_z^k \cdot Q_z^{\text{п}}\right\}, \qquad (6)$$

при обмеженнях:

$$\sum_{z=1}^{n_j} A_{jz} \cdot Q_z^{\text{п}} \geq U_j^{\text{кр}},\ j = 1, 2, ..., m, z = 1, 2, ..., n_j, \quad (7)$$

$$Q_z^{\text{п}} = 1, 2, ..., Q_z, \qquad (8)$$

$$C_z^k \geq 0, k = 1, 2, ..., \nu. \qquad (9)$$

Фізична трактовка задачі типу (6)–(9) є наступною. Необхідно знайти потрібну кількість ліній транспортної платформи Національної телекомунікаційної мережі z-го типу $Q_z^{\text{п}}$, які будуть подавлятись засобами РП та ЕМП k-го типу противника. Кожна лінія z-го типу складається з A_{jz} каналів транспортної платформи Національної телекомунікаційної мережі при вирішенні j-го завдання відповідно. На кількість ліній ТП НТМ, яку противником буде подавлено при вирішенні j-го завдання, накладено обмеження зверху – максимальна кількість ліній , яку можуть розгорнути всі розвідані об'єкти РЕП z-го типу та знизу – мінімальна кількість ліній ТП НТМ, яку необхідно подавити.

Аналіз методів вирішення задач типу (6)–(9) [8] дозволяє побудувати алгоритм її вирішення на основі методу нормованих функцій, з його адаптацією в бік врахування наявності відносно класичних підходів додаткових обмежень типу $Q_z^{\text{п}} = 1, 2, ..., Q_z$, блок 14. Це обмеження дозволяє виключити випадки призначення засобів РП та ЕМП на термінали ТП НТМ, кількість яких перевищує кількість розгорнутих терміналів (див. рис. 2).

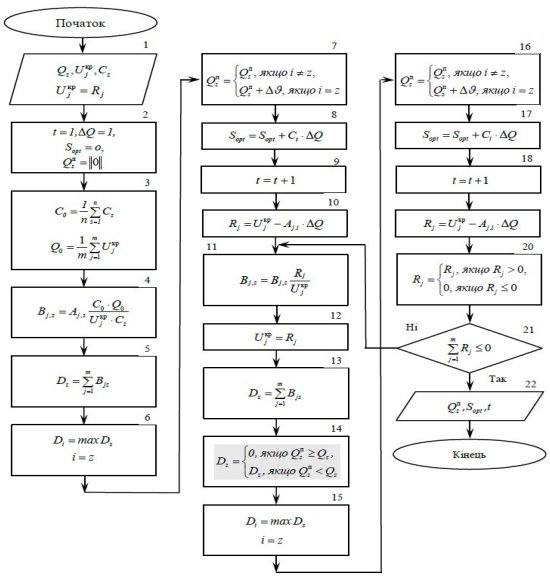

Рисунок 2. Алгоритм вирішення задачі оптимального розподілу противником неоднорідних засобів РП та ЕМП по елементах ТП НТМ адаптованим методом

Висновки і перспективи подальших досліджень

Аналіз результатів (5)–(9) показав, що для розробки способів РП та ЕМП ТП НТМ та створення моделі завадової обстановки в умовах ведення гібридних бойових та терористичних дій проти України необхідно розробити відповідну методику за наступними етапами:

1) обрати (розробити) сукупність методів вирішення задачі оптимізації розподілу ресурсу, що використовується для реалізації способів РП та ЕМП ТП НТМ противником в операціях;

2) формалізувати показники та удосконалити порядок обґрунтування обмежень на критерії ефективності порушення інформаційного обміну у ТП НТМ в операціях;

3) визначити порядок формування та оцінки елементів матриці економічних показників для практичної реалізації способів РП та ЕМП ТП НТМ противником;

4) визначити порядок оцінки ресурсу, що використовується для реалізації способів РП та ЕМП ТП НТМ противником.

Література

1. "Про основні засади забезпечення кібербезпеки України" : Закон України від 21 червня 2018 року N 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. **2. О. Черниш**. Основи формування нової ідеології ведення радіоелектронної боротьби у війнах і збройних конфліктах майбутнього / О. М. Черниш, С. О. Тищук, С. М. Шолохов // *Наука і оборона. – 2006.* – № 4. – С. 48–51. **3. С. Тищук.** Електромагнітна зброя / С. О. Тищук, С. М. Шолохов //*Волонтер. – 2005.* – № 5 (37). – С. 18–21. **4. К. Фомичев** Электромагнитное оружие. Перспективы применения в информационной борьбе/ Константин Фомичев, Леонид Юдин // *Электроника: Наука, Технология, Бизнес. – 1999.* – № 6, С. 40–44. **5. Г. Певцов.** Наукові основи обґрунтування способів бойового застосування сил та засобів радіоелектронного подавлення в операціях / Г. В. Певцов, С. М. Шолохов, Г. М. Тіхонов, І. М. Тіхонов // *Системи управління, навігації та зв'язку. – 2008.* – № 3(7). – С. 120–125 у ЦНДІ навігації і управління. **6**. **А. Воронин.** Многокритериальный синтез динамических систем / А. Н. Воронин – К.: *Наук. думка,* 1992. – 160 с. – АН Украины. Ин-т кибернетики. им. В. М. Глушакова.

7. В. Космодемьянский. Математические методы оптимизации / В. А. Космодемьянский– М.: 1967. – 96 с. – (МО СССР). **8. Е. Берзин.** Оптимальное распределение ресурсов и элементы синтеза систем / Е. А. Берзин ; под ред. Е. В. Золотова – М.: *Сов. радио*, 1974. – 303 с.

ПОСТАНОВКА ЗАДАНИЯ ОПТИМАЛЬНОГО РАСПРЕДЕЛЕНИЯ РЕСУРСА НЕОДНОРОДНЫХ СРЕДСТВ ДИСТРУКТИВНОГО ВЛИЯНИЯ НА ЕЛЕМЕНТЫ ПЛАТФОРМЫ НАЦИОНАЛЬНОЙ ТЕЛЕКОМУНИКАЦЙННОЙ СЕТИ В ОСОБЫЙ ПЕРИОД

Григорий Митрофаныч Тихонов *(кандидат воєнных наук, с.н.с.)* [1]
Сергей Николаевич Шолохов *(кандидат технических наук, доцент)* [2]
Богдан Анатольевич Николаенко *(кандидат технических наук)* [2]
Валерий Николаевич Тютюнник[1]

[1]*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*
[2] *Национальный техничечкий университет Украины "Киевський политехнический институт имени Игоря Сикорського" Украина*

Помехозащита системы связи єсть актуальным и важным направлением исследований, методология оценки влияния на него средств радио та електромагнитного подавления, на сегодняшний день, достаточно развита та известна. Национальная телекомуникационная сеть, как сукупность систем и сетей связи, в условиях ведения гибридной войны против Украины требует усовершенствования способов ее защиты от деструктивного влияния противника, что имеет на вооружении новейшие средства радио подавления та електромагнитного влияния. Незащищенная национальная телекомуникационная сеть не в состоянии выполнить основную свою функцию, а именно циркуляцию (передача, прийом, создание, обробку, хранение) та защиту национальных информационных ресурсов, обеспечение телекомуникационных (мультисервисных) услуг в интересах осуществления управления государством в мирное время, в условиях чрезвычайного положения и в особый период, и которая является сетью (системой) двойного назначения с использованием части ее ресурсов для предоставления услуг, вчасности с киберзащиты, другим потребителям. Качественная разработка способов та методов обеспечения помехозащиты елементов национальная телекомуникационная сеть невозможна без прогнозирования возможных сценариев действий противника и обстановки, что может сложиться.

Данный момент времени характеризуєтся принципиальными изменениями в условиях использования транспортной платформы национальной телекомуникационной сети в условиях ведения гибридной войны Росийської Федерации против Украины. Проведенный анализ показал, что в случае обострения ситуации на фронте, перехода противника к широкомасштабной вооруженной агресии или терористических действий ресурс транспортной платформы национальной телекомуникационной сети есть одним из первоочередных объектов влияния новейших средств радиоелектронного та електромагнитного подавления воинских частей (подразделений) РЕБ российско - терористических войск.

Проведено постановку задачи рационального распределения ресурса неоднородных средств радиоелектронной боротьбы противника по елементам транспортной платформы национальной телекомуникационной сети для дальнейшей разработки методики определения способов ее радиоелектронного подавления и создание модели радиоелектронной обстановки в условиях ведения гибридных, боевых та терористических действий противником против Украины.

Ключевые слова: *многокритериальная оптимизация, диструктивное влияние, радиоелектронная борьба, електромагнитное влияние, транспортная платформа, сценарий действий, помеховая обстановка, терористические дейтвия, гибридная война.*

PROBLEMS STATEMENT OF RATIONAL DISTRIBUTION OF MISCELLANEOUS WAYS OF INFORMATION WARFARE OF ENEMY BY TRANSPORT PLATFORM ELEMENTS OF NATIONAL TELECOMMUNICATION NETWORK FOR WAYS DEFINITION OF ITS RADIO-ELECTRONIC SUPPRESSION

Grigorii Tikhonov *(Candidate of military sciences, senior researcher)*[1]
Serhii Sholokhov *(Candidate of technical sciences, docent)*[2]
Bohdan Nikolaienko *(Candidate of technical sciences)*[2]
Valerii Tiutiunnyk[1]***,***

[1]*National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine*
[2]*National Technical University of Ukraine Polytechnic Institute named after Igor Sikorsky, Kyiv, Ukraine*

Interference protection of the communication system is a relevant and important area of research, the methodology for assessing the impact of radio and electromagnetic suppression on it is currently well developed and known. The national telecommunication network as a set of communication systems and networks in the context of a hybrid war against Ukraine needs to improve ways to protect it from the destructive influence of the enemy, which is equipped with the latest radio suppression and electromagnetic. Unprotected national telecommunication network will not be able to perform its main function, namely the circulation (transmission, reception, creation, processing, storage) and protection of national information resources, providing secure electronic communications, providing a range of modern secure information and communication (multiservice) services in the interests of government in peacetime, in a state of emergency and in a special period, and which is a dual-purpose network (system) using part of its resources to provide services, including cyber security, to other consumers. Qualitative development of methods and techniques to ensure noise immunity of national telecommunication network elements is impossible without predicting possible scenarios of enemy action and the noise situation that may arise.

The current moment of time is characterized by fundamental changes in the conditions of application of the transport platform of the national telecommunication network in the conditions of conducting a hybrid war of the Russian Federation against Ukraine. The analysis showed that in case of aggravation of the situation at the front, transition of the enemy to large-scale armed aggression or terrorist acts, the resource of transport platform of the national telecommunication network is one of the primary objects of influence of the latest means of electronic and electromagnetic suppression of units (units) of Russian terrorist forces.

The problem of rational distribution of the resource of inhomogeneous means of electronic warfare of the enemy on the elements of transport platform of the national telecommunication network for further development of methods for determining ways of its electronic suppression and creating a model of electronic situation in hybrid, combat and terrorist actions against Ukraine.

Keywords: *multicriteria optimization, destructive influence, electronic warfare, electromagnetic influence, transport platform, action scenario, disturbance, terrorist actions, hybrid war.*

References

1. "On the basic principles of cyber security of Ukraine": Law of Ukraine of June 21, 2018 N 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. O. Chernysh. Chernysh, SO Tyschuk, SO Sholokhov // Nauka i oborona [Fundamentals of the formation of a new ideology of electronic warfare in wars and armed conflicts of the future]. - 2006. - № 4. - P. 48–51. **3. S. Tishchuk.** Electromagnetic weapons / SO Tishchuk, SM Sholokhov // Volunteer. - 2005. - № 5 (37). - P. 18–21. **4. K. Fomichev** Electromagnetic weapons. Prospects for application in the information struggle / Konstantin Fomichev, Leonid Yudin // Electronics: Science, Technology, Business. - 1999. - № 6, S. 40–44. **5. G. Pevtsov.** GV Pevtsov, SM Sholokhov, GM Tikhonov, IM Tikhonov // Control systems, navigation and communication. - 2008. - № 3 (7). - P. 120–125 in the Central Research Institute of Navigation and Control. **6. A. Voronin.** Multicriteria synthesis of dynamical systems / AN Voronin - K .: Nauk. opinion, 1992. - 160 p. - Academy of Sciences of Ukraine. Inst. Of Cybernetics. them. VM Glushakov. **7. V. Kosmodemyansky.** Mathematical methods of optimization / VA Kosmodemyansky - M .: 1967. - 96 p. - (Ministry of Defense of the USSR). **8. E. Berzin.** Optimal resource distribution and elements of systems synthesis / EA Berzin; under ed. EV Zolotova - M .: Owls. radio, 1974. - 303 p.

DOI:**10.33099/2311-7249/2021-41-2-17-22**

УДК [001.8/.816/.817] + 001.92 + [371.315.5/.315.6/.335] +655.52

Леся Михайлівна Козубцова *(кандидат технічних наук)*[1]
Юрій Іванович Хлапонін *(доктор технічних наук, професор)*[2]
Ігор Миколайович Козубцов *(доктор педагогічних наук, старший науковий співробітник)*[1]

[1]***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[2]***Київський національний університет будівництва і архітектури, Київ, Україна***

МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ВИКОНАННЯ ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЙ

В науковій статті обґрунтовано методику оцінювання ефективності виконання заходів, спрямованих на забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури організацій. Дана робота є продовженням дослідження з попереднього опису "Майбутнє безпекове середовище 2030", розширюючи наукові межі щодо реалізації невідкладних заходів державної політики з нейтралізації загроз кібербезпеки організацій. Необхідність статті обумовлена раціональним вибором та застосуванням заходів, спрямованих на забезпечення кібернетичної безпеки об'єктів інформаційної інфраструктури організацій. Встановлено, що на практиці оцінити ефективність виконання заходів, спрямованих на забезпечення кібернетичної безпеки можна через наступні показники (ймовірності): ризик кібернетичної безпеки, кіберзахищеність, функціональна працездатність системи об'єкта критичної інформаційної інфраструктури, кіберстійкість. Для застосування принципу наступності в статті під удосконалену онтологію кібербезпеки обрано показник (ймовірність) ризику кібернетичної безпеки. Методика оцінки ризику кібербезпеки об'єктів критичної інформаційної інфраструктури організацій базується на визначенні ймовірності реалізації кібератак, а також рівнів їх збитку. Методика включає наступні етапи: етап розробки системи показників оцінювання ефективності виконання заходів; етап планування процедур збирання вихідних даних для оцінювання ефективності виконання заходів; етап обчислення значення показника ефективності виконання заходів; етап інтерпретації значення показника ефективності виконання заходів, спрямованих на забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури організацій. Вихідні значення для розрахунку кіберзахищеності отримують за результатами аудиту об'єктів критичної інформаційної інфраструктури організацій. При розрахунку значень ймовірності кібератак, а також рівня можливого збитку слід скористатися статистичними методами, експертними оцінками або елементами теорії прийняття рішень. Наукова новизна одержаного результату полягає в тому, що вперше запропоновано методику оцінювання ефективності заходів кібербезпеки за показником (ймовірності) ризику кібербезпеки, яка доповнюватиме методику планування заходів кібербезпеки об'єктів критичної інформаційної інфраструктури організацій.

Ключові слова: *методика, оцінювання, ефективність, заходи, кібербезпека, об'єкт критичної інформаційної інфраструктури, організація.*

Вступ

Постановка проблеми. Кібернетична безпека (кібербезпека) – стан захищеності критичних об'єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування і розвиток, своєчасне виявлення, запобігання і нейтралізація кібернетичних загроз в інтересах людини, суспільства, держави. На підставі положень Стратегії національної безпеки України, Воєнної доктрини України та Концепції розвитку сектору безпеки і оборони України визначено оперативну ціль «1.5. Удосконалення системи кібербезпеки та захисту інформації» [1, с. 33], Закону України "Про основні засади забезпечення кібербезпеки України" [2]; Стратегії кібербезпеки України [3]; Рішення Ради національної безпеки і оборони України від 10.07.17 "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року" "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" [4] встановлено, що на даний час на існуючих об'єктах критичної інфраструктури організацій відсутня методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури організацій за запропонованою методикою планування [5]. Однак залишається актуальним питанням з'ясувати за якими критеріями та показниками оцінити ефективність заходів і якого досягається рівня кібербезпеки ОКІІ організації виходячи із онтології поданої на рис. 1 [6]. Тому, на підставі [1-4] виникає об'єктивне наукове завдання щодо необхідності обґрунтування методики оцінювання ефективності виконання заходів забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури організацій.

Аналіз останніх досліджень і публікацій. Дана робота є логічним продовженням дослідження з попереднього опису "Майбутнє безпекове середовище 2030" [7] розширюючи наукові межі щодо реалізації невідкладних заходів державної політики з нейтралізації загроз кібербезпеки організацій [4].

В роботі [8] подана методологія оцінки ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури. Спроба її застосувати на практиці у Військовому інституту телекомунікацій та інформатизації імені Героїв Крут виявилась складною в обчислюванні. На відміну від цієї роботи в [9] подано методика оцінки ризиків інформаційної безпеки розрахована для підприємств малого та середнього бізнеса. Процес оцінки ризиків інформаційної безпеки ґрунтується на використанні методів оцінки ризиків економічної безпеки.

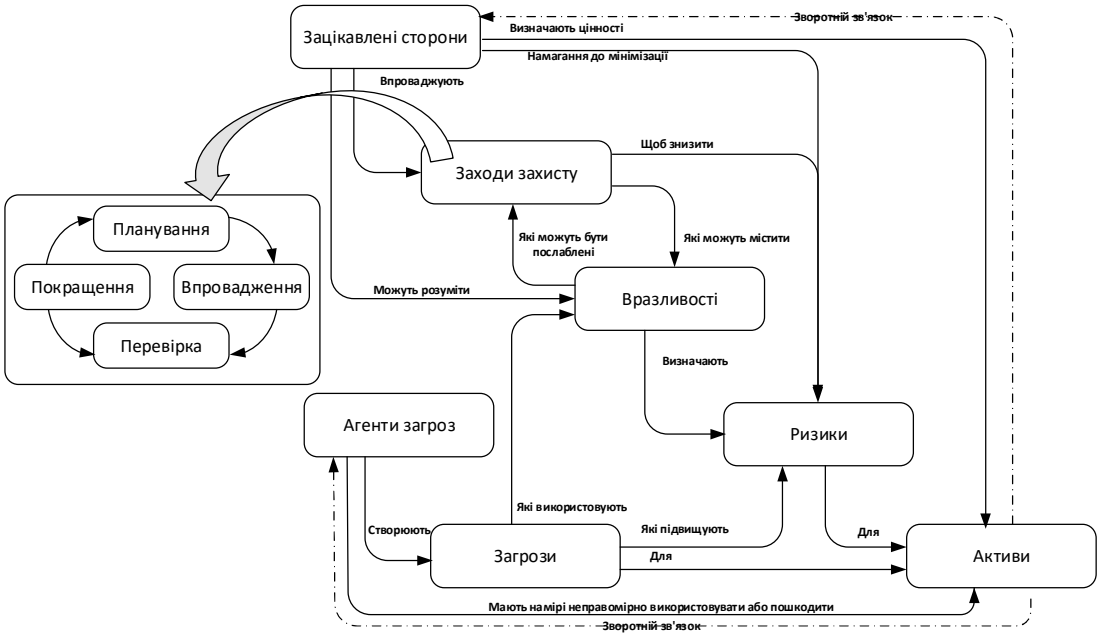

Рисунок 1. Структурна залежність заходів та ризиків у онтології кібербезпеки

Необхідність у методиці оцінювання ефективності виконання заходів забезпечення кібербезпеки ОКІІ організацій обумовлена нестабільністю у часі кібербезпеки на зазначених об'єкта та ризиком втрати активів.

Тому, виходячи з підстав, що перелічені в роботах [8; 9] методики не враховують показник кіберзахищеності $P_{КЗ}(S)$, автори вважають за потребу запропонувати науковому суспільству до обговорення методику оцінювання ефективності виконання заходів забезпечення кібербезпеки ОКІІ організацій на засадах кіберзахищеності.

Мета статті. Апробувати структуру методики оцінювання ефективності виконання заходів забезпечення кібербезпеки ОКІІ організацій.

Виклад основного матеріалу дослідження.

Вихідним положення нашого дослідження є запропонована методика планування заходів кібербезпеки ОКІІ організації [5]. Для неї визначимо логічний етап оцінювання ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації. У її структури логічним місцем є етап «9 Оцінювання ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації».

Для об'єктивності оцінювання ефективності виконання заходів кібербезпеки ОКІІ організації необхідно визначити сукупність показників та критеріїв оцінювання. Для цього скористаємося наступними рекомендаціями щодо формування показників та критеріїв оцінювання ефективності заходів кібербезпеки ОКІІ організації.

Розпочинати роботу з формування системи показників слід лише після того, як буде з'ясовано, що саме ми прагнемо виміряти та для чого це необхідно робити.

Зазвичай, потреба у формуванні системи показників пов'язана із здійсненням оцінювання ефективності заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації для забезпечення зворотного зв'язку. Результати оцінювання дають інформацію для прийняття рішення про те, чи варто продовжувати експлуатувати ОКІІ чи її варто припинити та обрати інші заходи для покращення кіберзахищеності.

Одним з відповідальних завдань, що покладається на експертну групу є складання актуального та адекватного переліку показників (індикаторів) та критеріїв для оцінювання ефективності заходів кібербезпеки ОКІІ організації.

Кількість індикаторів $I_{КЗ}$ для різних компонентів засобів Z_i є різною.

В сучасній теорії та практиці оцінювання ефективності заходів використовують різні показники та у відповідності ним критерії в залежності від наявних вихідних даних. Тому це питання актуальне і для оцінювання ефективності заходів кібербезпеки ОКІІ організації.

Перелічимо найбільш вживані показники оцінювання ефективності виконання заходів, спрямованих на забезпечення кібербезпеки через показник (ймовірність): ризику кібербезпеки [8]; кіберзахищеності [10]; функціональної працездатності системи (ОКІІ) [11]; кіберстійкості [12]. Вибір тих чи інших зазначених показників оцінювання ефективності виконання заходів залежить від наявних вихідних даних у експертів.

У випадку здійснювання процедури оцінювання ефективності виконання заходів,

спрямованих на забезпечення кібербезпеки через показник (ймовірність) кіберзахищеності, то вихідні дані отримуються за результатом обчислювання значення кіберзахищеності за методикою [10].

Згідно удосконаленої онтології кібербезпеки поданої на рис. 1 [6], виникає необхідність здійснювання процедури оцінювання ефективності виконання заходів, що спрямовані на забезпечення кібербезпеки ОКІІ через показник (ймовірності) ризику кібербезпеки або ймовірних наслідків впливу на активи організації. І тоді логічним є постановка завдання на вирішення зворотної задачі з пошуку оптимальних заходів які несуть мінімальний ризик. Отже, зменшення ризику можливо досягнути за рахунок додаткових організаційних і технічних засобів захисту, що дозволяють знизити ймовірність проведення кібератаки або зменшити можливі збитки від неї.

Ухилення від ризику шляхом зміни архітектури або схеми інформаційних потоків ОКІІ, що дозволяє виключити проведення тієї чи іншої атаки. Наприклад, фізичне відключення від Інтернету сегмента ОКІІ, в якому обробляється конфіденційна інформація, дозволяє уникнути зовнішніх атак на конфіденційну інформацію.

Прийняття ризику, якщо він зменшений до того рівня, на якому вже не становить небезпеку для ОКІІ організації.

При виборі заходів для підвищення рівня захисту ОКІІ враховується одне принципове обмеження – вартість реалізації цих заходів не повинна перевищувати вартості захищених інформаційних ресурсів, а також збитків організації від можливого порушення конфіденційності, цілісності або доступності інформації.

Виходячи із вище розглянутого в статті пропонується здійснювати процедуру оцінювання ефективності виконання заходів забезпечення кібербезпеки через показник (ймовірності) ризику кібербезпеки.

Критерії оцінки ймовірності ризику кібербезпеки ОКІІ $P_{R(ДІВ)}$ подано в табл. 1.

Вихідні значення для розрахунку кіберзахищеності отримують за результатами аудиту ОКІІ, а обчислення здійснюють за формулами методики [10].

В табл. 2 – 4 наведені критерії оцінки ризиків кібербезпеки, в яких для оцінки рівнів збитків та ймовірності кібератаки використовується п’ять понятійних рівнів.

Таблиця 1

Критерії оцінки ймовірності ризику кібербезпеки ОКІІ

№ п/п	Критерій	Ймовірність $P_{R(ДІВ)}$	Опис
1	$0 \le P_{R(ДІВ)} \le 0{,}25$	Дуже низький	Дуже низький рівень ризику
2	$0{,}25 \le P_{R(ДІВ)} \le 0{,}5$	Низький	Низький рівень ризику
3	$0{,}5 \le P_{R(ДІВ)} \le 0{,}75$	Середній	Середній рівень ризику
4	$0{,}75 \le P_{R(ДІВ)} \le 0{,}9$	Високий	Високий рівень ризику
5	$0{,}9 \le P_{R(ДІВ)} \le 1$	Дуже високий	Дуже високий рівень ризику

Таблиця 2

Критерії оцінки кіберзахищеності ОКІІ

№ п/п	Критерій	Рівень	Опис
1	$0 \le P_{КЗ}(S) \le 0{,}25$	незадовільний	Вибрані заходи кібербезпеки ОКІІ забезпечують незадовільний рівень кіберзахищеності, підлягає негайному припиненню експлуатація ОКІІ.
2	$0{,}25 \le P_{КЗ}(S) \le 0{,}5$	низький	Вибрані заходи кібербезпеки ОКІІ забезпечує низький рівень кіберзахищеності
3	$0{,}5 \le P_{КЗ}(S) \le 0{,}75$	середній	Вибрані заходи кібербезпеки ОКІІ забезпечує середній рівень кіберзахищеності
4	$0{,}75 \le P_{КЗ}(S) \le 0{,}9$	високий	Вибрані заходи кібербезпеки ОКІІ в цілому забезпечує високий рівень кіберзахищеності
5	$0{,}9 \le P_{КЗ}(S) \le 1$	найвищий	Вибрані заходи кібербезпеки ОКІІ забезпечують найвищий рівень кіберзахищеності.

Таблиця 3

Критерії оцінки рівня збитків $Z_{(ДІВ)}$

№ п/п	Критерій	Рівень збитку $Z_{(ДІВ)}$	Опис
1	$0 \le Z_{(ДІВ)} < 0{,}25$	Малий	Незначні втрати матеріальних активів, які швидко відновлюються або незначні наслідки для організації
2	$0{,}25 \le Z_{(ДІВ)} < 0{,}5$	Помірний	Помітні втрати матеріальних активів або помірні наслідки
3	$0{,}5 \le Z_{(ДІВ)} \le 0{,}75$	Середній	Суттєві втрати матеріальних активів або значна шкода
4	$0{,}75 \le Z_{(ДІВ)} \le 0{,}9$	Великий	Великі втрати матеріальних активів і велика шкода для організації
5	$0{,}9 \le Z_{(ДІВ)} \le 1$	Критичний	Критична або повна втрата матеріальних активів організації

Таблиця 4

Критерії оцінки ймовірності проведення ДІВ $P_{(ДІВ)}$

№ п/п	Критерій	Ймовірність $P_{(ДІВ)}$	Опис
1	$0 \le P_{(ДІВ)} \le 0{,}25$	Дуже низька	ДІВ практично ніколи не буде проведений
2	$0{,}25 \le P_{(ДІВ)} \le 0{,}5$	Низька	Ймовірність проведення ДІВ досить низький
3	$0{,}5 \le P_{(ДІВ)} \le 0{,}75$	Середня	Ймовірність проведення ДІВ середній
4	$0{,}75 \le P_{(ДІВ)} \le 0{,}9$	Висока	ДІВ швидше за все буде проведений
5	$0{,}9 \le P_{(ДІВ)} \le 1$	Дуже висока	ДІВ буде проведена

Методика оцінювання ефективності виконання заходів. Методика оцінки ризику кібербезпеки ОКІІ базується на визначенні ймовірності реалізації кібератак (ДІВ), а також рівнів їх збитку. Розробка та застосування в діяльності системи виміру оцінювання

ефективності виконання заходів відбувається за такими основними етапами [13, с. 33 – 35]:

Етап 1. Розробка системи показників оцінювання ефективності виконання заходів. Цей етап пов'язаний із процесом вибору показників та визначення системи міри.

Етап 2. Планування процедур збирання вихідних даних для оцінювання ефективності виконання заходів. На цьому етапі здійснюється підготовка до впровадження системи вимірювання значень показників, з плануванням доступу до необхідних даних, розробкою конфігурації обробки та розповсюдження інформації про значення показників.

Етап 3. Обчислення значення показника ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ.

Значення ризику обчислюється окремо для кожної кібератаки (ДІВ) і в загальному випадку представляється, як добуток ймовірності проведення кібератаки (ДІВ) на величину можливого збитку від цієї атаки (1):

$$P_{R(\text{ДІВ})} = P_{\text{ДІВ}} \times Z_{\text{ДІВ}} \quad (1)$$

де $P_{\text{R(ДІВ)}}$ – ймовірність ризику кібербезпеки ОКІІ;

$P_{(\text{ДІВ})}$ – ймовірність проведення кібератаки (ДІВ) на ОКІІ;

$Z_{(\text{ДІВ})}$ – збитки активів спеціальних користувачів від успішної проведеної кібератаки (ДІВ) на ОКІІ.

Обчислення ймовірності проведення кібератаки $P_{(\text{ДІВ})}$ для всієї системи S ОКІІ здійснимо за формулою (2):

$$P_{\text{ДІВ}} = 1 - P_{\text{КЗ}}(S) \quad (2)$$

тоді $P_{\text{R(ДІВ)}}$ з урахуванням (2) матимемо (3):

$$P_{R(\text{ДІВ})} = (1 - P_{\text{КЗ}}(S)) \times Z_{\text{ДІВ}}. \quad (3)$$

У методиці можуть використовувати кількісні або якісні шкали для визначення величини ризику кібербезпеки, але пропонується обирати числові вирази. При використанні кількісних шкал ймовірність проведення ДІВ приймаємо числові значення в інтервалі $P_{(\text{ДІВ})} \in [0, 1]$, а збиток $Z_{(\text{ДІВ})}$ може задаватися у вигляді грошового еквівалента матеріальних втрат, які користувачі організації понесуть у випадку успішного пропуску ДІВ.

Етап 4. Інтерпретація значення показника ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації.

Цей етап включає практичну роботу з обробки, аналізу та інтерпретації даних для прийняття рішень щодо посилення обраних заходів. Для інтерпретації рівня ризику за якісною шкалою застосуємо таблицю, в якій у першому стовпці задаємо понятійні рівні $Z_{(\text{ДІВ})}$, а в першому рядку – рівні ймовірності кібернетичного ДІВ $P_{(\text{ДІВ})}$. Комірки таблиці, розташовані на перетині відповідних рядків і стовпців, що містять рівень ризику безпеки $P_{\text{R(ДІВ)}}$ (табл. 5). В таблиці введено наступні умовні скорочення: Н – низький рівень ризику; С – середній рівень ризику; В – високий рівень ризику.

При розрахунку значень ймовірності кібератак (ДІВ), а також рівня можливого збитку слід скористатися статистичними методами, експертними оцінками або елементами теорії прийняття рішень. Статистичні методи передбачають аналіз накопичених даних пов'язаних з порушенням кібербезпеки. Проте статистичні методи не завжди вдається застосувати через брак статистичних даних про раніше проведені атаки на ресурси ОКІІ.

При використанні апарату експертних оцінок аналізуються результати роботи групи експертів, компетентних в області кібербезпеки, які на основі наявного у них досвіду визначають кількісні або якісні рівні ризику.

Елементи теорії прийняття рішень дозволяють застосовувати для обчислення значення ризику безпеки більш складні алгоритми обробки результатів роботи групи експертів.

Висновки й перспективи подальших досліджень

В сучасній теорії та практиці для оцінювання ефективності заходів, найчастіше застосовують показник (ймовірність): ризику кібербезпеки, кіберзахищеності, функціональної працездатності системи (ОКІІ), кіберстійкості. Складність застосування математичного апарату оцінювання ефективності заходів, через показник (ймовірність): ризику кібербезпеки, функціональної працездатності системи (ОКІІ) та кіберстійкості змусило до пошуку і підходу до розрахунку через показник кіберзахищеності.

Визначено сукупність показників та критеріїв для оцінювання ефективності заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації. В запропонованій методиці оцінювання ефективності виконання заходів здійснюється за показником кіберзахищеності ОКІІ організації та ризику.

На основі обраного показника та критеріїв обґрунтована структура методики оцінювання ефективності виконання заходів кібербезпеки.

Наукова новизна одержаного результату полягає в тому, що для (обчислювання) оцінювання ефективності обраних заходів кібербезпеки ОКІІ організації застосовано методику яка ґрунтується на обчислюванні показника (ймовірності) ризику кібербезпеки.

Запропонована методика націлена підвищити ефективність вибору заходів на етапі планування заходів кібербезпеки ОКІІ організації.

Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні та практичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого її вивчення в такому напрямі, як розробка методології оцінки ризиків кібербезпеки у гібридних інформаційних технологій в освіті.

Література

1. Петренко А.Г. План дій щодо впровадження оборонної реформи у 2016 – 2020 роках (дорожня карта оборонної реформи). К.: ДВПСП та МС МО України, 2016. 210 с. **2.** Закон України "Про основні засади забезпечення кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/2163-19. **3.** Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", затверджена

Указом Президента України від 15.03.16 №96/2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016. **4.** Рішення Ради національної безпеки і оборони України від 10.07.17 "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року" "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13.02.17 №254/2017. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17.
5. **Козубцова Л.М.** Обґрунтування структури методики планування заходів кібербезпеки об'єктів критичної інформаційної інфраструктури організації. *Materials of the XVII International scientific and practical Conference Prospects of world science - 2021 (Sheffield, July 30 - August 7, 2021).* Sheffield. Science and education LTDC, 2021. Volume 3. Pp. 87 – 92. **6. Козубцов І.М., Хлапонін Ю.І., Козубцова Л.М**. Ідея впровадження зворотного зв'язку як вдосконалення функціональної залежності реалізації кібернетичної безпеки. *Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку"* (Харків, 15 березня 201 р.). Харків. НАНГ України, 2021. С. 86 – 87. **7. Козубцов І.М., Козубцова Л.М.** Прогноз можливих наслідків настання "колапсу інформаційних систем спеціального призначення". *Актуальні проблеми управління інформаційною безпекою держави*: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). Київ: НА СБУ, 2021. С. 50 – 53. **8. Гончар С.Ф.** Методологія оцінки ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури. *Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки*. 2019. Том 30(69). Ч.1. С.40 – 43. **9. Плетнев П.В., Белов В.М.** Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса. *Доклады ТУСУРа*, № 1(25), Ч 2, июнь 2012. С.83 – 86. **10. Козубцова Л.М.** Удосконалена методика діагностування кібернетичної захищеності інформаційної системи з урахуванням деструктивних кібернетичних впливів. *Науковий журнал "Комп'ютерно-інтегровані технології: освіта, наука, виробництво"*. Луцьк, 2020. Випуск № 39. С.127 – 135. **11. Захарченко Р.И., Королев И.Д.** Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве. *Наукоемкие технологии в космических исследованиях Земли.* 2018. Т.10. №2. С.52 – 61. **12. Коцыняк М.А., Коцыняк М.М., Лаута О.С., Лаута А.С.** Киберустойчивость информационно-телекоммуникационной сети. *Информационные технологии, связь и защита информации МВД России*. 2015. С.104 – 105. **13. Нили Э., Адамс К., Кеннерли М.** Призма эффективности: Карта сбалансированных показателей для измерения успеха в бизнесе и управления им / пер. с англ. Д.: Баланс-Клуб, 2003. 400 с.

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ВЫПОЛНЕНИЯ МЕРОПРИЯТИЙ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОГО ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИЙ

***Леся Михайловна Козубцова** (кандидат технических наук)[1]*
***Юрий Иванович Хлапонин** (доктор технических наук, профессор)[2]*
***Игорь Николаевич Козубцов** (доктор педагогических наук, старший научный сотрудник)[1]*

[1]Военный институт телекоммуникаций и информатизации, Киев, Украина
[2]Киевский национальной университет строительства и архитектуры, Киев, Украина

В научной статье обоснована методика оценки эффективности выполнения мероприятий, направленных на обеспечение кибернетической безопасности объектов критической информационной инфраструктуры организаций. Данная работа является продолжением исследования по предварительному описанию "Будущая среда безопасности 2030", расширяя научные пределы по реализации неотложных мер государственной политики по нейтрализации угроз кибербезопасности организаций. Необходимость статьи обусловлена рациональным выбором и применением мер, направленных на обеспечение кибернетической безопасности объектов информационной инфраструктуры организаций. Установлено, что на практике оценить эффективность выполнения мероприятий, направленных на обеспечение кибернетической безопасности можно через следующие показатели (вероятности): риск кибернетической безопасности, киберзахищенисть, функциональная работоспособность системы объекта критической информационной инфраструктуры, киберстийкисть. Для применения принципа преемственности в статье под усовершенствованную онтологию кибербезопасности выбран показатель (вероятность) риска кибернетической безопасности. Методика оценки риска кибербезопасности объектов критической информационной инфраструктуры организаций основывается на определении вероятности реализации кибератак, а также уровней их ущерба. Методика включает следующие этапы: этап разработки системы показателей оценки эффективности выполнения мероприятий; этап планирования процедур сбора исходных данных для оценки эффективности выполнения мероприятий; этап вычисления значения показателя эффективности выполнения мероприятий; этап интерпретации значения показателя эффективности выполнения мероприятий, направленных на обеспечение кибербезопасности объектов критической информационной инфраструктуры организаций. Исходные значения для расчета киберзахищености получают по результатам аудита объектов критической информационной инфраструктуры организаций. При расчете значений вероятности кибератак, а также уровня возможного ущерба следует воспользоваться статистическими методами, экспертными оценками или элементами теории принятия решений. Научная новизна исследования заключается в том, что впервые предложена методика оценки эффективности мероприятий кибербезопасности по показателю (вероятности) риска кибербезопасности, которая будет дополнять методику планирования мероприятий кибербезопасности объектов критической информационной инфраструктуры организаций.

***Ключевые слова:** методика, оценка, эффективность, мероприятия, кибербезопасность, объект критической информационной инфраструктуры, организация.*

METHODS OF EVALUATION OF EFFICIENCY OF IMPLEMENTATION OF CYBER SECURITY MEASURES OF CRITICAL INFORMATION INFRASTRUCTURE BODIES OF THE BODY

***Lesja Kozubtsova** (Candidate of Technical Sciences)[1]*
***Yuri Khlaponin** (Doctor of Technical Sciences, Professor)[2]*
***Igor Kozubtsov** (Doctor of Pedagogical Sciences, Senior Research Fellow)[1]*

[1]Military institute of telecommunications and informatization technologies, Kiev, Ukraine
[2]Kiev National University of Civil Engineering and Architecture, Kiev, Ukraine

The scientific article substantiates the method of assessing the effectiveness of measures aimed at ensuring the cyber security of critical information infrastructure of organizations. This work is a continuation of the study on the preliminary description of "The Future of the Security Environment 2030", expanding the scientific scope for the implementation of urgent public policy measures to neutralize threats to cybersecurity of organizations. The need for the article is due to the rational choice and application of measures aimed at ensuring the cyber security of information infrastructure facilities of organizations. It is established that in practice it is possible to estimate efficiency of performance of the actions directed on maintenance of cyber security through the following indicators (probabilities): risk of cyber security, cybersecurity, functional operability of system of object of critical information infrastructure, cyberstability. To apply the principle of continuity in the article under the improved cybersecurity ontology, the indicator (probability) of cybersecurity risk is selected. The methodology for assessing the risk of cybersecurity of critical information infrastructure of organizations is based on determining the probability of cyber attacks, as well as the levels of their damage. The methodology includes the following stages: the stage of developing a system of indicators for evaluating the effectiveness of activities; the stage of planning the procedures for collecting initial data to assess the effectiveness of the activities; the stage of calculating the value of the performance indicator; stage of interpretation of the value of the indicator of efficiency of performance of the actions directed on maintenance of cybersecurity of objects of a critical information infrastructure of the organizations. The initial values for the calculation of cybersecurity are obtained based on the results of the audit of critical information infrastructure of organizations. Statistical methods, expert estimates, or elements of decision theory should be used to calculate cyber attack probability values as well as the level of possible damage. The scientific novelty of the study is that for the first time a method of evaluating the effectiveness of cybersecurity measures on the indicator (probability) of cybersecurity risk is proposed, which will complement the methodology of planning cybersecurity measures of critical information infrastructure of organizations.

Keywords: methodology, evaluation, efficiency, measures, cybersecurity, object of critical information infrastructure, organization.

References

1. Petrenko A.H. (2016) Action plan for the implementation of defense reform in 2016-2020 (road map of defense reform) [Plan dii shchodo vprovadzhennia oboronnoi reformy u 2016-2020 rokakh (dorozhnia karta oboronnoi reformy)]. K.: DVPSP ta MS MO Ukrainy, 210 p. **2.** Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine". [Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy"]. **3.** On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cyber Security Strategy of Ukraine", approved by the Decree of the President of Ukraine dated 15.03.16 №96/2016. [Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy", zatverdzhena Ukazom Prezydenta Ukrainy vid 15.03.16 #96/2016]. **4.** Decision of the National Security and Defense Council of Ukraine dated 10.07.17 "On the status of implementation of the decision of the National Security and Defense Council of Ukraine dated December 29, 2016" "On threats to cybersecurity and urgent measures to neutralize them", enacted by Presidential Decree of 13.02.17 №254/2017. [Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 10.07.17 "Pro stan vykonannia rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku" "Pro zahrozy kiberbezpetsi derzhavy ta nevidkladni zakhody z yikh neitralizatsii", vvedenoho v diiu Ukazom Prezydenta Ukrainy vid 13.02.17 #254/2017]. **5. Kozubtsova L.M.** (2021) Substantiation of the structure of the methodology of planning cybersecurity measures of the critical information infrastructure of the organization [Obg`runtuvannya struktury` metody`ky` planuvannya zaxodiv kiberbezpeky` ob'yektiv kry`ty`chnoyi informacijnoyi infrastruktury` organizaciyi] *Materials of the XVII International scientific and practical Conference Prospects of world science - 2021* (Sheffield, July 30 - August 7, 2021). Sheffield. Science and education LTDC, 2021. Vol. 3. Pp.87 – 92.**6. Kozubtsov I.M., Khlaponin Yu.I., Kozubtsova L.M.** (2021) The idea of introducing feedback as improving the functional dependence of the implementation of cyber security. [Ideia vprovadzhennia zvorotnoho zviazku yak vdoskonalennia funktsionalnoi zalezhnosti realizatsii kibernetychnoi bezpeky] *Mizhnarodna naukovo-praktychna konferentsiia "Zastosuvannia informatsiinykh tekhnolohii u pidhotovtsi ta diialnosti syl okhorony pravoporiadku"* (Kharkiv, 15 bereznia 2021 r.). Kharkiv. NANH Ukrainy. Pp. 86 – 87. **7. Kozubtsov I.M., Kozubtsova L.M.** (2021) Forecast of possible consequences of the "collapse of special purpose information systems" [Prohnoz mozhlyvykh naslidkiv nastannia "kolapsu informatsiinykh system spetsialnoho pryznachennia"]. *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy*: zb. tez nauk. dop. nauk.-prakt. konf. (Kyiv, 26 bereznia 2021 r.). Kyiv: NA SBU. S.50 – 53. **8. Honchar S.F.** (2019) Methodology for assessing the risks of cybersecurity of the information system of critical infrastructure facilities [Metodolohiia otsinky ryzykiv kiberbezpeky informatsiinoi systemy obiektiv krytychnoi infrastruktury]. *Vcheni zapysky TNU imeni V.I. Vernadskoho*. Seriia: tekhnichni nauky. Tom 30(69). Ch.1. S.40 – 43. **9. Плетнев П.В., Белов В.М.** Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса. *Доклады ТУСУРа*, № 1(25), Ч 2, июнь 2012. С.83 – 86. **10. Kozubtsova L.M.** (2020) Improved methodology for diagnosing cyber security of an information system taking into account destructive cybernetic influences [Udoskonalena metodyka diahnostuvannia kibernetychnoi zakhyshchenosti informatsiinoi systemy z urakhuvanniam destruktyvnykh kibernetychnykh vplyviv]. *Naukovyi zhurnal "Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo*". Lutsk. Vypusk #39. S. 127 – 135. **11. Zaharchenko R.I., Korolev I.D.** (2018) Methodology for assessing the sustainability of the functioning of critical information infrastructure objects operating in cyberspace [Metodika otsenki ustoychivosti funktsionirovaniya ob'ektov kriticheskoy informatsionnoy infrastrukturyi funktsioniruyuschey v kiberprostranstve]. *Naukoemkie tehnologii v kosmicheskih issledovaniyah Zemli.* T.10. #2. S.52 – 61. **12. Kotsyinyak M.A., Kotsyinyak M.M., Lauta O.S., Lauta A.S.** (2015) Cyber resilience of the information and telecommunication network [Kiberustoychivost informatsionno-telekommunikatsionnoy seti]. *Informatsionnyie tehnologii, svyaz i zaschita informatsii MVD Rossii.* S.104 – 105. **13. Nili E., Adams K., Kennerli M.** (2003) The Performance Prism: A Balanced Scorecard for Measuring and Managing Business Success [Prizma effektivnosti: Karta sbalansirovannyih pokazateley dlya izmereniya uspeha v biznese i upravleniya im] / per. s angl. D.: Balans-Klub. 400 s.

DOI:**10.33099/2311-7249/2021-41-2-23-30**

УДК: 355:358.4

Леонід Михайлович Артюшин *(доктор технічних наук, професор)*[1]
Анатолій Анатолійович Лобанов *(доктор військових наук, професор)*[2]
Володимир Вікторович Герасименко *(кандидат військових наук)*[2]

[1]*Державний науково-дослідний інститут авіації України, Київ, Україна*
[2]*Національний університет оборони України імені Івана Черняховського, Київ, Україна*

МАТЕМАТИЧНА МОДЕЛЬ ПОБУДОВИ БОЙОВОГО ПОРЯДКУ СПІЛЬНОЇ АВІАЦІЙНОЇ ГРУПИ ПІЛОТОВАНОЇ ТА БЕЗПІЛОТНОЇ АВІАЦІЇ

Для здійснення автоматизованого управління бойовими порядками спільних авіаційних груп необхідно створення системи математичних моделей етапів функціонування бойового порядку, а також засобів реалізації цієї системи, включно з процедурами управління та інтеграції. Найбільш вдало така задача може бути розв'язана при застосуванні логіко-динамічних моделей та теорії логіко-динамічних систем.

Метою статті є створення банку моделей, як системи моделей математичного опису етапів функціонування бойового порядку спільної авіаційної групи, що становить основу математичної моделі бойового порядку спільної авіаційної групи пілотованої та безпілотної авіації.

Задача синтезу логіко-динамічних моделей полягає у розділенні вихідної моделі на сукупність структурних станів (режимів), причому систему у кожному структурному стані можна розглядати як самостійну. Моделювання кожного з станів полягає у об'єднанні ряду режимів, що характеризуються постійним значенням аеродинамічних характеристик пілотованих та безпілотних літальних апаратів залежно від значення функцій предикат змінних. Відповідно, модель виконання бойового завдання спільною авіаційною групою пілотованої та безпілотної авіації розбивається на ряд етапів. Зміст задачі дослідження передбачає використання повної нелінійної моделі динаміки польоту без розділення руху на повздовжній, боковий та вертикальний, при прийнятих припущеннях.

Визначення заданого відносного положення пілотованих та безпілотних літальних апаратів у бойовому порядку дозволить описати їх спільний відносний рух, що формує особливості системи управління бойовим порядком, а обрання системи координат відносно веденого надасть переваги на всіх подальших етапах розв'язання задачі управління.

Ключові слова: *автоматизоване управління; банк моделей; модель бойового порядку; траєкторна система координат; рівняння руху; спільна авіаційна група.*

Вступ

Сьогодні, для управління бойовими порядками пілотованої та безпілотної авіації при виконанні ними спільного завдання використовується широке розмаїття систем управління, в основу яких покладено як ручне, так і автоматизоване керування з використанням систем штучного інтелекту. Але недоліки та переваги кожної з систем управління вимагають пошуку та створення системи моделей математичного опису етапів функціонування бойового порядку з процедурами управління та інтеграції. Ця задача може бути розв'язана при застосуванні логіко-динамічних моделей та теорії логіко-динамічних систем. Синтез логіко-динамічних моделей полягає у розділенні вихідної моделі на сукупність структурних станів (режимів), а моделювання кожного з станів полягає у об'єднанні ряду режимів, що характеризуються постійним значенням аеродинамічних характеристик пілотованих та безпілотних літальних апаратів. Відповідно, модель виконання бойового завдання спільною авіаційною групою пілотованої та безпілотної авіації розбивається на ряд етапів. Отже, зміст задачі дослідження передбачає використання повної нелінійної моделі динаміки польоту без розділення руху на повздовжній, боковий та вертикальний, при прийнятих припущеннях, та визначення заданого відносного положення пілотованих та безпілотних літальних апаратів у бойовому порядку, що дозволяє описати їх спільний відносний рух.

Постановка проблеми. Ефективність бойового застосування авіації у спільних бойових порядках буде значно перевищувати ефективність окремого застосування пілотованої та безпілотної авіації саме за рахунок поєднання їх сильних та взаємної нейтралізації слабких сторін. Таким чином, виникає проблема створення складної математичної моделі або системи моделей, що дозволять з прийнятними точністю та достовірністю відтворити процес управління бойовим порядком спільної авіаційної групи пілотованої та безпілотної авіації, що є складним як у теоретичному, так і у практичному розумінні, а розв'язання цієї проблеми у науковій спільноті не набуло широкого розмаху і є актуальним науковим завданням.

Аналіз останніх досліджень та публікацій. Створення комплексу моделей на основі якого формується банк моделей описано у [1]. Моделі, що описують функціональну динаміку бойового порядку спільної авіаційної групи та структуру бойового порядку, що представлена у класі відносин "частина – ціле", представлено у [2, 3]. Приклади розв'язання задач ієрархічності управління та координації взаємодії в групі літальних апаратів при застосуванні підходів та апарату логіко-динамічних моделей та теорії логіко-динамічних систем наведено у [4, 5]. Етапи польоту, що моделюються, наведені у [6], а порядок опису маневрів літальних апаратів на цих етапах наведені у [7]. Закони змінення перевантаження за відповідними осями при маневруванні описані у [8], а рівняння динаміки польоту літального апарату на цих маневрах описані у [9, 10]. Прототип моделі турбореактивного двигуна наведено у [11], а обернена задачі динаміки, на основі якої синтезований закон функціонування автомату тяги турбореактивного двигуна, наведена у [12]. Опис руху літального апарату в системах координат, що прийняті у механіці та динаміці польоту, наведено у [13]. Висновки та рівняння, як основа синтезу алгоритмів управління відносним рухом літаків у траєкторній системі координат веденого та складова частина математичної моделі бойового порядку спільної авіаційної групи пілотованої та безпілотної авіації наведені у [14]. Погляди військового керівництва провідних країн світу щодо теоретичних та практичних розробок у спільному застосуванні пілотованої та безпілотної авіації наведені у [15, 16].

Метою статті є створення банку моделей, як системи моделей математичного опису етапів функціонування бойового порядку спільної авіаційної групи, а також засобів реалізації цієї системи, включно з процедурами управління та інтеграції, що становить основу математичної моделі бойового порядку спільної авіаційної групи пілотованої та безпілотної авіації.

Виклад основного матеріалу дослідження.

Комплекс моделей $M = \{M_i\}$ математичного опису етапів функціонування бойового порядку (модель літального апарату пілотованого або безпілотного) та модель обстановки функціонування $M^{\text{ОФ}}$) утворює склад банку моделей [1]. Банк моделей дає можливість задати набір відносин Ж , що дозволяють обирати визначенні співвідношення послідовності моделей, необхідних при моделюванні певних етапів функціонування бойового порядку та розв'язання задач, що при цьому виникають. Цей набір відносин визначає структуру банку моделей. Крім цього, необхідно задати також набір відношень Д перетворення моделей. Тоді банк математичних моделей може бути визначений наступним чином:

$$\text{Б}M = \{M, \text{Ж}, \text{Д}\}.$$

Складність структури процесів та взаємозв'язків пари моделей $M^{\text{БП}}, M^{\text{ОФ}}$ може бути представлена множиною часткових моделей.

Вихідним положенням для побудови системи моделей є множина цілей $\text{Ц}\{\text{Ц}_i\}$, для досягнення яких формується бойовий порядок спільної авіаційної групи. Таким чином, першою базовою моделлю бойового порядку спільної авіаційної групи будемо вважати модель динамічної операції Д_i, що здійснюється для досягнення цілі Ц_i. Множини $\text{Ц}\{\text{Ц}_i\}$ та $\text{Д}\{\text{Д}_i\}$ повинні мати спільне відображення. Моделі Д_i мають складну ієрархічну структуру, у якій об'єднані динаміка пілотованих та безпілотних літальних апаратів, динаміка зміни структури, динаміка взаємодії підсистеми тощо.

Для заданої послідовності $\text{Ц}_1, \text{Ц}_2, \dots, \text{Ц}_k$ будується відповідна послідовність $\text{Д}_1, \text{Д}_2, \dots, \text{Д}_k$, що розглядається як деяка цільова структура $\text{Р}\{\text{Д}_i\}^k$, тобто пакет динамічних операцій для досягнення конкретних цілей. Моделі $\text{Д}_i, \text{Р}\{\text{Д}_i\}$ описують функціональну динаміку бойового порядку спільної авіаційної групи, яка у загальному вигляді описується у моделі $M_{\text{ОФ}}^{\text{БП}}$. Другою базовою моделлю бойового порядку спільної авіаційної групи є модель структури бойового порядку $M_{\text{С}}^{\text{БП}}$, що представлена у класі відносин "частина – ціле" [2, 3].

Положеннями класичної теорії управління, що описують бойовий порядок спільної авіаційної групи геометрично визначеною сукупністю рухомих тіл, неможливо відобразити ієрархічність управління та координацію взаємодії в групі пілотованих та безпілотних літальних апаратів, а також ввести у модель відповідну категорію цілей для бойового порядку взагалі та декомпозованих підцілей для кожного окремого пілотованого чи безпілотного літального апарату. Дана задача може бути розв'язана при застосуванні підходу та апарату логіко-динамічних моделей (ЛДМ) та теорії логіко-динамічних систем [4, 5].

Задача синтезу ЛДМ полягає у розділенні вихідної моделі на сукупність структурних станів (режимів), причому систему у кожному структурному стані можна розглядати як незалежну, таку, що функціонує самостійно. Відповідно до такого підходу модель виконання бойового завдання спільною авіаційною групою пілотованої та безпілотної авіації розбивається на ряд етапів: зліт; збір у повітрі та побудова бойового порядку спільної авіаційної групи; політ у район виконання завдання; виконання завдання; повернення на аеродром посадки; розпуск бойового порядку та захід на посадку; посадка [6]. Кожен з етапів представляє собою виконання визначеного маневру або їх сукупності [7]. Маневр задається законом змінення перевантаження за відповідними осями [8].

У загальному вигляді кусково-безперервна функція структурного стану записується як неупорядкована i-послідовність N_{iy} функції перевантажень n_{yi}:

$$N_{iy}(H, \Theta) = \sum_{i=1}^{n} L_{ij}^{n_y}(H, \Theta) n_{yij}, \qquad (1)$$

де $L_{ij}^{n_y}$ – логічні змінні, що є функціями предикат

дійсних змінних H та Θ; n_{yij} – значення n_y при визначених H та Θ польоту; j = 1, 2, ..., n – номер стану. При цьому L_j повинні задовольняти умовам єдиності $L_S \wedge L_P = 0,\ S \neq P$, та повноти $\bigvee_{s=1}^{S} L_s = 1$ (i = 1, 2, …, N – номер пілотованого чи безпілотного літального апарату в строю).

Моделювання кожного з станів полягає у об'єднанні ряду режимів, що характеризуються постійним значенням аеродинамічних характеристик пілотованих та безпілотних літальних апаратів залежно від значення функцій предикат змінних M та H . При такій характеристиці режиму польоту літального апарату коефіцієнти, що входять до логічних рівнянь моделі, представляються у вигляді

$$Z_i(H,M) = \sum_{j=1}^{n} L_{ij}(H,M)K_{ij} \qquad (2)$$

де $Z_i(H,M)$ – мета функціонування літального апарату, як функція предикат дійсних змінних M та H;

$L_{ij}(H,M)$ – логічні змінні, що є функціями предикат дійсних змінних M та H;

H, M – змінні, що входять до формул визначення аеродинамічних характеристик пілотованих та безпілотних літальних апаратів залежно від мети функціонування Z_i;

K_{ij} – значення відповідних коефіцієнтів при H та M (залежать від типу літального апарату);

i – номер пілотованого або безпілотного літального апарату в бойовому порядку;

j – номер режиму.

Область існування логічних змінних – $L_{ij}\{0,1\}$, а область визначення – підмножини $\{H_L \pm \Delta H\}$ та $\{M_\mathcal{V} \pm \Delta M\}$ множин $\{H\}$ та $\{M\}$, тобто

$$L_{ij} = \begin{cases} 1 \text{ при } H \in (H_L \pm \Delta H) \text{ та } M \in \{M_\mathcal{V} \pm \Delta M\} \\ 0 \text{ у всіх решті випадків} \end{cases} \qquad (3)$$

де $L = 1,2,\dots,q$ – множина значень H;

$\mathcal{V} = 1,2,\dots,p$ – множина значень M;

$j = 1,2,\dots,k,\ \ k = q \times p$.

Наведене вище розбиття моделі виконання бойової задачі групою пілотованих та безпілотних літальних апаратів є основою синтезу логічної частини моделювання та визначає набір відношень Ж банку моделей. Логічними операціями відбувається "зшивання" режимів у стани, стани у маневри тощо. На рис. 1 та 2 представлені, відповідно, структура виконання бойової задачі пілотованою та безпілотною авіацією та структурно-логічна схема маневру бойового порядку пілотованих та безпілотних літальних апаратів у вертикальній площині.

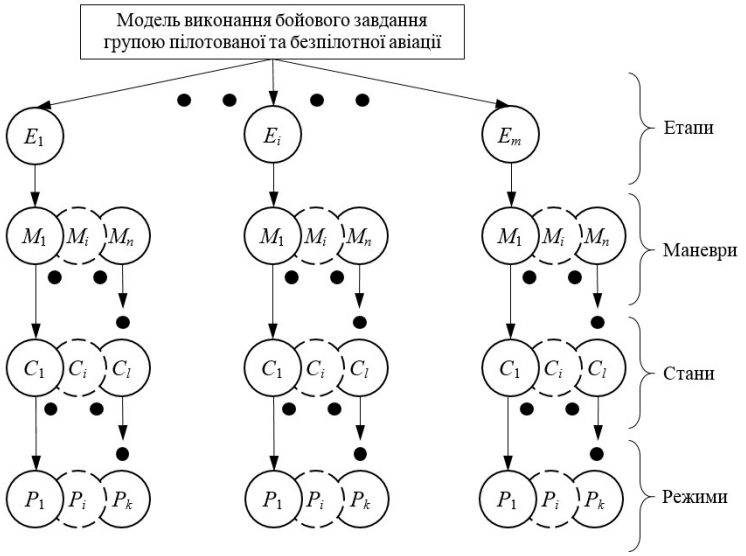

Рисунок 1 – Структура виконання завдання групою пілотованої та безпілотної авіації

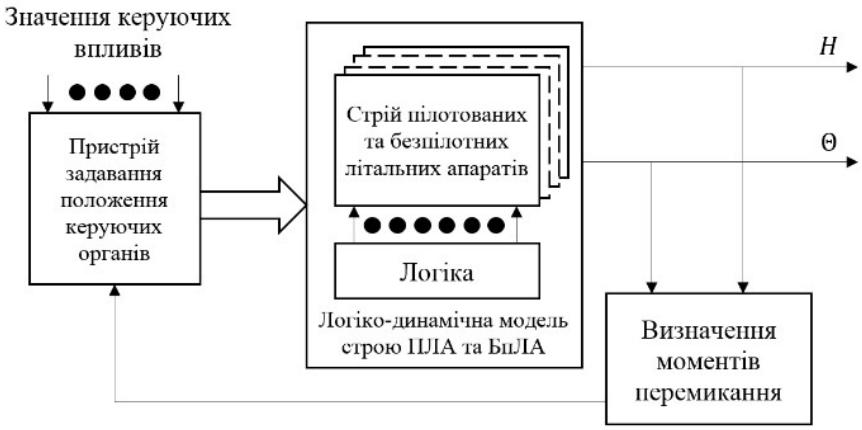

Рисунок 2 – Структурно-логічна схема виконання маневру строю пілотованої (ПЛА) та безпілотної (БпЛА) авіації

Підсумовуючі наведене, а також використовуючи результати та позначення [3], представимо на рис. 3 узагальнену логіко-математичну модель бойового порядку спільної авіаційної групи пілотованої та безпілотної авіації, що містить в собі моделі пілотованих та безпілотних літальних апаратів та систем управління ними, структурну та логічну частину.

Зміст задачі дослідження передбачає використання достатньо повної нелінійної моделі динаміки польоту без розділення руху на повздовжній та боковий. При цьому прийняті наступні припущення:

літак розглядається як тверде тіло;

політ виконується над пласкою Землею, що не обертається;

центробіжні моменти інерції дорівнюють 0;

тяга двигунів спрямована вздовж осі $0X$ літака.

Рівняння динаміки польоту можуть бути прийняті відповідно до [9,10]. До них додається модель турбореактивного двигуна [11]:

$$T_{\text{дв}}\Delta P + \Delta P = \left(\frac{\partial P}{\partial \delta_{\text{руд}}}\right)_0 \Delta\delta_{\text{руд}}, \qquad (4)$$

де ΔP – приріст тяги, Н;

$\Delta\delta_{\text{руд}}$ – пересування ричагу управління двигуном, рад;

$T_{\text{дв}}$ – константа часу роботи двигуна, 1/с;

$\left(\frac{\partial P}{\partial \delta_{\text{руд}}}\right)_0$ – прийомистість двигуна, Н/рад.

Закони управління системи автоматизованого управління мають вигляд:

для каналу управління по тангажу

$$\varphi_{\text{ст}} = \frac{T_{\text{и}}P+1}{T_{\text{и}}P}\left[\mu_z(q)\frac{T_\delta}{T_\delta+1}\omega_z + \int_{\Delta n_y = n_y - n_{y\,\max}(q)}^{\Delta n_y = n_y - n_{y\,\min}(q)} i_{\Delta\vartheta}\left(\vartheta - \vartheta_{\text{зад}}\right)\frac{T_\vartheta}{T_\vartheta+1}\right];$$

для каналу управління по крену

$$\delta_{\text{е}} = \frac{T_{\text{и}}p+1}{T_{\text{и}}p}\left[i_{\Delta\gamma}\frac{2T_1p+1}{T_1p+1}\frac{T_\gamma p}{T_\gamma p+1}\left(\gamma - \gamma_{\text{зад}}\right) + \mu_x(q)\omega_x\right]; \qquad (5)$$

для каналу управління по курсу

$$\delta_{\text{е}} = \frac{T_{\text{и}}p+1}{T_{\text{и}}p}\left[i_{\Delta\gamma}\frac{2T_1p+1}{T_1p+1}\frac{T_\gamma p}{T_\gamma p+1}\left(\gamma - \gamma_{\text{зад}}\right) + \mu_x(q)\omega_x\right];$$

$$\gamma_{\text{зад}} = i_{\Delta\Psi}\frac{1}{T_2p+1}\left(\Psi - \Psi_{\text{зад}}\right).$$

Відхилення руля напрямку відбувається відповідно до закону

$$\delta_{\text{н}} = \frac{T_{\text{и}}p+1}{T_{\text{и}}p}\mu_y(q)\omega_y. \qquad (6)$$

Закон функціонування автомату тяги, синтезованого на основі розв'язання оберненої задачі динаміки [12], має структуру

$$\delta_{\text{руд}} = K_V\left[r(\bar{V} - V) - \dot{V}\right], \qquad (7)$$

де K_V [рад с/м], r [1/с] – константи;

$\bar{V}, V$ – задане та поточне значення повітряної швидкості;

$\dot{V}$ – прискорення літака, мс$^{-2}$.

Вказані рівняння разом з рівняннями відносного руху є основою синтезу алгоритмів управління відносним рухом літаків (8) та суттєвою складовою частиною математичної моделі бойового порядку [3].

$$\begin{aligned}
\ddot{x} &= a_{ix} - \dot{V}_j + \ddot{\Theta}_j y - \ddot{\Psi}_j z\cos\Theta_j - \tfrac{1}{2}\dot{\Psi}_j^2 y\sin 2\Theta_j - \dot{\Psi}_j\dot{\Theta}_j z\sin\Theta_j + \dot{\Psi}_j^2 x\cos^2\Theta_j + \dot{\Theta}_j^2 x - 2\dot{\Psi}_j\dot{z}\cos\Theta_j + 2\dot{\Theta}_j\dot{y};\\
\ddot{y} &= a_{iy} - \dot{\Theta}_j\dot{V}_j - \ddot{\Theta}_j x + \ddot{\Psi}_j z\sin\Theta_j - \tfrac{1}{2}\dot{\Psi}_j^2 x\sin 2\Theta_j - \dot{\Psi}_j\dot{\Theta}_j z\cos\Theta_j + \dot{\Psi}_j^2 y sin^2\Theta_j + \dot{\Theta}_j^2 y - 2\dot{\Theta}_j\dot{x} + 2\dot{\Psi}_j\dot{z}\sin\Theta_j; \qquad (8)\\
\ddot{z} &= a_{iz} - \dot{\Psi}_j V_j\cos\Theta_j - \ddot{\Psi}_j y\sin\Theta_j + \ddot{\Psi}_j x\cos\Theta_j - \dot{\Psi}_j\dot{\Theta}_j x\sin\Theta_j - \dot{\Psi}_j\dot{\Theta}_j y\cos\Theta_j + \dot{\Psi}_j^2 z - 2\dot{\Psi}_j\dot{y}\sin\Theta_j + 2\dot{\Psi}_j\dot{x}\cos\Theta_j.
\end{aligned}$$

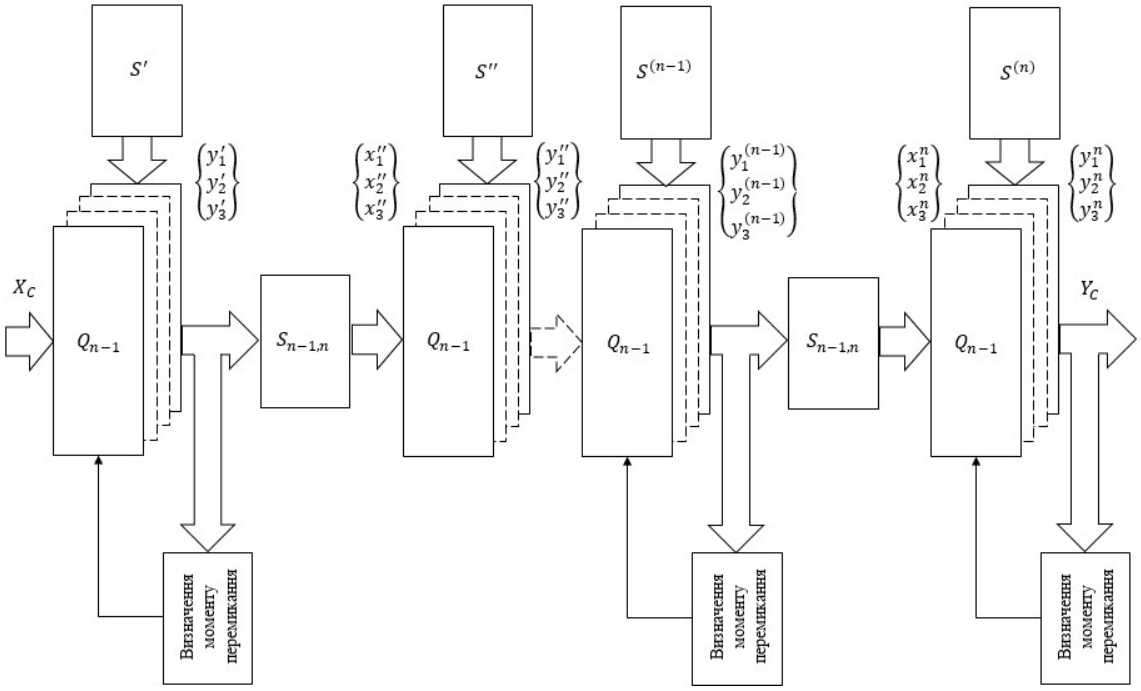

Рисунок 3 – Узагальнена логіко-математична модель бойового порядку пілотованої та безплотної авіації

Для пояснення питання управління параметрами бойових порядків спільної авіаційної групи пілотованої та безпілотної авіації розглянемо порядок управління на прикладі управління конфігурацією складної механічної системи. Елементом системи тут є літальний апарат, рух якого описується у загальноприйнятих системах координат, що застосовуються у механіці та динаміці польоту [13].

При розв'язанні задачі забезпечення заданого відносного положення пілотованих та безпілотних літальних апаратів у бойовому порядку природно розкрити опис їх відносного руху. Існуюче уявлення руху здебільшого визначить особливості відповідної системи управління. Обрання системи координат на початковому етапі дає суттєві переваги на всіх подальших етапах розв'язання задачі.

Незалежно від причин відхилення параметрів бойового порядку пілотованої та безпілотної авіації від запрограмованих, виникаючі розбіжності усуваються за рахунок зміни режимів польоту ведених літаків. Це основний аргумент за організацію управління маневруванням літаків у бойовому порядку у траєкторній системі координат O_i, X_k, Y_k, Z_k пов'язаної з i-м веденим безпілотним літальним апаратом (рис. 4, 5).

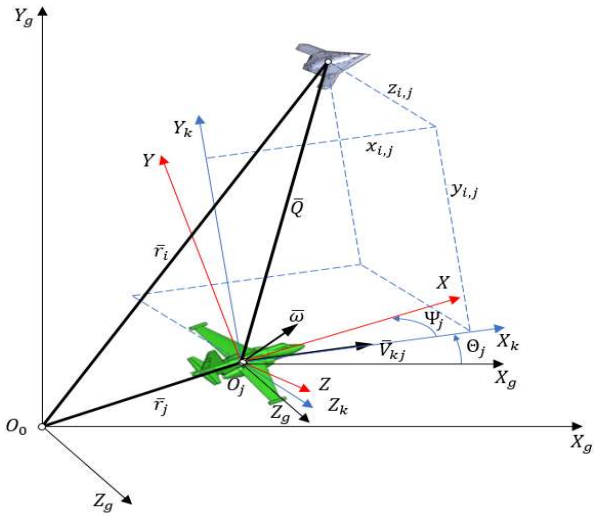

Рисунок 4 – Схема сил, що діють на пілотований літак ведучого в траєкторній системі координат веденого безпілотного літака

Як швидко i -й ведений безпілотний літак оцінює своє положення відносно j -го ведучого пілотованого літака у "власній" системі координат і відповідно до цього здійснює рух, процес організації управління маневруванням літаків у бойовому порядку позбавлений труднощів, пов'язаних з додатковими перетвореннями координат. Крім того, інформація про вектор швидкості $\bar{V}_{ki}$ веденого безпілотного літака дозволяє контролювати траєкторію його руху відносно пілотованого літака.

Формування на борту веденого безпілотного літака потрібних значень керуючих функцій забезпечує ув'язку розв'язання задачі управління рухом пілотованих та безпілотних літаків у бойовому порядку з практикою групового маневрування, відповідно до чого ведені безпілотні літаки виконують необхідні для витримування заданого бойового порядку маневри.

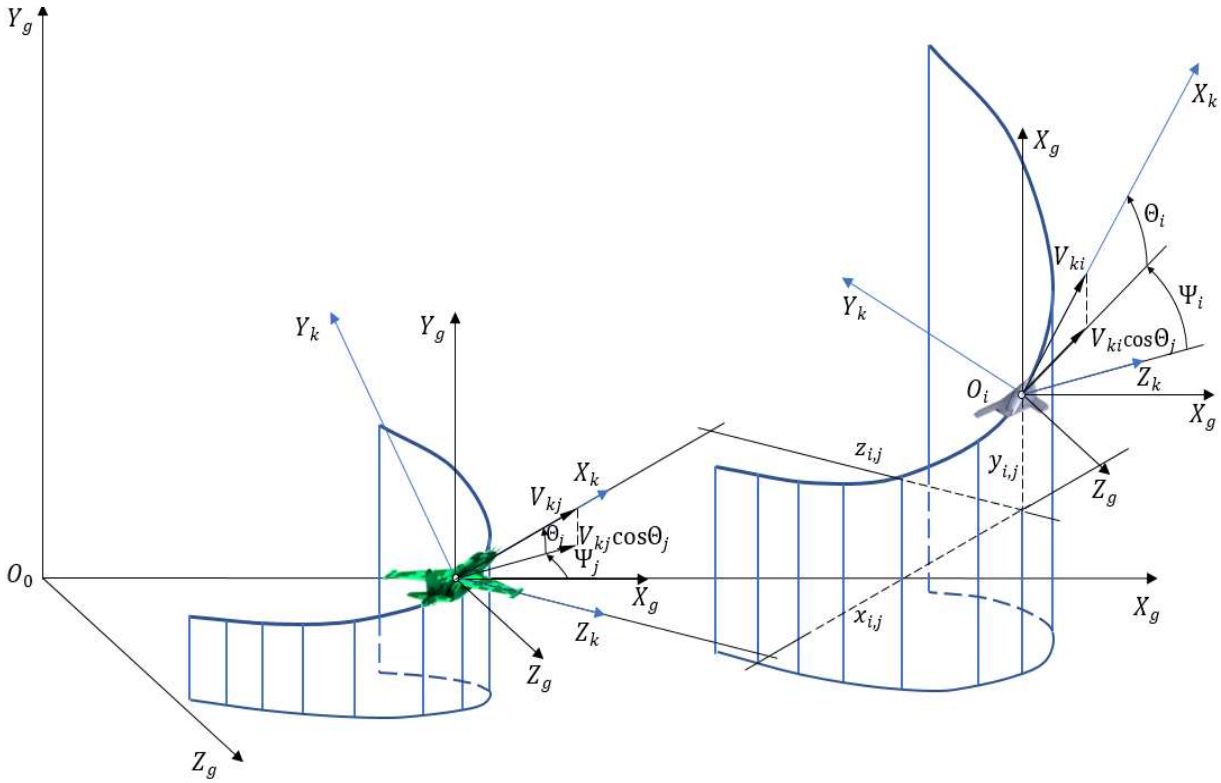

Рисунок 5 – Схема сил на маневрі, що діють на пілотований літак ведучого та ведений безпілотний літак

Прийняття у якості базової траєкторної системи координат веденого дозволить обійти ряд труднощів принципового характеру, притаманних організації управління в системі координат ведучого. Так, складові переносного прискорення, обумовлені обертальними рухами ведучого, досить суттєво впливають на величини відносних прискорень. Вони зростають пропорційно значенням параметрів строю та можуть бути компенсовані тільки за рахунок значної зміни абсолютних прискорень веденого літака з можливим виходом на відповідні обмеження. У відносному русі ведучого літака в системі координат веденого переносне прискорення створює ведений та сам його ж компенсує. Це ж прискорення може бути використано для компенсації складових відносного прискорення, викликаного маневруванням ведучого літака, що забезпечить зменшення абсолютних прискорень веденого літака у процесі управління.

Використання траєкторної системи координат ведучого пов'язано з необхідністю передачі додаткової інформації з пілотованого літака ведучого на ведений безпілотний літак: або заданих значень керуючих функцій, або інформації щодо кутового положення та швидкості польоту ведучого літака. Для такого специфічного об'єкту управління, як бойовий порядок, недолік досить суттєвий. Тому, спираючись на запропоновані моделі, на нашу думку, синтез алгоритмів управління літальними апаратами у бойовому порядку спільної авіаційної групи доцільно здійснювати на базі апарату теорії нейронних мереж.

Рівняння відносного руху літальних апаратів у траєкторній системі координат веденого (8) та висновки з них розкриті у теорії, що використовується для міжлітакової навігації [14]. Рівняння (8) є основою синтезу алгоритмів управління відносним рухом літаків та суттєвою складовою частиною математичної моделі бойового порядку спільної авіаційної групи пілотованої та безпілотної авіації.

Висновки і перспективи подальших досліджень

Таким чином, темпи розвитку авіаційної техніки підштовхують керівництво збройних сил провідних країн світу до теоретичного обґрунтування і практичної розробки питань спільного застосування пілотованої і безпілотної авіації [15, 16].

На теперішній час, основною метою дослідницьких робіт є підвищення ефективності виконання авіацією бойових завдань та забезпечення дій при одночасному зниженні ризику втрат дороговартісних пілотованої авіаційної техніки та льотних екіпажів при значному скороченні матеріальних витрат. Для цього, під час виконання завдань, до бойових порядків пілотованої авіації буде залучатися і безпілотна авіація, управління якою буде здійснюватися з використанням нейронних мереж [16], в ланці вироблення керуючих сигналів без втручання людини. Подібне спільне застосування літальних апаратів різних типів, класів і приналежності є лише проміжним етапом на шляху створення груп безпілотних літальних апаратів, що зможуть самоорганізовуватися та діяти з високим ступенем автономності, самостійно приймати рішення з урахуванням ситуаційної обізнаності. Тому, цілком ймовірно, що в майбутньому виконання всіх основних завдань авіації буде покладено на безпілотні авіаційні комплекси.

Література

1. Жук К. Д. О построении банков летательных моделей в программировании жизненных циклов объектов новой техники // Электронное моделирование. – 1981, № 14. – С. 14–21. **2. Артюшин Л. М.,** Герасименко В. В., Коваль В. В. Метод формування спільної авіаційної групи. Сучасні інформаційні технології у сфері безпеки та оборони № 1(40)/2021. – С. 63–68. URL: https://doi.org/10.33099/2311-7249/2021-40-1-63-68.
3. Артюшин Л. М., Герасименко В. В., Коваль В. В. Синтез раціональних структур бойових порядків спільних авіаційних груп. Журнал наукових праць "Соціальний розвиток та безпека". Том 11, № 3, – 2021. – С. 209–220. DOI: 10.33445/sds.2021.11.3.20. **4. Жук К. Д.**, Тимченко А. А., Доленко Т. И. Исследование структуры и моделирование логико-динамических систем. – К.: Наукова думка, 1975. – 197 с. **5. Жук К. Д.**, Тимченко А. А. Автоматизированное проектирование логико-динамических систем. – К.: Наукова думка, 1981. – 320 с. **6.** Наказ Міністерства оборони України від 05 січня 2015 року № 2 "Про затвердження правил виконання польотів державної авіації України". розділ IX, глава 14 – Особливості виконання групових польотів. **7. Крюков Н. П.,** Кремень М. А. Методом опорных точек // Авиация и космонавтика. – 1983. – № 6. – С. 26–27. – № 7. – С. 27–28. **8. Лебедь В. Г.,** Миргород Ю. І., Українець Є. О. Аерогідрогазодинаміка. Харків : ХУПС ім. Івана Кожедуба, 2011. – 415 с. **9. Немешилов Ю. О**. Моделі систем управління літальними апаратами та методи експериментальних досліджень: Навч. посібн./ Ю.О. Немешилов. – Харків: Нац. аерокосмічн. ун-т ім. М.Є. Жуковського "ХАІ", 2019. – 160 с. **10. Силков В. И.** Динамика полета и боевого маневрирования летательных аппаратов. Часть 2. Устойчивость и управляемость. Учебное пособие. – К.: КВВАИУ, 1984. – 318 с. **11.** Справочник по теории автоматического управления // Под ред. А. А. Красовского. – М.: Наука, 1987. – 712 с. **12. Крутько П. Д.,** Попов Е. П. Синтез управления скоростью движения летательных аппаратов на основе решения обратной задачи динамики // Докл. АН СССР, 1986. – Т.260, № 4. – С.809–812. **13. Горбатенко С. А.** Механика полета: общие сведения. Уравнения движения / Горбатенко С.А. и др. – М.: Машиностроение, 1969. – 500 с. **14. Тарасов В. Г**. Межсамолетная навигация. – М.: Машиностроение, 1980. – 184 с. **15. Greg L.** Zacharias. 2019. Autonomous Horizons: Autonomy in the Air Force – A Path to the Future, Volume 1: Human Autonomy Teaming (AF/ST TR 15-01). Air University Press. **16. Greg L**. Zacharias. March 2019. Autonomous Horizons: Autonomy in the Air Force – A Path to the Future, Volume 2: Autonomous Horizons. The Way Forward. (AF/ST TR 15-02). Air University Press.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПОСТРОЕНИЯ БОЕВОГО ПОРЯДКА СОВМЕСТНОЙ АВИАЦИОННОЙ ГРУППЫ ПИЛОТИРУЕМОЙ И БЕСПИЛОТНОЙ АВИАЦИИ

Леонид Михайлович Артюшин (доктор технических наук, профессор)[1]
Анатолий Анатолиевич Лобанов (доктор военных наук, профессор)[2]
Владимир Викторович Герасименко (кандидат военных наук)[2]

[1]Государственный научно-исследовательский институт авиации Украины, Киев, Украина
[2]Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Для осуществления автоматизированного управления боевыми порядками совместных авиационных групп необходимо создание системы математических моделей этапов функционирования боевого порядка, а также средств реализации этой системы, включая процедуры управления и интеграции. Наиболее удачно такая задача может быть решена при применении логико-динамических моделей и теории логико-динамических систем.

Цель статьи состоит в создании банка моделей, как системы математического описания этапов функционирования боевого порядка совместной авиационной группы, как основы математической модели боевого порядка совместной авиационной группы пилотируемой и беспилотной авиации.

Задача синтеза логико-динамических моделей состоит в разделении исходной модели на составляющие структурных состояний (режимов), причем систему в каждом структурном состоянии можно рассматривать как самостоятельную. Моделирование каждого из состояний состоит в объединении ряда режимов, которые характеризуются постоянным значением аэродинамических характеристик пилотируемых и беспилотных летательных аппаратов в зависимости от значения функции предикат переменных. Соответственно, модель выполнения боевой задачи совместной авиационной группой пилотируемой и беспилотной авиации разбивается на ряд этапов. Содержание задачи исследования предусматривает использование полной нелинейной модели динамики полета без разделения движения на продольное, боковое и вертикальное, при принятых допущениях.

Определение заданного относительного положения пилотируемых и беспилотных летательных аппаратов в боевом порядке позволит описать их совместное относительное движение, которое формирует особенности системы управления боевым порядком, а выбранная система координат относительно ведомого даст преимущества в решении задачи управления.

Ключевые слова: *автоматизированное управление; банк моделей; модель боевого порядка; траекторная система координат; уравнения движения; совместная авиационная группа.*

THE MATHEMATICAL MODEL OF MANNED AND UNMANNED TEAMING COMBAT FORMATION

Leonid Artyushin (Doctor of technical sciences, professor)[1]
Anatoliy Lobanov (Doctor of military sciences, professor)[2]
Volodymyr Herasymenko (Candidate of military sciences)[2]

[1]State Aviation Research Institute of Ukraine, Kyiv, Ukraine
[2]National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine

To implement automatic control of joint aviation groups combat formations, it is necessary to create a system of the mathematical models of combat formations functioning stages, as well as means of implementing this system, including control and integration procedures. This problem can be most successfully solved when applying logical-dynamic models and the theory of logical-dynamical systems.

The goal of the article is to create a bank of models as a system of mathematical description of combat formations functioning stages, as a basis of the mathematical model of a manned and unmanned teaming combat formation.

The task of synthesis of logical-dynamic models is to divide the initial model into components of structural states (modes), and the system in each structural state can be considered as independent. Modeling of each of the states consists in combining a number of modes that are characterized by a constant of the aerodynamic characteristics of manned and unmanned aerial vehicles, depending on the data of the variables predicate function. Accordingly, the combat mission model of a joint aviation group of manned and unmanned aircraft is divided into a number of stages. The content of research task provides to use of a complete nonlinear model of flight dynamics without dividing into longitudinal, lateral and vertical motion, with the taken assumptions.

Determination of the relative position of manned and unmanned aerial vehicles in combat formation will allow to describe their joint relative movement, which forms the features of the combat formation control system,

and the selected coordinate system relative to the loyal wing aircraft will give advantages in solving the control problem.

Keywords: *automatic control; bank of models; model of combat formation; trajectory coordinate system; equations of motion; joint aviation group.*

References

1. Zhuk K. D. (1981), O postroenii bankov letatelnyih modeley v programmirovanii zhiznennyih tsiklov ob'ektov novoy tehniki [About construction of the aircraft models banks in the programming of life cycles of new equipment objects], Elektronnoe modelirovanie, № 14, p. 14–21. **2. Artiushyn L. M., Herasymenko V. V., Koval V. V.** (2021), Metod formuvannia spilnoi aviatsiinoi hrupy [The method of a joint aviation group formation], Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, № 1(40), p. 63–68. DOI:10.33099/ 2311-7249/2021-40-1-63-68. **3. Artiushyn L. M., Herasymenko V. V., Koval V. V.** (2021), Syntez ratsionalnykh struktur boiovykh poriadkiv spilnykh aviatsiinykh hrup [Synthesis of rational structures of joint aviation groups combat formation], Zhurnal naukovykh prats "Sotsialnyi rozvytok ta bezpeka", Tom 11, № 3, p. 209–220. DOI: 10.33445/sds.2021. 11.3.20. **4. Zhuk K.D., Timchenko A.A., Dolenko T.I.** (1975), Issledovanie strukturyi i modelirovanie logiko-dinamicheskih sistem [Study of the structure and modeling of logical-dynamical systems], Kyiv, Naukova dumka, 197 p. **5. Zhuk K.D., Timchenko A.A.** (1981) Avtomatizirovannoe proektirovanie logiko-dinamicheskih system [Computer-aided design of logical-dynamic systems], Kyiv, Naukova dumka, 320 p. 6. Nakaz Ministerstva oborony Ukrainy № 2 (2015), "Pro zatverdzhennia pravyl vykonannia polotiv derzhavnoi aviatsii Ukrainy" [On approval of the rules of flights of the state aviation of Ukraine], rozdil IX, hlava 14 – Osoblyvosti vykonannia hrupovykh polotiv. **7. Kryukov N. P., Kremen M. A.** (1983) Metodom opornyih tochek [By the reference points method], Aviatsiya i kosmonavtika, № 6, p. 26–27, № 7, p. 27–28. **8. Lebed V. H., Myrhorod Y. I., Ukrainets Y. O.** (2011), Aerohidrohazodynamika [Aerogidrogasodinamica] Kharkiv, 415 p. **9. Nemeshylov Y. O.** (2019), Modeli system upravlinnia litalnymy aparatamy ta metody eksperymentalnykh doslidzhen [Aircraft control systems models and experimental research methods], Kharkiv, 160 p. **10. Silkov V. I.** (1984), Dinamika poleta i boevogo manevrirovaniya letatelnyih apparatov, Chast 2. Ustoychivost i upravlyaemost [Dynamics of flight and combat maneuvering of aircraft], Kyiv, 318 p. **11. Krasovskiy A. A.** (1987), Spravochnik po teorii avtomaticheskogo upravleniya [Handbook on Automatic Control Theory], Moscow, 712 p. **12. Krutko P. D., Popov E. P.** (1986), Sintez upravleniya skorostyu dvizheniya letatelnyih apparatov na osnove resheniya obratnoy zadachi dinamiki [Synthesis of control of the speed of movement of aircraft on the basis of solving the inverse problem of dynamics], Dokl. AN SSSR, p. 809–812. **13. Gorbatenko S. A.** (1969) Mehanika poleta: obschie svedeniya. Uravneniya dvizheniya [Flight mechanics: general information. Equations of motion], Moscow, 500 p. **14. Tarasov V. G.** (1980), Mezhsamoletnaya navigatsiya [Inter-site navigation], – Moscow, 184 p. **15. Greg L. Zacharias** (2019), Autonomous Horizons: Autonomy in the Air Force – A Path to the Future, Volume 1: Human Autonomy Teaming (AF/ST TR 15-01). Air University Press. **16. Greg L. Zacharias** (2019), Autonomous Horizons: Autonomy in the Air Force – A Path to the Future, Volume 2: Autonomous Horizons. The Way Forward. (AF/ST TR 15-02). Air University Press.

DOI:**10.33099/2311-7249/2021-41-2-31-40**

УДК: 378:147

Спартак Юрійович Гогонянц *(кандидат військових наук, старший науковий співробітник.)*
Євген Григорович Руденко

Національний університет оборони України імені Івана Черняховського, Київ, Україна

МЕТОДИКА ОБГРУНТУВАННЯ СТРУКТУРИ ЕКСПЕРТНО-НАВЧАЛЬНОЇ СИСТЕМИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Сучасні темпи розвитку інформаційних технологій створили передумови для появи широкого спектру інструментів надання освітніх послуг із використанням технологій дистанційного навчання. Це підтверджується активізацією використання систем дистанційного навчання в умовах санітарно-епідеміологічних обмежень та необхідністю гострої економії коштів. Аналіз існуючих систем дистанційного навчання вищих військових навчальних закладів показав, що їх структура не досконала і потребує уніфікації процесу їх побудови з метою забезпечення ефективності підготовки військового фахівця. Реалізація цього процесу вимагає застосування теоретико-прикладних інструментів побудови структури експертно-навчальної системи військового призначення в системі дистанційного навчання вищих військових навчальних закладів. Головною причиною наявності зазначеного факту стала нераціональна побудова структури експертно-навчальної системи військового призначення в системі дистанційного навчання вищих військових навчальних закладів.

Виходячи із цього, метою даної роботи є формування типової науково обґрунтованої структури експертно-навчальної системи військового призначення вищого військового навчального закладу для забезпечення надання якісних сучасних освітніх послуг з використанням інформаційних технологій. У роботі використані методи: аналізу – під час дослідження особливостей структури систем дистанційного навчання вищих військових навчальних закладів з урахуванням досвіду провідних країн світу; формалізації – для змістовного опису процесу функціонування системи дистанційного навчання; таксономії – для багатовимірного порівняльного аналізу структур системи дистанційного навчання вищого військового навчального закладу; синтезу – для формування типової структури експертно-навчальної системи військового призначення. Розроблена методика визначення доцільного варіанту побудови структури експертно-навчальної системи військового призначення в системі дистанційного навчання вищого військового навчального закладу, що базується на процедурах багатовимірного порівняльного аналізу показників якості функціонування показників. За результатами застосування методики розроблена типова структура експертно-навчальної системи військового призначення системи дистанційного навчання вищого військового навчального закладу та вироблені рекомендації щодо організації роботи системи дистанційного навчання вищого військового навчального закладу. Використання раціональної структури експертно-навчальної системи військового призначення дає можливість розв'язувати складні та проблемні ситуації у процесі підготовки військових фахівців вищих військових навальних закладів. Цей факт дозволяє усунути обмеження у практиці побудови структури експертно-навчальної системи військового призначення і створює нову можливість охопити ширший спектр факторів, що впливають на якість роботи. Застосування цієї методики дозволяє системі дистанційного навчання вищого військового навчального закладу прогнозувати результати спільного функціонування відповідних підсистем системи дистанційного навчання з урахуванням їх внеску в загальний результат.

Ключові слова: *дистанційне навчання; експертно-навчальна система; таксономія; аналіз; синтез.*

Вступ

Сучасні тенденції розвитку освітніх технологій вимагають зусиль щодо розвитку дистанційного навчання (далі ДН) як одного з ефективних інструментів реалізації моделі навчання впродовж життя [1]. Актуалізація цього питання набуває характеристик у контексті санітарно-епідеміологічних обмежень у всьому світі та вимагає вдосконалення процедур надання якісних освітніх послуг.

Дистанційне навчання - це особлива форма цілеспрямованого процесу оволодіння знаннями, вміннями та навичками, відмітною рисою якого є взаємодія віддалених учасників навчального процесу в спеціалізованому середовищі, заснованому на сучасних психолого-педагогічних та інформаційно-комунікаційних технологіях [2] .

Світові тенденції розвитку дистанційного навчання у просунутих країнах свідчать про зусилля забезпечити, з одного боку, наближення віртуального навчального середовища до реального життя за допомогою використання імітаційних технологій та експертно-навчальних систем, з іншого - впровадження в навчання окремих навичок та знання слухачів. Перспективні засоби дистанційного навчання повинні забезпечувати ефективну підготовку фахівців з урахуванням потреб та можливостей, запровадження рейтингової системи їх оцінювання на відомчому рівні.

Розвиток інженерії знань та методів створення експертних систем визначив архітектуру інтелектуальних навчаючих систем у вигляді сукупності взаємодіючих експертних систем, кожна з яких оперує зі своїм типом знань. Розвиток такого підходу обумовив появу спеціалізованого класу експертних систем – експертно- навчальних систем (ЕНС). Під ЕНС розуміють програмну систему, яка реалізує певну педагогічну ціль на основі знань експертів у відповідній предметній галузі, в галузі діагностування знань осіб, що навчаються, та управління навчанням, яка дозволяє демонструвати поведінку на рівні експертів [3].

Існуючий науково-методичний апарат не повністю враховує вплив на ефективність системи дистанційного навчання якості її компонентів і отримує об’єктивний прогноз результату її функціонування для вибору найбільш відповідного варіанту.

Використовуються підходи до окремої оцінки ефективності елементів системи дистанційного навчання та відповідні показники їх якості. Це обмежує можливість врахування важливих факторів у процесі прийняття рішень і вимагає розгляду більш доцільної структури експертно-навчальної системи військового призначення (далі ЕНС ВП) у вищих військових навчальних закладах (далі ВВНЗ).

Застосування технологій дистанційного навчання, поряд із покращенням якості функціонування ЕНС ВП, дозволить знизити вартість навчання, суттєво зменшивши потребу у відповідному обладнанні, скоротивши час та кількість поїздок до ВВНЗ.

Постановка проблеми. Сьогодення вимагає забезпечення більш якісного освітнього процесу та вдосконалення професійної підготовки майбутніх військових фахівців. Однак на сьогодні розробка таких технологій та систем знаходиться у стані досліджень. Це дає змогу стверджувати, що забезпечення якісної підготовки військових фахівців можна досягти завдяки раціональній побудові структури ЕНС ВП у ВВНЗ, яка дозволить знаходити самостійні рішення в складних проблемних та суперечливих ситуаціях з різним ступенем невизначеності, що зустрічаються під час навчання. Дослідження окресленої проблеми вимагає впровадження в освітній процес закладів військової освіти ЕНС ВП, використання якої реалізує підвищення якості професійної підготовки військового фахівця.

Аналіз останніх досліджень і публікацій. У роботі Б. Литвак [4] показано, що сучасною тенденцією в підготовці майбутніх фахівців є використання нового класу інформаційних технологій – експертно-навчальних систем, основним призначенням яких є підвищення якості освітнього процесу. У роботах науковців [1,5–7] розглянуто сучасні інформаційні технології – експертно-навчальні системи, що використовуються під час підготовки фахівців. Проблема професійної підготовки фахівців за допомогою використання ЕНС знайшла відображення у роботах вчених [8-9]. Сучасною тенденцією в підготовці майбутніх військових фахівців є використання нового класу інформаційних технологій навчання – експертно-навчальної системи військового призначення, основним призначенням яких є розв’язання поставлених завдань [10-12]. У наших попередніх дослідженнях [13-14] обґрунтовано архітектуру експертно-навчальної системи з підготовки військових фахівців.

Метою статті є обґрунтування типової науково обґрунтованої структури ЕНС ВП у системи дистанційного навчання вищого військового навчального закладу.

Виклад основного матеріалу дослідження

Завдання щодо обґрунтування системи показників ефективності побудови архітектури ЕНС ВП вищого військового навчального закладу, передбачає урахування їх відповідності вимогам щодо об’єктивного відображення субпроцесів, які перебігають в межах відповідних підсистем управління, забезпечення, конфіденційності і безпеки інформації; контроля якості знань [15-16], а також можливостями центрального репозиторію ресурсів (далі ЦРР) СДН та моделлю розподілу видів навчальних занять.

Ураховуючи особливості визначення раціональної структури і складу системи доцільно розглядати структуру під час вирішення сукупності окремих завдань щодо управління освітнім процесом, формування навчального контенту і удосконалення центрального репозиторію ресурсів системи ДН, розгортання системи контролю якості знань та зворотнього зв’язку.

При цьому досліджуються такі показники (характеристики) під час виконання завдань, які визначаються в основному структурою системи, а не її складом.

Стосовно ЕНС ВП такими якісними показниками прийнято [13]:

актуальність – відповідність вимогам керівних документів;

структурованість – відповідність навчального контенту відповідній моделі ДН та підтримка міжнародних стандартів;

наявність зворотнього зв'язку;

економічність – припустимий виграш від ефекту ДН до загальних витрат;

мобільність – здатність системи забезпечувати доступ до навчального контенту і Центрального репозиторію системи ДН з мобільних пристроїв без обмежень;

стійкість і захищеність – здатність ліцензійного програмного забезпечення забезпечити конфіденційність і безпеку інформації.

Для систем ДН ВВНЗ такими кількісними показниками (характеристиками) можуть бути:

інтенсивність підготовки фахівців за допомогою системи ДН;

інтенсивність підвищення кваліфікації педагогічного складу з питань використання технологій дистанційного навчання;

$P_{упр}$ – середня ймовірність виконання завдань підсистемою управління ДН;

$P_{цр}$ – ймовірність виконання завдань центральним репозиторієм ресурсів системи ДН;

$P_{еф.зан}$ – ефективність моделі розподілу видів навчальних занять;

$P_{контр}$ – ймовірність виконання завдань підсистеми контроля якості знань;

$P_{заб}$ – ймовірність виконання завдань підсистемою забезпечення ДН;

$P_{зах}$ – ймовірність виконання завдань підсистемою конфіденційності і безпеки інформації за припущенням, що контент, конфіденційна інформація некатегоровані і не можуть бути використані для ототожнення користувачів системи;

$C_{обл}$ – вартість мінімального комплекту серверного обладнання для розгортання системи ДН.

$C_{пс}$ – вартість підготовки слухача за звітній період;

$C_{пз}$ – вартість оновлення ПЗ за звітній період.

Важливим показником (важливою характеристикою) ЕНС ВП є час, який витрачається на виконання завдань відповідно до цільового призначення.

Порівнювальне оцінювання варіантів системи ДН може бути здійснено за допомогою таксономічного методу [7].

Враховуючи вимоги до систем ДН, критерієм відбору раціонального варіанту системи є максимальне значення показника ваги варіанту побудови системи

$$max\, 1 - \beta, \qquad (1)$$

Послідовність розрахунку показників якості функціонування системи дистанційного навчання вищого військового навчального закладу.

На першому етапі проводиться визначення значення середньої ймовірності виконання завдань підсистемою управління ДН на підставі результатів порівняльного аналізу наявних платформ дистанційного навчання

$$P_{упр} = 1 - e^{\left(-\frac{N_{вик}}{N_{завд}}\right)}, \qquad (2)$$

де $N_{вик}$ – математичне сподівання кількості завдань, що виконані системою ДН за визначений період часу;

$N_{завд}$ – кількість завдань, що покладаються на систему ДН за визначений період часу.

На другому етапі визначається ймовірність виконання завдань центральним репозиторієм ресурсів системи ДН

$$P_{цр} = P_{дост}\frac{N_{зап}}{N_{норм}}, \qquad (3)$$

де $N_{зап}$ – математичне сподівання кількості запитів до ЦРР СДН щодо доступу до навчального матеріалу електронної бібліотеки та ресурсів навчального призначення;

$N_{норм}$ – кількість електронних видань електронної бібліотеки та ресурсів навчального призначення за відповідною тематикою;

$P_{дост}$ – ймовірність доступу до електронних видань електронної бібліотеки та ресурсів навчального призначення за відповідною тематикою.

На третьому етапі визначається ефективність моделі розподілу видів навчальних занять – середня ймовірність відповідності визначеній керівними документами моделі навчання

$$P_{еф.зан} = \frac{1}{n_{нз}}\sum_{j}^{n_{нз}}\frac{T_j}{T_{ет.j}};\ j = \overline{1, n_{нз}}, \qquad (4)$$

де $n_{нз}$ – кількість видів навчальних занять в моделі;

T_j – кількість годин, що виділені на проведення j-го виду заняття;

$T_{ет.j}$ – еталона кількість годин, що виділені на проведення j-го виду заняття.

На четвертому етапі визначається ймовірність виконання завдань підсистеми контроля якості знань та зворотного зв'язку

$$P_{контр} = \begin{cases} \frac{N_{завд}}{N_{тест}}, \text{ інакше } 1, N_{тест} \le n_{кор} N_{завд}, \end{cases} \qquad (5)$$

де $N_{тест}$ – кількість тестових у банку питань;

$N_{завд}$ – кількість тестів у завданні;

$n_{кор.}$ – кількість користувачів, що тестуються.

На п'ятому етапі визначається ймовірність виконання завдань підсистемою забезпечення ДН.

В основу послідовності розрахунку $P_{заб.}$ ймовірність виконання завдань ДН покладено комплексний підхід до оцінювання ефективності функціонування підсистеми забезпечення ДН на основі урахування внесків підсистем нормативно-правового, організаційного, науково-методичного, інформаційно-телекомунікаційного, математичного та програмного, матеріально-технічного, кадрового, фінансово-економічного забезпечення.

Визначення показника ефективності функціонування системи ДН проводиться як середньозважене значення ймовірності виконання завдання системою ДН з урахуванням ступеня важливості результатів функціонування підсистем нормативно-правового, організаційного, науково-методичного, інформаційно-телекомунікаційного, математичного та програмного, матеріально-технічного, кадрового, фінансово-економічного забезпечення, а також негативного впливу суттєвих чинників на реалізацію потенційних можливостей системи

$$P_{заб} = \sum_{i=1}^{8} (1 - K_i) \cdot B_i \cdot P_i(t_n), \qquad (6)$$

де $P_i(t_n) = n_i \frac{\mu_i t_n}{N_i}$ – ймовірнісні виконання завдань i-ю підсистемою забезпечення (нормативно-правового, організаційного, науково-методичного, інформаційно-телекомунікаційного, математичного та програмного, матеріально-технічного, кадрового, фінансово-економічного) ДН ВВНЗ як функції ступеня реалізації комплексу відповідних заходів;

N_i – кількість завдань, що виконує i-а підсистема;

μ_i – продуктивність виконання завдань i-ю підсистемою;

n_i – кількість виконавчих елементів i-ї підсистеми;

B_i – важливість внесків i-ю підсистемою системи забезпечення;

K_i – коефіцієнт невідповідності ВВНЗ ліцензійним вимогам.

На шостому етапі визначається ймовірність виконання завдань підсистемою конфіденційності і безпеки інформації, за припущенням, що контент, конфіденційна інформація некатегорована і не можуть бути використані для ототожнення користувачів системи

$$P_{зах} = 1 - e^{-I_{нд} T_{під} (1 - P_{нд})}, \qquad (7)$$

де $P_{нд}$ – ймовірність несанкціонованого доступу до облікових даних користувачів та контенту ДН;

$I_{нд}$ – інтенсивність спроб несанкціонованого доступу до облікових даних користувачів та контенту ДН;

$T_{під}$ – тривалість функціонування системи ДН.

На сьомому етапі визначається вартість комплекту серверного обладнання для розгортання системи ДН

$$C_{обл.} = \sum_{p=1}^{P} n_{обл.р} C_{обл.р}; \; p = \overline{1, P}, \qquad (8)$$

де $C_{обл.р.}$ – вартість p-го типу серверного обладнання;

$n_{обл.р.}$ – кількість одиниць p-го типу серверного обладнання.

На восьмому етапі визначається вартість підготовки слухача за звітній період

$$C_{пс} = \sum_{s=1}^{S} C_{пс.s}, \qquad (9)$$

де $C_{пс.s}$ – вартість підготовки слухача за видами утримання у звітному періоді.

На восьмому етапі визначається вартість оновлення програмного забезпечення з розрахунку на 100 од. ПЕОМ

$$C_{он} = \frac{T_{екс}}{T_{ліц}} C_{ПЗ}, \qquad (10)$$

де $C_{ПЗ}$ – вартість програмного забезпечення;

$T_{екс.}$ – тривалість експлуатації програмного забезпечення;

$T_{ліц}$ – час активації програмного забезпечення.

Результати розрахунків зводяться у зведену таблицю варіантів побудови системи ДН ВВНЗ.

Таксономічні методи є методами багатомірного порівняльного аналізу [7,11]. У загальному випадку під таксономією розуміється теорія класифікації і систематизації складноорганізованих галузей діяльності, які мають звичайно ієрархічну побудову. Виникає від слова “таксон” – група дискретних об’єктів, які пов’язані загальними властивостями і ознаками, що дає підставу для присвоювання ним визначеної таксономічної категорії – рангу. Метод може застосовуватися не тільки під час порівняльного аналізу об’єктів у

галузі природних, політичних наук, а й під час дослідження систем військового призначення, у тому числі технічних систем.

Основним елементом, що використовується у таксономічному методі є, так звана, таксономічна відстань. Вона визначається за правилами аналітичної геометрії між точками – показниками, що розташовані у багатомірному просторі [7]. Розмірність цього простору визначається кількістю показників, які характеризують функціонування системи, що досліджується.

За допомогою таксономічної відстані можна визначити розташування точки щодо інших та її місце в усій сукупності, а отже, класифікувати і впорядкувати як показники, так і варіанти системи (альтернативи).

Як і в попередньому випадку вихідними даними щодо визначення раціонального варіанту

системи методом таксономії є показники ефективності, які можуть бути задані матрицею:

$$\left[E_{ij}\right], i=\overline{1,N},\ j=\overline{1,R}, \qquad (11)$$

Під час аналізу варіантів системи можуть використовуватися і інші параметри, які зводяться у ту ж матрицю (11). Оскільки елементи матриці можуть мати різні одиниці вимірювання доцільно для полегшення обчислювань їх привести до стандартизованого вигляду за формулою

$$Z_{ij}=\frac{E_{ij}-E_j}{S_j}, \qquad (12)$$

де $E_j \frac{1}{N}\sum_i E_{ij},\ i=\overline{1,N}$;

$S_j=\frac{1}{N}\sum_i\left(E_{ij}-E_j\right)^{\frac{1}{2}}$;

E_j – середнє арифметичне значення j –го показника по варіантах;

S_j – середнє квадратичне відхилення j –го показника.

Z_{ij} – стандартизоване значення j –го показника ефективності функціонування для i –го варіанта системи

$$C_{rs}=\frac{1}{N}\sum_{i=1}^{N}\left|Z_{ri}-Z_{si}\right|,\ r,s=1,R, \qquad (13)$$

Обчислені відстані дозволяють упорядкувати і класифікувати показники, що розглядаються.

Відстані між показниками (точками) багатомірного простору володіють властивостями

$$C_{rr}=0;\ C_{rs}=C_{sr};\ C_{rs}\le C_{rl}+C_{ls}, \qquad (14)$$

Отримана симетрична матриця відстаней дозволяє визначити пріоритетний ряд показників (параметрів) на основі надання їм коефіцієнтів важливості. Для цього можна використати підхід, що ґрунтується на обчисленні так званої критичної відстані [7]. За критичну відстань можна вибрати найбільшу відстань між показниками (параметрами), які розташовані поблизу один від одного, що вказує на найбільш сильні зв'язки між показниками (параметрами). Критична відстань розраховується за формулою

$$C_k=\max\ \min C_{rs};\ r,s=\overline{1,R};\ r\ne s, \qquad (15)$$

Після цього для кожного j-го показника (параметра) знаходять всі відстані, що не перевищують критичну

$$\rho_{js}=\left\{C_{js}\le C_k\right\},\ j=r=\overline{1,R};\ s=\overline{1,R}, \qquad (16)$$

Необхідно відзначити, що значення відстаней, що обраховуються як $\min C_{rs}$, визначаються з аналізу рядків матриці відстаней.

Значення також визначаються по рядках цієї матриці. Далі відстані підсумовуються

$$Q_j=\sum\rho_{js},\ s=\overline{1,R}, \qquad (17)$$

При цьому вилучаються всі S, які не відповідають виразу (16).

Вважається, що важливість показника (параметра) тим більше, чим більше сума відстаней показника (параметра) від сусідніх.

Тому обирається показник (параметр), для якого сума відстаней (17) найбільша

$$Q_m=\max_j Q_j,\ j=\overline{1,R}, \qquad (18)$$

і обчислюється коефіцієнт важливості показника (параметра)

$$\lambda_j=\frac{Q_j}{Q_m}, \qquad (19)$$

Очевидне, що найбільш важливому показнику (параметру) відповідає значення $\lambda_j=1$.

Для розв'язання задачі визначення раціонального варіанта системи (альтернативи) необхідно насамперед розділити показники на показники – стимулятори і показники – дестимулятори [7]. Показники, збільшення яких спричинює зростання кінцевого ефекту функціонування системи називають стимуляторами на відміну від дестимуляторів, зростання яких спричиняє зменшення ефекту функціонування системи. Після цього будується еталонний варіант системи, що досліджується, якому відповідає точка P_0 в багатомірному просторі з координатами (значеннями стандартизованих показників)

$$Z_{01}, Z_{02},..., Z_{0j},..., Z_{0R}, \qquad (20)$$

де $Z_{0j}=\max^{Z_{ij}}$ коли $j\in S$;

$Z_{0j}=\min_i^{Z_{ij}}$, коли $j\in Д$;

$S, Д$ – множини стимуляторів і дестимуляторів відповідно;

Z_{ij} – стандартизоване значення j-го показника, для і-го варіанта системи.

Відстані між точкою P_0 та точками, які відповідають варіантам системи (альтернативам), визначаються за формулою

$$C_{i0}=\left[\sum\left(Z_{ij}-Z_{0j}\right)^2\right]^{\frac{1}{2}},\ i=\overline{1,R},\ j=\overline{1,R}, \qquad (21)$$

Ступінь переваги варіантів системи визначається за формулою

$$\beta_i=\frac{C_{i0}}{C_0},\ i=1,N, \qquad (22)$$

де; $C_0=C_0+2S_0$;

$C_0=\frac{1}{N}\sum_i C_{i0}$;

$S_0=\left[\frac{1}{N}\sum_i\left(C_{i0}-C_0\right)\right]^{\frac{1}{2}}$.

Чим ближче значення β_i до нуля, тим краще варіант системи, що досліджується. Таким чином, використання таксономічних методів дозволяє визначити як важливості показників (параметрів),

що характеризують ефективність функціонування системи, так і порівнювати варіанти системи (альтернативи).

Вихідні данні для проведення розрахунків відповідають варіантам побудови СДН для підготовки військових фахівців за очною формою навчання (вар. 1-3), для підготовки фахівців за дуальною формою навчання (вар. 4-9), для підготовки фахівців за дистанційною формою навчання (вар. 10-15), для підготовки фахівців на КППК за дистанційною формою навчання (вар. 16-18). (табл. 1).

Для варіантів 1-3 ступінь задоволення потреб у інформаційному ресурсі складає 0,55-0,9, з ефективністю забезпечення 0,7-0,9. Для варіантів 4-9 для дослідження прийнято, що коефіцієнт відповідності функціоналу системи управління освітнім процесом для двох варіантів (Рупр): 77 і 66, ступінь задоволення потреб у інформаційному ресурсі для кожного варіанту управління в межах 0,55-0,9, з ефективністю забезпечення в межах 0,7-0,9.

Для варіантів 10-18 прийнято, що коефіцієнт відповідності функціоналу системи управління освітнім процесом для двох варіантів: 77 і 66, ступінь задоволення потреб у інформаційному ресурсі для кожного варіанту управління в межах 0,55-0,9, з ефективністю забезпечення в межах 0,7-0,9. Кількість і зміст варіантів визначаються можливостями щодо побудови системи і реальними значеннями показників, що їх характеризують.

Таблиця 1

Вихідні данні для багатовимірного порівняльного аналізу варіантів побудови системи ДН

№ варіанту	Показник, одиниці виміру, номер							
	$T_{підг}$, міс	$Р_{упр}$	$Р_{цр}$	$Р_{конт}$	$Р_{заб}$	$С_{обл}$, тис. грн	$С_{пс}$, тис. грн	$С_{он}$, тис.грн на рік
	1	2	3	4	5	6	7	8
Для підготовки фахівців за очною формою навчання								
1	24	0,77	0,55	0,84	0,7	60	427	4,69
2	24	0,77	0.75	0,84	0,8	60	427	4,69
3	24	0,77	0.9	0,84	0,9	60	427	4,69
Для підготовки фахівців за дуальною формою навчання								
4	6	0,77	0,55	0,9	0,7	120	427	4,69
5	6	0,77	0.75	0,84	0,8	120	427	4,69
6	6	0,77	0.9	0,9	0,9	120	427	4,69
7	6	0,66	0,55	0,84	0,7	120	427	4,69
8	6	0,	0.75	0,9	0,8	120	427	4,69
9	6	0,66	0.9	0,9	0,9	120	427	4,69
Для підготовки фахівців за дистанційною формою навчання								
10	9	0,77	0,55	0,9	0,7	220	273	8,5
11	9	0,77	0.75	0,84	0,8	220	273	8,5
12	9	0,77	0.9	0,9	0,9	220	273	8,5
13	9	0,66	0,55	0,9	0,7	220	273	8,5
14	9	0,66	0.75	0,84	0,8	220	273	8,5
15	9	0,66	0.9	0,84	0,9	220	273	8,5
Для підготовки фахівців на КППК за дистанційною формою навчання								
16	2	0,77	0,55	0,84	0,9	220	17,6	10,2
17	2	0,77	0.75	0,9	0,9	220	17,6	10,2
18	2	0,77	0.9	0,9	0,9	220	17,6	10,2
Тип ознаки	-	+	+	+	+	-	-	-
Mj	9,33	0,7333	0,73	0,89	0,8	160	307,4	6,67
σj	6,96	0,518	0,14	0,022	0,089	63,24	68,2	2,27

В ході розрахунків до уваги прийняті якісні показники системи описані у п. 2. у відповідності до змісту завдань побудови системи ДН. Тип ознаки відповідного показника визначається характером впливу на результат функціонування, як негативний або позитивний.

Аналіз результатів розрахунків щодо визначення раціонального варіанту побудови системи ДН показав, що за умов підготовки

фахівців за очною формою навчання в межах зазначеного бюджету раціональним варіантом побудови системи ДН буде варіант №3. За таких умов задоволення потреб у інформаційному ресурсі ЦРР СДН складатиме 90%, а забезпечення потреб ДН складатиме 90% (табл. 2).

Для підготовки фахівців за дуальною формою навчання в межах зазначеного бюджету раціональним варіантом побудови системи ДН буде варіант №9. За таких умов задоволення потреб у інформаційному ресурсі ЦРР СДН, забезпечення потреб ДН складатиме 90%. При цьому можливості підсистеми управління освітнім процесом не повинна бути нижчими за значення 0,66.

Результати розрахунків та визначення раціонального варіанту побудови системи ДН.

Для підготовки фахівців та проведення курсів перепідготовки та підвищення кваліфікації за дистанційною формою навчання доцільними варіантами будуть №15 і №18 відповідно. Значення відповідних показників ефективності мають ідентичні значення за винятком вартісних показників, що підтверджує твердження уніфікованого підходу до побудови систем ДН ВВНЗ.

Таблиця 2

Зведені результати багатовимірного порівняльного аналізу варіантів побудови системи ДН

Варіант		Показник, номер								Cio	dio	di	M[Cio]	σ[Cio]	Co
Ранг	№	1	2	3	4	5	6	7	8				23,9	17,42	76,16
		Для підготовки фахівців за очною формою навчання													
18	1	2,104	0,707	-1,285	0	-1,12	-1,581	1,753	-0,87	8,11	0,106	0,893512			
17	2	2,104	0,707	1,42	0	0	-1,581	1,753	-0,87	7,39	0,097	0,902897			
15	3	2,104	0,707	1,21	0	1,12	-1,581	1,753	-0,87	7,31	0,096	0,903978			
		Для підготовки фахівців за дуальною формою навчання													
14	4	-0,478	0,707	-1,285	0	-1,12	-0,632	1,753	-0,87	7,04	0,092	0,907528			
10	5	-0,478	0,707	1,42	0	0	-0,632	1,753	-0,87	6,2	0,081	0,918512			
12	6	-0,478	-1,414	1,21	0	1,12	-0,632	1,753	-0,87	6,46	0,084	0,915104			
16	7	-0,478	-1,414	-1,285	0	-1,12	-0,632	1,753	-0,87	7,35	0,096	0,903425			
13	8	-0,478	-1,414	1,42	0	0	-0,632	1,753	-0,87	6,55	0,086	0,913884			
9	9	-0,478	0,707	1,21	0	1,12	-0,632	1,753	-0,87	6,1	0,08	0,919803			
		Для підготовки фахівців за дистанційною формою навчання													
8	10	-0,0478	0,707	-1,285	0	-1,12	0,948	-0,5048	-0,87	5,81	0,076	0,923699			
5	11	-0,0478	0,707	1,42	0	0	0,948	-0,5048	0,807	5,05	0,066	0,933693			
6	12	-0,0478	-1,414	1,21	0	1,12	0,948	-0,5048	0,807	5,36	0,07	0,929546			
11	13	-0,0478	-1,414	-1,285	0	-1,12	0,948	-0,5048	0,807	6,41	0,084	0,915838			
7	14	-0,0478	-1,414	1,42	0	0	0,948	-0,5048	0,807	5,47	0,071	0,92808			
3	15	-0,0478	0,707	1,21	0	1,12	0,948	-0,5048	0,807	4,92	0,064	0,935285			
		Для підготовки фахівців на КПІПК за дистанційною формою навчання													
4	16	-1,052	0,707	-1,285	0	-1,12	0,948	-4,249	1,556	4,96	0,065	0,934839			
2	17	-1,052	0,707	1,42	0	0	0,948	-4,249	1,556	3,68	0,048	0,951676			
1	18	-1,052	0,707	1,21	0	1,12	0,948	-4,249	1,556	15,25	0,2	0,799654			
	Zoj	-1,052	0,707	1,42	0	1,12	-1,581	-4,249	-0,87						

Висновки і перспективи подальших досліджень

Аналіз стану систем дистанційного навчання вищих військових навчальних закладів показав, що вони потребують певного удосконалення структури, що не можливо без наукового підходу.

Розроблена методика визначення доцільного варіанту побудови структури ЕНС ВП у системі дистанційного навчання вищого військового навчального закладу, що базується на процедурах багатовимірного порівняльного аналізу показників якості функціонування показників.

Надійність та точність результатів оцінки результатів роботи визначається використанням перевірених, адекватних реальному процесу науково-методичного апарату оцінки, залученням фахівців у цій галузі, що мають практичний досвід використання технологій дистанційного навчання в спеціалізованому експертному середовищі. Її складність та універсальність компенсується ретельною підготовкою до її впровадження з урахуванням характеристик системи ДН на основі

її глибокого розкладання та чітко визначених правил оцінки відповідних показників її ефективності.

Подальші дослідження полягають у реалізації структури ЕНС військового призначення у систему ДН ВВНЗ.

Література

1. Національна стратегія розвитку освіти в Україні на період до 2021 року: затверджена. Указ Президента України від 25 червня 2013 р. № 344/2013. Офіційний вісник Президента України. 2013. 05 липня. № 17. С. 31. **2.** Про затвердження Концепції дистанційного навчання у Збройних Силах України: наказ Міністерства оборони України від 21.12.2015 р. № 744. URL: http://www.viti.edu.ua/files/npb/dfn3.pdf **3. Петрушин В. А.** Экспертно-обучающие системы. Киев: Наук. думка, 1992. 196 с. **4. Литвак Б. Г.** Разработка управленческого решения : Б. Г. Литвак. – 3-е изд., испр. – М. :Дело, 2002. – 392 с. **5. Голенков В. В.,** Гулякина Н. А., Елисеева О. Е. Инструментальные средства проектирования интеллектуальных обучающих систем: методическое пособие по курсу “Интеллектуальные обучающие и тренажерные системы” для студентов специальности. Искусственный интеллект. Минск: БГУИР, 1999. 102 с. **6. Джексон П.** Введение в экспертные системы. Москва: Издательский дом “Вильямс”, 2001. 624 с. **7. Нейлор К.** Как построить экспертную систему. Москва: Энергоатомиздат, 1991. 286 с **8. Костюченко М. П.** Інформаційно-кібернетичні та психолого-дидактичні аспекти проектування експертно-навчальних систем. Искусственный интеллект. 2013. № 4. С. 127–137. **9. Словак К.** Використання експертних систем під час узагальнення та систематизації у процесі навчання вищої математики. Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. Серія: педагогіка. 2011. № 1. С. 141–148. **10. Загорка О. М.,** Мосов С.П., Сбитнєв А.І., Стужук П.І. Елементи дослідження складних систем військового призначення: навч. посіб. / Київ. НАОУ, 2005. 124 с. **11. Беляев М. И.,** Гриншкун В. В., Краснова Г. А. Технология создания электронных средств обучения. **12. Сааті Т.,** Кернс К. Аналітичне планування. Организація систем: книга. Пер. с англ. – New York, 1991. 224 с. **13. Гогонянц С.Ю.,** Георгадзе О.А., Руденко Є.Г. Архітектура та класифікація експертно-навчальних систем з підготовки військових фахівців. Сучасні інформаційні технології у сфері безпеки та оборони. 2020. №2. С.133-138. **14. Шевчук О. Б.** Педагогічні принципи проектування та розробки експертних систем навчання. Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. Серія: педагогіка. 2016. № 1. С. 38–43. **15. Сиротенко А. М.** Теорія і практика дистанційного навчання у Збройних Силах України. Ч. 1: Основи використання технологій дистанційного навчання в освітньому процесі вищих військових навчальних закладів та військових навчальних підрозділів закладів вищої освіти : навч.-метод. посіб. / колектив авторів. / Київ. НУОУ ім. Івана Черняховського, 2020. 220 с. **16. Салкуцан С. М.** Обгрунтування рекомендацій щодо вдосконалення системи дистанційного навчання Збройних Сил України. науково-дослідна робота / колектив авторів. / Київ. НУОУ ім. Івана Черняховського, 2019. 170 с.

МЕТОДИКА ОБОСНОВАНИЯ СТРУКТУРЫ ЭКСПЕРТНО-ОБУЧАЮЩЕЙ СИСТЕМЫ ВОЕННОГО НАЗНАЧЕНИЯ

Спартак Юрійович Гогонянц *(кандидат военных наук, старший научный сотрудник)*
Євген Григорович Руденко

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Современные темпы развития информационных технологий создали предпосылки для появления широкого спектра инструментов предоставления образовательных услуг с использованием технологий дистанционного обучения. Это подтверждается активизацией использования систем дистанционного обучения в условиях санитарно-эпидемиологических ограничений и необходимостью острой экономии средств. Анализ существующих систем дистанционного обучения высших военных учебных заведений показал, что их структура не совершенна и требует унификации процесса их построения с целью обеспечения эффективности подготовки военного специалиста. Реализация этого процесса требует применения теоретико-прикладных инструментов построения структуры экспертно-обучающей системы военного назначения в системе дистанционного обучения высших военных учебных заведений. Главной причиной наличия указанного факта стала нерациональная построение структуры экспертно-обучающей системы военного назначения в системе дистанционного обучения высших военных учебных заведений.

Исходя из этого, целью данной работы является формирование типичной научно обоснованной структуры экспертно-обучающей системы военного назначения высшего военного учебного заведения для обеспечения предоставления качественных современных образовательных услуг с использованием информационных технологий. В работе использованы методы: анализа - при исследовании

особенностей структуры систем дистанционного обучения высших военных учебных заведений с учетом опыта ведущих стран мира; формализации - для содержательного описания процесса функционирования системы дистанционного обучения; таксономии - для многомерного сравнительного анализа структур системы дистанционного обучения высшего военного учебного заведения; синтеза - для формирования типовой структуры экспертно-обучающей системы военного назначения. Разработана методика определения целесообразного варианта построения структуры экспертно-обучающей системы военного назначения в системе дистанционного обучения высшего военного учебного заведения, основанного на процедурах многомерного сравнительного анализа показателей качества функционирования показателей. По результатам применения методики разработана типовая структура экспертно-обучающей системы военного назначения системы дистанционного обучения высшего военного учебного заведения и выработаны рекомендации по организации работы системы дистанционного обучения высшего военного учебного заведения. Использование рациональной структуры экспертно-обучающей системы военного назначения дает возможность решать сложные и проблемные ситуации в процессе подготовки военных специалистов высших военных стремительных заведений. Этот факт позволяет устранить ограничения в практике построения структуры экспертно-обучающей системы военного назначения и создает новую возможность охватить более широкий спектр факторов, влияющих на качество работы. Применение этой методики позволяет системе дистанционного обучения высшего военного учебного заведения прогнозировать результаты совместного функционирования соответствующих подсистем системы дистанционного обучения с учетом их вклада в общий результат.

Ключевые слова: *дистанционное обучение, экспертно-обучающая система, таксономия, анализ, синтез.*

METHODOLOGY FOR JUSTIFICATION OF THE STRUCTURE OF THE EXPERT-TRAINING SYSTEM OF MILITARY PURPOSE

Spartak Hohoniants *(**candidate of military sciences, senior researcher**)*
Evgeny Rudenko

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

The current pace of development of information technology has created the preconditions for the emergence of a wide range of tools for providing educational services using distance learning technologies. This is confirmed by the intensification of the use of distance learning systems in the conditions of sanitary and epidemiological restrictions and the need for acute cost savings. Analysis of existing distance learning systems of higher military educational institutions has shown that their structure is not perfect and requires unification of the process of their construction in order to ensure the effectiveness of military training. The implementation of this process requires the use of theoretical and applied tools to build the structure of the expert-educational system of military purpose in the system of distance learning of higher military educational institutions. The main reason for this fact was the irrational construction of the structure of the expert-educational system of military purpose in the system of distance learning of higher military educational institutions.

Based on this, the purpose of this work is to form a typical scientifically sound structure of the expert-educational system of military purpose of a higher military educational institution to ensure the provision of quality modern educational services using information technology. The following methods are used in the work: analysis - during the study of the peculiarities of the structure of distance learning systems of higher military educational institutions, taking into account the experience of the leading countries of the world; formalization - for a meaningful description of the process of functioning of the distance learning system; taxonomy - for multidimensional comparative analysis of the structures of the distance learning system of a higher military educational institution; synthesis - to form a typical structure of the expert training system for military purposes. A method for determining the appropriate option for building the structure of the expert-educational system of military purpose in the system of distance learning of higher military educational institution, based on the procedures of multidimensional comparative analysis of indicators of the quality of functioning of indicators. Based on the results of the application of the methodology, a standard structure of the expert-educational system of military purpose of the distance learning system of a higher military educational institution was developed and recommendations were made on the organization of the distance learning system of a higher military educational institution. The use of a rational structure of the expert training system for military purposes makes

it possible to solve complex and problematic situations in the process of training military specialists in higher military bulk institutions. This fact eliminates the limitations in the practice of building the structure of the expert training system for military purposes and creates a new opportunity to cover a wider range of factors that affect the quality of work. The application of this technique allows the distance learning system of a higher military educational institution to predict the results of joint operation of the respective subsystems of the distance learning system, taking into account their contribution to the overall result.

Key words: *distance learning, expert-educational system, taxonomy, analysis, synthesis.*

References

1. National strategy for the development of education in Ukraine for the period up to 2021 : hardened. Decree of the President of Ukraine dated 25 chervnya 2013 p. No. 344/2013. Official notice of the President of Ukraine. 2013.05 linden. No. 17. P. 31. **2.** About the consolidation of the Concept of remote control at the Zbroynykh Forces of Ukraine: the mandate of the Ministry of Defense of Ukraine from 21.12.2015. No. 744. URL: http://www.viti.edu.ua/files/npb/dfn3.pdf **3. Petrushin V. A.** Expert training systems. Kiev: Nauk. Dumka, 1992. 196 p. **4. Litvak B. G.** Development of a management solution: B. G. Litvak. - 3rd ed., Rev. - M. : Delo, 2002. 392 p. **5. Golenkov V. V.,** Gulyakina N. A., Eliseeva O. E. Instrumental tools for designing intelligent teaching systems: a methodological guide for the course "Intellectual teaching and training systems" for students of the specialty. Artificial Intelligence. Minsk : BSUIR, 1999. 102 p. **6. Jackson P.** Introduction to expert systems. Moscow : Williams Publishing House, 2001. 624 p. **7. Naylor K.** How to build an expert system. Moscow : Energoatomizdat, 1991. 286 p. **8. Kostyuchenko M. P.** Information-cybernetic and psychological-didactic aspects of the design of expert systems. Artificial Intelligence. 2013. No. 4. P. 127–137. **9. Slovak K.** Vikoristannya of expert systems for an hour of publicizing and systematization in the process of developing the best mathematics. Scientific notes of the Ternopil National Pedagogical University named after Volodymyr Hnatiuk. Series : pedagogy. 2011. No. 1. P. 141–148. **10. Zagorka O. M.,** Mosov S. P., Sbitnev A. I., Stuzhuk P. I. Element of the doslidzhennya folding systems viyskovogo designation: navch. posib. / Kiev. NAOU, 2005. 124 p. **11. Belyaev M. I.,** Grinshkun V. V., Krasnova G. A. Technology for creating electronic teaching aids. **12. Saati T.,** Kerns K. Analytical planning. Organization of systems: book. Per. from English - New York, 1991. 224 p. **13. Hohoniants S. Yu.,** Georgadze O. A., Rudenko E. G. Architecture and classification of expert training systems for the training of military specialists. Modern information technologies in the field of security and defense. 2020. №2. P.133-138. **14. Shevchuk O. B.** Pedagogical principle of design and development of expert systems of science. Scientific notes of the Ternopil National Pedagogical University named after Volodymyr Hnatiuk. Series: pedagogy. 2016. No. 1. P. 38–43. **15. Sirotenko A. M.** Theory and practice of distance learning in the Armed Forces of Ukraine. Part 1: Fundamentals of the use of distance learning technologies in the educational process of higher military educational institutions and military educational units of higher education institutions: teaching method. way. team of authors. / Kyiv. NUOU them. Ivan Chernyakhovsky, 2020. 220 p. **16. Salkutsan S. M.** Substantiation of recommendations for improving the system of distance learning of the Armed Forces of Ukraine. research work / team of authors. / Kyiv. NUOU them. Ivan Chernyakhovsky, 2019. 170 p

DOI:**10.33099/2311-7249/2021-41-2-41-46**

УДК: 355.23(477):378.5

Віталій Олександрович Кацалап *(**кандидат військових наук, доцент**)*
Роман Володимирович Гарматенко

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДИК ПСИХОЛОГІЧНОГО ВПЛИВУ НА ВІЙСЬКОВОСЛУЖБОВЦІВ ЗБРОЙНИХ СИЛ УКРАЇНИ В УМОВАХ ПРОВЕДЕННЯ ОПЕРАЦІЇ ОБ'ЄДНАНИХ СИЛ

У статті наведено порівняльний аналіз методик психологічного впливу, який здійснюється на військовослужбовців Збройних Сил України в умовах проведення операції об'єднаних сил з використанням інформаційної інфраструктури, як України, так і Російської Федерації. Інформаційний простір переповнений деструктивною інформацією, яка здебільшого носить прихований характер психологічного впливу та має на меті змінити моделі поведінки військовослужбовці Збройних Сил України у спосіб, що сприятиме досягненню військових та політичних цілей країни агресора.

Оцінювання прогнозованої ефективності від психологічного впливу в зазначених підходах має ряд припущень та обмежень пов'язаних з поділом населення країни між тими, хто отримав інформацію з певного об'єкта впливу та тими, хто знаходяться за межами інформаційного простору.

Методики психологічного впливу на цільові аудиторії мають певну послідовність, а саме: визначення переліку інформації, яка буде віднесена до інформації деструктивного характеру; уточнення подій, які підтверджують інформаційні процеси та негативні наслідки від їх реалізації; визначення категорій управляючих впливів (побудова гіпотези); порівняння отриманих результатів на основі апроксимаційного експерименту; проведення аналізу результатів, які можуть повністю підтвердити гіпотезу; перевірити відповідність результатів; визначення статистичних даних щодо прояву усіх деструктивних психологічних впливів.

Наведені результати дослідження підтверджують домінуючу роль та важливість оцінювання психологічного впливу на військовослужбовців Збройних Сил України в умовах проведення операції об'єднаних сил, що вимагає пріоритетного розвитку в Україні.

Ключові слова*: фейки, дезінформація, інформаційний вплив, психологічний вплив, категорії обміну інформацією, управляючі інформаційні впливи, апроксимаційний експеримент.*

Вступ

В умовах сьогодення військовослужбовці Збройних Сил України постійно перебувають під потужним психологічним впливом Російської Федерації, як в районах постійної дислокації, так і під час виконання завдань в операції об'єднаних сил. Інформаційний простір переповнений деструктивною інформацією, яка здебільшого носить прихований характер впливу та має на меті змінити моделі поведінки військовослужбовців Збройних Сил України у спосіб, що сприятиме досягненню військових та політичних цілей країни агресора.

Постановка проблеми. На даний час існують методичні підходи, які дозволяють провести моделювання деструктивної інформації та оцінити наслідки від її негативного інформаційного впливу. В основі цих моделей використовується поняття нечіткої множини та лінгвістичної зміни інформації про етнічні, політичні й релігійні вподобання суспільних груп. Оцінювання прогнозованої ефективності від психологічного впливу в зазначених підходах має ряд припущень та обмежень пов'язаних з поділом населення країни між тими, хто отримав інформацію з певного об'єкта впливу та тими, хто знаходяться за межами інформаційного простору [1].

Сукупність наведених обмежень не дозволяє якісно здійснити моделювання психологічного впливу за ступенем насичення деструктивною інформацією кожного із можливих суб'єктів впливу.

Аналіз останніх досліджень і публікацій. Аналіз джерел [2–4] показує, що деструктивна інформація в інформаційному просторі перетворилась в алгоритм дій. Оцінювання цього алгоритму залежить від інформаційних технологій, які використовуються для створення комунікації між суб'єктом та об'єктом психологічного впливу. За такої обставини важливою особливістю є врахування поведінки певної цільової аудиторії під час визначення умов надання нею переваг до конкретної інформації в певному сегменті інформаційного простору.

Виходячи із зазначеного, **метою статті** є опис порівняльного аналізу методик психологічного впливу на військовослужбовців Збройних Сил України в умовах операції об'єднаних сил.

Виклад основного матеріалу дослідження

Від початку збройної агресії Російської Федерації проти України та тимчасової окупації нею частини української території, як за час проведення антитерористичної операції, так і в ході ведення операції об'єднаних сил на тимчасово окупованій території Донецької та Луганської областей створились умови, коли держава-агресор цілеспрямовано застосовує не тільки збройні формування Російської Федерації, а ще й комплекс сучасних прихованих та невійськових методів протиборства, зокрема широкомасштабний деструктивний інформаційно-психологічний та агітаційно-пропагандистський вплив на населення України, як на Сході нашої держави, так і на решті її території.

Аналіз наведених подій дозволяє виділити три категорії обміну інформацією між суб'єктами впливу:

управляючі інформаційні впливи;

передавання інформації – опосередковані впливи;

повідомлення про події – суперечливі впливи.

Під обміном інформацією між суб'єктами впливу розуміємо двосторонню взаємодію, у якій сторони виконують функції ініціатора або відповідача для кожного одиничного акту обміну.

Ініціатор формує керуючу взаємодію, тобто видає запит на визначену функцію управління. Відповідач формує відповідь на керуючий запит.

Реакція на передану інформацію реалізовується у запитах на визначену інформацію, яка видається ініціатором, та у відповідях, що формуються відповідачем. Повідомлення про події формуються та надсилаються ініціатором. Якщо існує необхідність у підтвердженні про прийом такого повідомлення, то воно формується відповідачем у вигляді відповіді.

Доцільно виділити три рівні управляючих інформаційних впливів:

управління рівнем аналізу;

управління рівнем систематизації;

управління рівнем взаємодії.

Управління рівнем аналізу забезпечує механізми контролю керуючих впливів та координації усіх інформаційних ресурсів, які здійснюють управління повідомленнями від одного або декількох об'єктів психологічного впливу. Управління рівнем аналізу є єдиним засобом, який забезпечує управління сукупністю можливих чинників безпосереднього психологічного впливу на декілька цільових аудиторій.

Управління рівнем систематизації забезпечує механізми розподілу інформаційних ресурсів із N – категорій управляючих впливів. Кожна із N – категорій управляючих впливів може впливати на сукупність елементів між суб'єктами психологічного впливу коли не конкретизована цільова аудиторія .

Об'єкти N – категорій взаємодіють одним з одним і забезпечують керуючі інформаційні впливи на кожен із N – категорій управляючих впливів, що використовуються для передачі даних між відповідними ініціаторами та акторами. Для передачі даних з метою управління N – категоріями інформаційних впливів використовується деструктивна інформація повторного суперечливого сприйняття.

Управління рівнем взаємодії забезпечує сукупність засобів керуючих впливів та управління одним суб'єктом деструктивного психологічного впливу на визначену конкретну цільову аудиторію.

Для ефективної реалізації розглянутих категорії управляючих впливів необхідно визначити один з основних показників якості психологічного впливу, яким є інтенсивність інформаційних потоків.

Інтенсивність інформаційних потоків залежить від величини перепаду інтелектуальних потенціалів конкретної цільової аудиторії або конкретного соціуму. Інтенсивність інформаційних потоків також може залежати від внутрішніх та зовнішніх взаємозв'язків – ділового спілкування, інтелектуального обміну між людьми та групами, а також від можливостей мобілізувати інформаційні ресурси, концентрувати їх в потрібному напрямку.

Для підтримання управління психологічним впливом, як сукупності усіх можливих впливів на цільову аудиторію створюється ситуація коли буде недостатньо використання засобів управляючих впливів.

Якщо такої повноти немає – відсутня підтримка від передавання інформації (опосередкованого впливу) та повідомлення про події (суперечливі впливи) то функціональна повнота управління цільовими аудиторіями буде забезпечена відкритою поведінкою людей у соціуму в межах однієї цільової аудиторії.

У контексті розгляду активних інформаційних впливів актуальним є питання не тільки опису процесу психологічного впливу, а й інформаційної протидії. Це, у свою чергу, дозволить якісно вивчити характер процесів, які розглядаються, а також дає можливість ставити та вирішувати завдання щодо знаходження оптимальних способів їх організації.

У загальному вигляді зазначені процеси є нелінійними і тому допускають неочевидні шляхи їх розвитку. Разом з тим, навіть у найпростіших випадках аналіз математичних моделей та результатів розрахунків дають змогу визначати ключові характеристики, управління якими стимулюватиме напрямок розвитку ситуації у необхідному напрямку [4].

Інформаційний простір швидко еволюціонує, постійно навчається разом з людиною і вже може прогнозувати поведінку соціальних груп та краще розуміти людину та її інтереси. Соціальним мережам, відомо про людину та соціальні групи абсолютно все, це надпотужний інструмент для розповсюдження дезінформації, саме тому, що за їхньою допомогою можна швидше зрозуміти інтереси, страхи та мотивації у поведінці цільової аудиторії та надати об'єкту саме ту інформацію, що

здійснить безпосередній вплив на рішення будь-якого суб'єкту.

Тому для аналізу в загальному інформаційному процесі необхідно визначити перелік типових (окремих) інформаційних процесів (дій, фактів), що можуть спричинити деструктивні наслідки по відношенню до цільової аудиторії.

При цьому, слід зауважити, що коли за певний період часу прояв нової деструктивної інформації, якої візуально немає, то вона вноситься до переліку як нова, та визначається її вплив на поточні події і, за необхідністю, коригуються критерії, а також уточнюється реальний стан загального процесу.

З урахуванням цієї особливості, структурна блок-схема методики психологічного впливу на цільові аудиторії має вигляд, який наведений на рис. 1.

Рис. 1. Блок-схема методики психологічного впливу

Наведена методика має ряд недоліків пов'язаних із тим, що цільові аудиторії можуть вірити в дезінформацію і самі можуть її поширювати, не здогадуючись про це. В такому випадку цільова аудиторія буде одночасно знаходитись під деструктивним психологічним впливом та транслювати цей вплив на інші соціальні групи. У такому випадку зміст блок-схеми методики моделювання психологічного впливу необхідно деталізувати.

Блок 1.

1. Запитання повинно бути достатньо вузьким, щоб на нього можна було відповісти.

Занадто широке запитання. Що українські ЗМІ пишуть про США та НАТО?

Достатньо вузьке запитання. Чи є негативна інформація про США або НАТО у висвітленні українських ЗМІ про президентські вибори з початку року?

2. Запитання повинно бути про те, що можна вимірювати.

Не можна виміряти. Чи надасть НАТО Україні ПДЧ?

Можна вимірювати. Чи позитивно відреагували службовці НАТО та країн-членів Альянсу на зміну в Конституції України про рух у НАТО?

Блок 2.

Минулі події повинні бути обмежені часом.

Не обмежене часом. Що угорські службовці кажуть про Україну?

Обмежене часом. Що угорські службовці сказали про Україну 60 днів до і 60 днів після парламентських виборів в Україні?

Блок 3.

Гіпотеза – це припущення, здогад або запропоноване пояснення, яке зроблене на основі обмежених доказів і використовується для початку подальших досліджень. Іншими словами гіпотеза це первісна відповідь на ваше запитання для дослідження. Мета подальших досліджень та

експериментів це підтвердити гіпотезу.

Приклад. Чи є негативне висвітлення інформації про США або НАТО в українських ЗМІ про президентські вибори з початку року?

Гіпотеза. В українських ЗМІ пишуть про членство у НАТО в контексті президентських виборів.

Блок 4.

В порівняльному апроксимаційному експерименті використовуються 10 якостей суспільних та публічно доступних даних М. Сальганік (Університет Прінстон), а саме: "Великі"; завжди включені; не реагують на спостереження; неповні; іноді недоступні; не репрезентативні; дрейфуючі; алгоритмічно сплутані; "Брудні"; конфіденційні/делікатні.

Блок 5.

Для аналізу результатів, які можуть повністю підтвердити гіпотезу рівня інформаційного впливу необхідно мати певну сукупність показників, а для визначення його значимості, аж до критичного (допустимого) значення, – відповідні критерії.

У [4, 5] стверджується, що формалізація та оцінювання психологічного впливу за допомогою точних математичних моделей і методів суттєво обмежені через:

різнорідність, розподіленість, багатозв'язність і динамічність джерел і об'єктів інформаційних загроз, що його породжують;

надто велику кількість параметрів, що відображають суспільні інформаційні відносини і характеризують відповідні інформаційні загрози;

відсутність необхідних статистичних даних внаслідок неповноти, неоперативності і недостовірності практично доступної інформації.

Саме ця аргументація свідчить на користь застосування апроксимаційного експерименту.

Замість звичайного порівняння деструктивного психологічного впливу на цільові аудиторії можливо провести апроксимаційний експеримент. Прикладом апроксимаційного експерименту є порівняння двох схожих подій. Таке порівняння з'ясовує, які саме фактори впливають на поведінку цільових аудиторії рис.2.

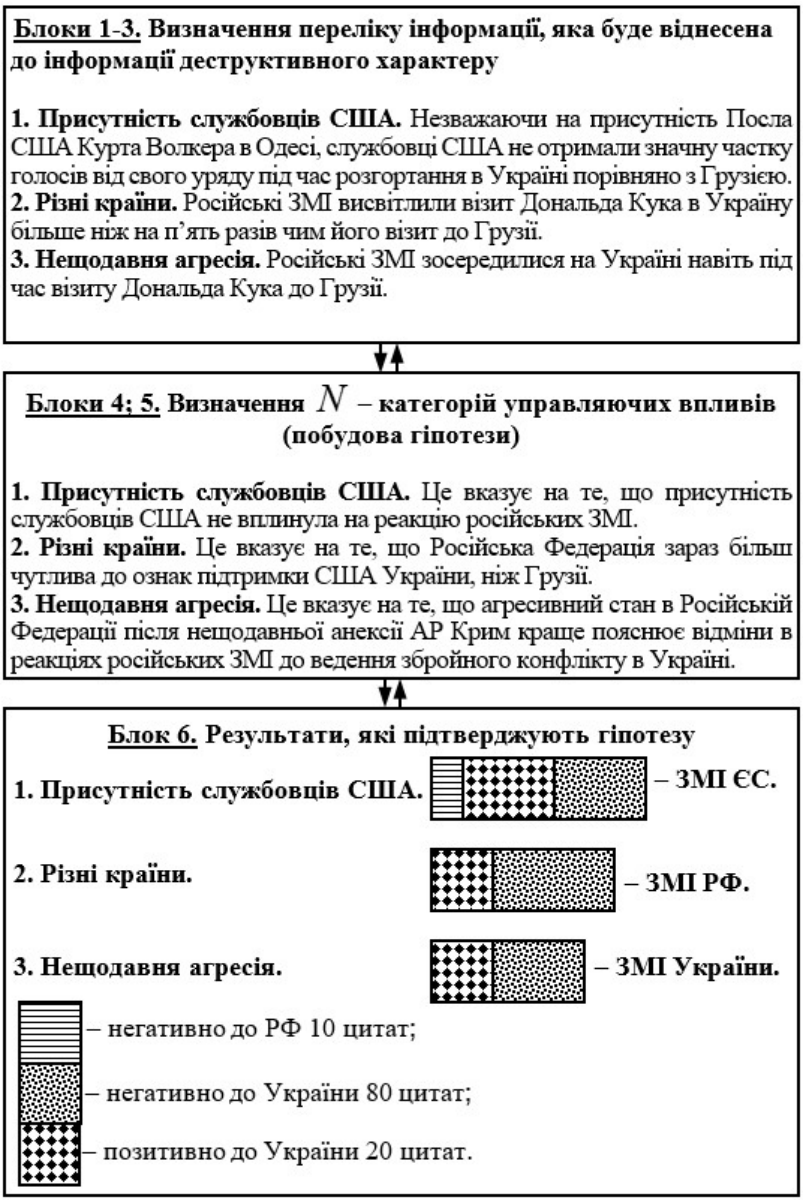

Рис. 2. Приклад порівняння, як апроксимаційного експерименту

Таким чином, наведений приклад порівняння, як апроксимаційного експерименту дозволяє оцінити та дослідити методики психологічного впливу на військовослужбовців Збройних Сил України в умовах проведення операції об'єднаних сил.

Висновки і перспективи подальших досліджень

Дослідження щодо психологічного впливу на цільову аудиторію ставлять нас перед фактом інформаційної загрози соціуму. Тому порівняльний аналіз методик психологічного впливу на військовослужбовців Збройних Сил України в умовах проведення операції об'єднаних сил є необхідним інструментом оцінювання інформаційного простору.

Наведений порівняльний аналіз методик психологічного впливу на військовослужбовців Збройних Сил України в умовах проведення операції об'єднаних сил дозволяє визначити окремі напрями інформаційної протидії. Це пояснюється цілим рядом причин.

По-перше, при виявлені дезінформації необхідно якнайшвидше довести відповідну інформацію до експертів, у той час як для виконання інших функцій робота в реальному масштабі часу, як правило, не обов'язкова.

По-друге, при різких змінах інформації зазначене дозволяє здійснювати аварійний нагляд за різноманітними системами, які збирають та обробляють інформацію від конкретних суб'єктів.

Наведені результати наукового дослідження підтверджують домінуючу роль та важливість оцінювання психологічного впливу на військовослужбовців Збройних Сил України в умовах проведення операції об'єднаних сил, що вимагає пріоритетного розвитку в Україні.

В подальших дослідженнях передбачається опис статистичних даних поведінки військовослужбовців Збройних Сил України в умовах прихованого психологічного впливу.

Література

1. Богданович В.Ю. Теоретичні основи забезпечення національної безпеки України в умовах позаблоковості: Монографія / В.Ю. Богданович, І.С. Романченко, І.Ю. Свида. – Львів: АСВ, 2011. – 414 с. **2.** *Frank, Robert H.* The Frame of Reference as a Public Good // The Economic Journal. – 1997. – Vol. 107 (November). – P. 1832–1847. **3.** *Easterlin, Richard A.* Does Economic Growth Improve the Human Lot? // Nations and Households in Economic Growth : Essays in Honor of Moses Abramovitz : / Paul A. David and Melvin W. Reder, eds. – New York : Academic Press, Inc., 1974. – 411 p. **4.** Кацалап В.О. Методика оцінки загроз інформаційній безпеці України у воєнній сфері / В.О. Кацалап // Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони" К.: НУОУ. – 2018. – №1(31). – С. 149-154. **5.** Захаров, А. В. Теория игр в общественных науках : учебник для вузов / А. В. Захаров ; Нац. исслед. ун-т "Высшая школа экономики". – М. : Изд. дом Высшей школы экономики, 2015. – (Учебники Высшей школы экономики). – 304 с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДИК ПСИХОЛОГИЧЕСКОГО ВЛИЯНИЯ НА ВОЕННОСЛУЖАЩИХ ВООРУЖЕННЫХ СИЛ УКРАИНЫ В УСЛОВИЯХ ПРОВЕДЕНИЯ ОПЕРАЦИИ ОБЪЕДИНЕННЫХ СИЛ

Виталий Александрович Кацалап *(кандидат военных наук, доцент)*
Роман Владимирович Гарматенко

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье приведен сравнительный анализ методик психологического воздействия, которое осуществляется на военнослужащих Вооруженных Сил Украины в условиях проведения операции объединенных сил с использованием информационной инфраструктуры, как Украины, так и Российской Федерации.

Информационное пространство переполнено деструктивной информации, которая обычно носит скрытый характер психологического воздействия, его цель изменить модели поведения военнослужащих Вооруженных Сил Украины за счет достижения военных и политических целей страны агрессора.

Оценка прогнозируемой эффективности от психологического воздействия в указанных подходах имеет ряд предположений и ограничений связанных с разделением населения страны между теми, кто получил информацию от определенного объекта воздействия и теми, кто находятся за пределами информационного пространства.

Методика психологического воздействия на целевые аудитории имеет определенную последовательность, а именно: определение перечня информации, которая будет отнесена к информации деструктивного характера; уточнение событий, которые подтверждают информационные процессы и негативные последствия от их реализации; определение категорий управляющих воздействий (построение гипотезы) сравнение полученных результатов на основе апроксимационного эксперимента; проведение анализа результатов, которые могут полностью подтвердить гипотезу; проверить соответствие результатов; определения статистических данных относительно проявления всех деструктивных психологических воздействий.

Приведенные результаты исследования подтверждают доминирующую роль и важность оценки психологического воздействия на военнослужащих Вооруженных Сил Украины в условиях проведения операции объединенных сил что требует приоритетного развития в Украине.

Ключевые слова: *фейки, дезинформация, информационное воздействие, психологическое воздействие, категории обмена информацией, управляющие информационные воздействия, аппроксимационный эксперимент.*

COMPARATIVE ANALYSIS OF METHODS OF PSYCHOLOGICAL INFLUENCE ON THE MILITARY SERVANTS OF THE ARMED FORCES OF UKRAINE IN THE CONDITIONS OF THE LUNCH OPERATION

Vitaliy Katsalap *(Candidate of military sciences, Associate professor)*
Roman Garmatenko

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

The article presents a comparative analysis of methods of psychological influence on servicemen of the Armed Forces of Ukraine in the conditions of a joint operation using the information infrastructure of both Ukraine and the Russian Federation. The information space is full of destructive information, which is mostly hidden in psychological nature and aims to change the behavior of servicemen of the Armed Forces of Ukraine in a way that will contribute to the military and political goals of the aggressor country.

Assessing the predicted effectiveness of psychological influences in these approaches has a number of assumptions and limitations related to the division of the population between those who received space.

Methods of psychological influence on target audiences have a certain sequence, namel: determining the list of information that will be classified as destructive information; clarification of events that confirm the information processes and the negative consequences of their implementation; determination of categories of control influences (hypothesis construction); comparison of the obtained results on the basis of the approximation experiment; analysis of results that can fully confirm the hypothesis; check the compliance of the results; determination of statistical data on the manifestation of all destructive psychological influences.

The results of the study confirm the dominant role and importance of monitoring the situation in ensuring the state's defense capabilities and its military security, which requires priority development in Ukraine.

Keywords: *fakes, misinformation, informational influence, psychological influence, categories of information exchange, control informational influences, approximation experiment.*

References

1. V. Bogdanovich Ukraine's Military Security: Research Methodology and Ways of Supply. - K .: Circulation, 2003. - 323 p. **2.** Frank, Robert H. The Frame of Reference as a Public Good // The Economic Journal. – 1997. – Vol. 107 (November). – P. 1832–1847. **3.** Easterlin, Richard A. Does Economic Growth Improve the Human Lot? // Nations and Households in Economic Growth : Essays in Honor of Moses Abramovitz : / Paul A. David and Melvin W. Reder, eds. – New York : Academic Press, Inc., 1974. – 411 p. **4.** V. Katsalap. Methods for assessing threats to information security of Ukraine in the military sphere / V. Katsalap // Scientific journal "Modern information technologies in the field of security and defense" K .: NUOU. - 2018. - №1 (31). - P. 149-154.

5. A. Zakharov. Theory of games in social sciences: a textbook for universities / A. Zakharov; Nat. research. University "Higher School of Economics". - M .: Изд. House of the Higher School of Economics, 2015. - (Textbooks of the Higher School of Economics). - 304 p.

DOI:**10.33099/2311-7249/2021-41-2-47-52**

УДК: 355.40:159.162

Олександр Володимирович Войтко *(кандидат військових наук)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

МОДЕЛЬ РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ ПРИ РЕАЛІЗАЦІЇ СТРАТЕГІЧНОГО НАРАТИВУ ДЕРЖАВИ

Вивчення та проведення досліджень щодо процесів розповсюдження та отримання інформації з засобів масової інформації та інформації, що циркулює в соціальних мережах залишається перспективним науковим напрямком, як для аналітиків, маркетологів так і для проведення спеціальних інформаційних та психологічних дій в інтересах застосування військ (сил).

Аналіз соціальної мережі або декількох мереж дозволяє скласти соціальний зв'язок між користувачами і контентом соціальної мережі та визначити перспективні напрямки задоволення їхніх інтересів до інформації, що безпосередньо буде використовуватись для визначення цільових аудиторій. Це безпосередньо пов'язано з розвитком технологічного процесу та процесу удосконалення засобів комунікації між людьми, які на теперішній час охоплюють майже кожний куток земної кулі, особливо важливо стало розуміти процеси щодо розповсюдження інформації.

В статті автором проаналізовано модель розповсюдження епідемії SIR, яка була використана для опису розповсюдження чуток від одного користувача до іншого, та її модифікації. За результатами аналізу запропоновано та описано модель розповсюдження інформації серед цільових аудиторій при реалізації стратегічного наративу держави. Логіка функціонування моделі базується на поданні цільової аудиторії інформаційного каналу як суми трьох груп людей, а саме: підписників, активних та неактивних фоловерів. Також модель враховує інтенсивність підписування на новинного агента, відписування від нього та прочитування новин, що дозволяє розрахувати ймовірність прочитування новини.

За допомогою сервісу програмного забезпечення Melting Asphalt автором візуалізовано процес розповсюдження інформації у відповідності до запропонованої моделі.

Ключові слова*:модель розповсюдження інформації, цільова аудиторія, наратив, підписники, фоловери.*

Вступ

Російська Федерація залишається воєнним противником України, який здійснює збройну агресію проти України, тимчасово окупував територію Автономної Республіки Крим та місто Севастополь, території у Донецькій та Луганській областях, системно застосовує воєнні, політичні, економічні, інформаційно-психологічні, космічні, кібер- та інші засоби, що загрожують незалежності, державному суверенітету і територіальній цілісності України [1].

Набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору є пріоритетним напрямком при реалізації національних інтересів держави. Для організації виконання такого завдання необхідно мати ефективну та дієву систему стратегічних комунікацій держави, яка використовує єдиний інформаційний простір, має надійні канали комунікації з населенням та відповідну розгалужену інформаційну інфраструктуру.

Постановка проблеми. Російські та проросійські засоби масової інформації продовжують поширювати інформаційні матеріали, спрямовані на дискредитацію воєнно-політичного керівництва нашої держави та дестабілізацію суспільно-політичної обстановки. Одним із найважливіших завдань агресора є відмова України від вступу до НАТО.

У попередніх публікаціях автором вирішувалося завдання щодо наукового обґрунтування вступу до ЄС, НАТО на підставі аналізу статистичних даних громадської думки та прогнозування сценаріїв її розвитку [2,3].

Отримані прогнозні дані дозволили визначити особливості впровадження стратегічного наративу держави системою стратегічних комунікацій та реалізувати інтереси держави у вигляді підтримки населенням її стратегічного курсу на набуття повноправного членства України в ЄС та НАТО.

Аналіз останніх досліджень і публікацій. Збройна агресія Російської Федерації проти України здійснюється за різними напрямами "гібридної війни". Агресивні впливи проводяться як одночасно, так і послідовно, фактично на всі сфери життєдіяльності нашої держави, при цьому отримані результати в одній сфері відразу використовуються для посилення впливу в інших сферах. Дослідженнями "гібридних дій" на сьогоднішній день займається велика низка вітчизняних та закордонних вчених. В роботах Ланде Д.В., Даника Ю.Г., Сальнікової О.Ф., Сніцаренка П.М. та багато інших, висвітлено матеріали щодо форм і способів, які використовує агресор для досягнення своїх імперських цілей, та містять ряд теоретичних положень, рекомендацій щодо можливих шляхів протидії. Надзвичайно важливим завданням буде дослідження процесів, які характеризують розповсюдження матеріалів

інформаційних впливів, а також аналіз якісних характеристик інформації для оцінювання потенційного охоплення цільових аудиторій і ступеню сприйняття даної інформації відповідною аудиторією.

В мережі Internet доступна низка програмних сервісів, з використанням яких можливо змоделювати процес розповсюдження інформації. Автором за допомогою одного із таких сервісів (Melting Asphalt) запропоновано варіант візуалізації моделі розповсюдження інформації серед цільової аудиторії. Запропоновані показники, які впливають на розповсюдження інформації серед цільових аудиторій [4].

Метою статті є розроблення та опис моделі розповсюдження інформації серед цільової аудиторі при реалізації стратегічного наративу держави, а також візуалізація цього процесу з використанням сучасних програмних сервісів.

Виклад основного матеріалу дослідження

Російська Федерація постійно веде інформаційно-психологічні операції спрямовані на відповідні цільові аудиторії, воєнно-політичне керівництво та населення України з метою зміни їх поведінки. Для того, щоб ефективно протистояти таким впливам необхідно дізнатись як розповсюджується інформація серед цільової аудиторії тобто відтворити процес інформаційно-психологічного впливу - розробити модель розповсюдження інформаційного матеріалу серед цільової аудиторії. Проблема визначення цільових аудиторій широкого формату набула в дослідження маркетологів та підприємців, які розробляли оцінку споживача, щоб точніше втілити потреби покупця та розробити окремі пропозиції для кожного.

Під час дослідження з моделювання розповсюдження інформації в соціальній мережі, було обрано модель розповсюдження епідемії. Модель епідемії W. O. Kermack була використана для опису розповсюдження чуток [5]. Дана модель досі використовується під час моделювання процесів розповсюдження інформації. В даному випадку, процес розповсюдження інформації безпосередньо можна порівняти з процесами розповсюдження вірусної інфекції. Розповсюдження починається з конкретної персони та продовжується в невеликих групах, поки не осягне всю цільову аудиторію, досягне свого max та піде на спад. Враховуючи зазначене, найпростіша модель розповсюдження інформації в мережі показує, що для визначення поширення, потрібно визначити певні комунікаційні вузли та активних фоловерів (рис.1).

Фоловери це, користувачі соцмережі, що слідкують за оновленнями статусу чи новинною стрічкою новинного агента та розповсюджують її (репостять). Під репостом розуміємо використання чужого тексту в себе у блозі чи в соціальній мережі, з посиланням на автора або першоджерело.

Отже, споживання інформації буде здійснюватися в мережі від вузла до вузла з певними обмеженнями. Сучасні соціальні мережі мають більш складний набір комунікаційних вузлів та більш хаотичні [6].

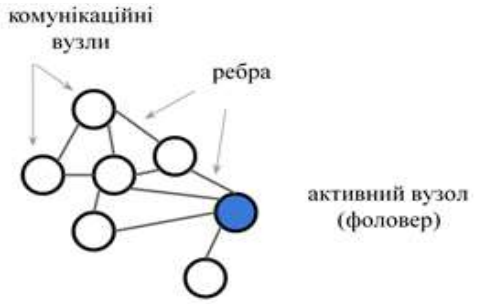

Рис.1 Проста модель розповсюдження інформації

Але головним об'єктом моделі є саме людина, на яку здійснюється інформаційно-психологічний вплив та її місце знаходження (локація). Кожна людина щоденно, відповідно до власного розкладу подій, витрачає певний час в різних локаціях. Наприклад, цільова аудиторія віком від 18 до 21 року можуть відвідувати локації такі як дім, навчальний заклад, робота, транспорт та інші можливі локації. Кількість різних місць перебування кожного типу в моделі визначається на основі загальної кількості людей в моделі та середній чисельності цільових аудиторій, які зазвичай відвідують дану локацію. Отже, всі можливі локації будуть створювати структуру оточуючого середовища для цільової аудиторії (рис.2).

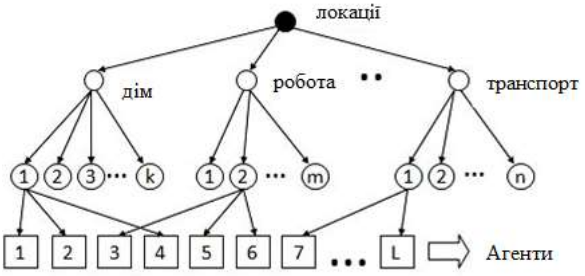

Рис.2 Структура оточуючого середовища моделі

Таким чином, перейдемо до розгляду детермінованої моделі епідемії SIR (susceptible – infected – removed), яка описує розповсюдження інформації від одного користувача до іншого, яку можна відобразити наступною схемою (рис. 3).

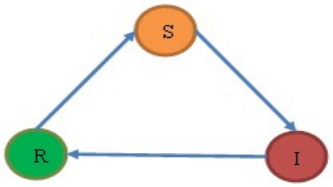

Рис.3 Схема роботи SIR-моделі

В основі моделі взяті три основні групи людей на, які розбивається загальна кількість людей в мережі. Наприклад, кількість користувачів в певній соціальній мережі можна визначити як:

$$N(t) = S(t) + I(t) + R(t), \quad (1)$$

де: $N(t)$ – загальна кількість людей (не змінна);

$S(t)$ – кількість користувачів, які сприятливі до інформації;

$I(t)$ – кількість користувачів, які отримали інформацію, і її розповсюджують;

$R(t)$ – кількість користувачів, які несприятливі до інформації.

Несприятливість до інформації можливо

визначати, як втрату цікавості до певної інформації та небажання розповсюджувати її серед інших агентів мережі, що може призвести до знищення матеріалів або втрату фоловера та його перехід до іншої цільової аудиторії.

Вихідну модель розповсюдження інформації можна сформулювати системою диференційних рівнянь [7]:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta\frac{S(t)I(t))}{N}; \\ \frac{dI(t)}{dt} = \beta\frac{S(t)I(t))}{N} - \gamma \mathrm{I(t)}; \\ \frac{dR(t)}{dt} = \gamma I(t). \end{cases} \quad (2)$$

де: β – параметр, який відображає швидкість передачі інформації новим агентам, або ймовірність передачі інформації при комунікації між агентами серед цільової аудиторії;

γ – параметр, який відображає швидкість втрати цікавості до інформації за час розповсюдження інформації , тобто інформація стає не цікавою для цільової аудиторії так як втратила свою цінність та актуальність.

Рівняння (2) можна описати наступними кроками:

Вузли в соціальній мережі представлені, як вузли, що схильні до отримання інформації за виключенням вузла або вузлів, які отримали інформацію та починають її розповсюдження;

На кожному часовому кроці вузли, які розповсюджують інформацію отримують можливість передати інформацію кожному з вузлів, що сприятливі до інформації з ймовірністю, яка дорівнює швидкості розповсюдження;

Вузли, які розповсюджують інформацію переходять в стан несприятливості та втрачають інтерес.

Отже, початковими умовами в момент часу $t = 0$ будуть:

$$\mathrm{S}(0) \geq 0, \mathrm{I}(0) \geq 0, \mathrm{R}(0) \geq 0$$

Враховуючи дані умови розглянемо кожне з рівнянь даної системи.

Перше рівняння описує зміну кількості людей, які не мають своєї думки та піддаються інформаційно-психологічному впливу.

Друге рівняння описує одночасне збільшення кількості зацікавлених осіб за рахунок тих, хто мав нейтралітет(тобто не визначився із вподобаннями).

Трете описує процес отримання інформації та набуття статусу активного учасника [8-9].

Таким чином, SIR-модель являє собою базовою та доцільно розглянути її розширену (модифіковану) модель.

Розширена SIR-модель, враховує зміну моделі у часі, а саме те, що кількість людей $\mathrm{N(t)}$ буде постійною, постійно змінюватись. В свою чергу, в розрізі процесів розповсюдження інформації може бути важливим, особливо при адаптації даної моделі для розповсюдження довгострокових періодів, під час яких відбувається збільшення в кількості користувачів соціальної мережі або навпаки.

Для даного типу моделі врахуємо два нових параметри:

λ – параметр, який відображає середню частоту приєднання до мережі;

μ – параметр, який відображає середню частоту покидання мережі.

В свою чергу, дана модель також буде описуватись системою диференційованих рівнянь, які будуть мати наступний вигляд:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta\frac{S(t)I(t))}{N} + \lambda(\mathrm{N(t)} - \mathrm{S(t)}); \\ \frac{dI(t)}{dt} = \beta\frac{S(t)I(t))}{N} - \gamma \mathrm{I(t)} - \mu \mathrm{I(t)}; \\ \frac{dR(t)}{dt} = \gamma I(t) - \mu R(t). \end{cases} \quad (3)$$

Дана модель враховує початкові умови, що і попередня модель та може бути представлена у вигляді наступної схеми (рис. 4).

Рис.4 Схема роботи розширеної SIR-моделі

Водночас, існує достатня кількість модифікованих моделей, які побудовані на основі SIR-моделі, наприклад, такі як SIS, яка припускає повторне зараження тих, хто одужав (втрата цікавості до інформації), або SIRS, яка враховує втрату імунітету з часом та інші SEIR, SEIS. В кожній моделі враховується специфічні фактори, які необхідні для повноцінного опису процесів епідемії, тому більш детальний опис інших моделей враховувати не будемо спираючись на меншу ступінь релевантності по відношенню до процесів розповсюдження інформації.

Перейдемо до безпосереднього розгляду запропонованої моделі розповсюдження інформації. Дана модель може бути подана у вигляді наступної системи диференціальних рівнянь [10 - 12]:

$$\begin{cases} dA/_{dt} = -A(t)\mu + B(t)\xi + C(t)\xi\lambda; \\ dB/_{dt} = -B(t)\mu - B(t)\xi + C(t)\lambda(1-\xi); \\ dC/_{dt} = \big(A(t) + B(t)\big)\mu - C(t)\lambda. \end{cases}$$

З початковими умовами в момент часу $t = 0$:

$$A(0) = A_0, B(0) = B_0, C(0) = C_0.$$
$$A_0 > 0, B_0 > 0, C_0 > 0.$$

Рішення цієї системи рівнянь може бути подано у наступному вигляді:

$$A(t) = C_1\mathrm{g} + C_2\,\nu e^{t(-\mu-\lambda)} - C_3\,e^{t(-\mu-\xi)};$$
$$B(t) = -C_1 r - C_2\,u e^{t(-\mu-\lambda)} + C_3\,e^{t(-\mu-\xi)};$$
$$C(t) = C_1 + C_2 e^{t(-\mu-\lambda)}.$$

де: $C_1 = \frac{A\_0 + B_0 + C_0\,u - C_0\,\nu}{\mathrm{g} - r + u - \nu}$,

$C_2 = \frac{-A_0 - B_0 + C_0\mathrm{g} - C_0\,r}{\mathrm{g} - r + u - \nu}$,

$C_3 = \frac{A_0 r - A_0 u + B_0\mathrm{g} - B_0\nu + C_0 g u - C_0\,ru}{\mathrm{g} - r + u - \nu}$;

$\mathrm{g} = \left[\frac{\lambda\xi}{\mu} - \frac{\xi(-\lambda\xi+\lambda)}{\mu(-\mu-\xi)}\right]$,

$\nu = \left[-\xi + \frac{\xi(-\lambda\xi\ \ \lambda)}{\lambda(\lambda-\xi)}\right]$,

$r = \frac{(-\lambda\xi+\lambda)}{-\mu-\xi}$,

$u = \frac{(-\lambda\xi\ \ \lambda)}{\lambda-\xi}$.

Логіка функціонування моделі, що розглядається, базується на поданні цільової аудиторії інформаційного каналу як суми трьох груп людей:

A – кількість активних фоловерів новинного каналу, тобто тих, хто прочитав інформаційну новину;

B – кількість неактивних фоловерів каналу, тобто тих, хто не прочитав новину, але є фоловером;

C – кількість непідписників, які відповідно і не читали новину.

Крім того до моделі входять наступні параметри:

λ – інтенсивність підписування на новинного агента;

μ – інтенсивність відписування від новинного агента;

ξ – інтенсивність прочитування новини.

Дані щодо кількісних значень перших двох параметрів можна отримати за допомогою моніторингу за новинним агентом та кількістю його фоловерів. Параметр ξ враховує такі властивості новини як актуальність і час опублікування, а також активність взаємодії фоловерів у внутрішніх мережах новинного агенту.

Актуальність новини будемо трактувати як імовірність зустрічі вибраної новини в усіх джерелах, що розглядаються. Тобто

$$\varphi = \frac{m}{M}$$

де m– кількість новинних джерел, які описують вибрану новину;

M– загальна кількість джерел.

Параметр, який характеризує час опублікування новини, визначається наступним чином:

$$\delta = \frac{e}{E}$$

де: e – кількість новин за визначеною тематикою, до якої відноситься контрольована новина, що розташовані в новинній стрічці користувача вище контрольної новини;

E – загальна кількість новин за визначеною тематикою у новинній стрічці користувача.

Наступний параметр ω – характеризує імовірність користувачів впливати на процес зростання прочитуваності новини. Будемо вважати, що

$$\omega = \frac{s}{(A_0 + B_0)}$$

де: s – кількість користувачів, що здійснили одну з дій: лайк або репост;

$(A_0 + B_0)$– кількість фоловерів новинного агента.

Таким чином імовірність прочитування новини можна подати наступним виразом:

$$\xi = \varphi\delta\omega$$

На основі викладеного можна зробити висновок, що якщо відомі всі розглянуті параметри моделі, то можуть бути розраховані значення функції A(t) в потрібний момент часу.

З метою візуалізації моделі розповсюдження інформації використаємо сервіс програмного забезпечення Melting Asphalt який заснований в 2012 році Kevin Simler для проведення досліджень. Саме цей сервіс має написану в програмному коді потрібну нам систему рівнянь. Використовуючи базову систему рівнянь моделі розповсюдження інформації та змінивши її параметри у відповідності до рівнянь 4, 5 отримано програмний продукт моделювання розповсюдження інформації серед цільової аудиторії та візуалізацію цього процесу [13]. Зазначений сервіс надає можливість візуалізувати процес розповсюдження інформації серед цільових аудиторій рис. 5.

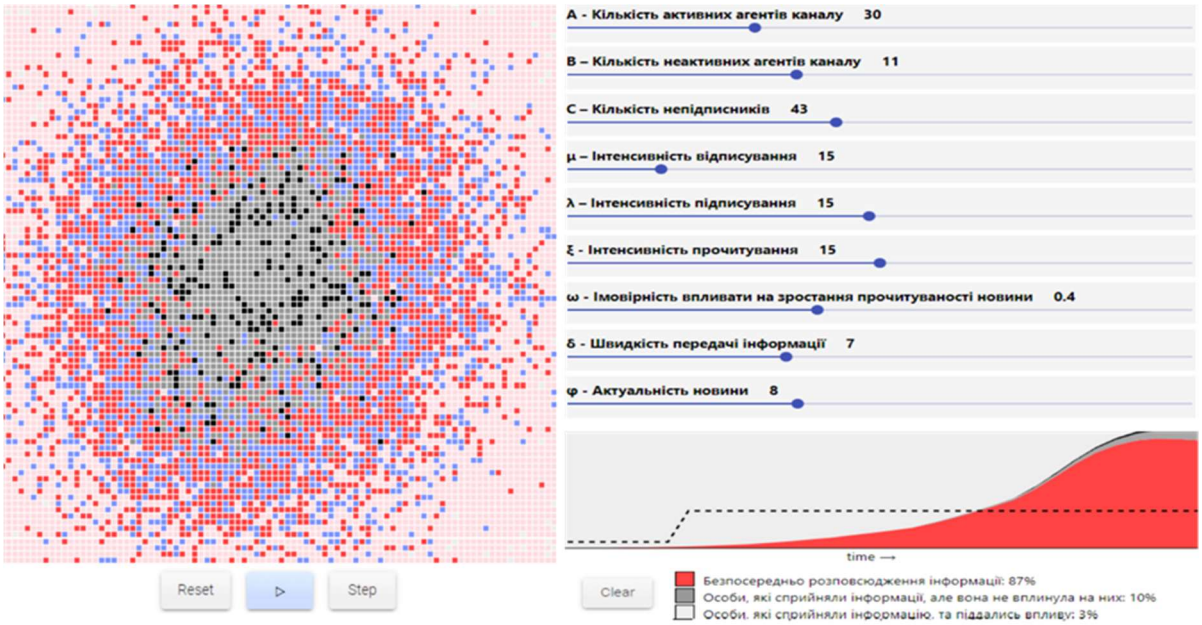

Рис. 5. Візуалізація моделі розповсюдження інформації

Використовуючи запропонований математичний інструментарій та враховуючи зазначені показники моделі розповсюдження інформації серед цільової аудиторії ми зможемо змоделювати процес розповсюдження інформації та прогнозувати варіанти побудови сил і засобів в системі стратегічних комунікацій при реалізації стратегічного наративу держави, для їх ефективного використання.

Висновки і перспективи подальших досліджень

Основною ціллю для системи стратегічних

комунікацій Міністерства оборони та Збройних Сил України є досягнення стратегічного наративу. Досягнення такої мети можливе тільки за умови системної роботи всіх складових системи стратегічних комунікацій держави. В умовах конфлікту з Російською Федерацією збільшення витрат на розширення структурних елементів системи стратегічних комунікацій є недопустимим, тому постає завдання щодо розподілення існуючих ресурсів сил та засобів системи стратегічних комунікацій і їх ефективного використання.

Застосування запропонованого математичного інструментарію дозволить розрахувати необхідну кількості засобів (інформаційних каналів) в інтересах реалізації стратегічного наративу держави наддасть можливість обґрунтовано сформувати потребу та обсяги матеріалів інформаційно-психологічного впливу на цільові аудиторії (населення різних регіонів країни) з визначенням як кількісного, так і якісного складу новинних каналів. В свою чергу це дозволить визначити основні завдання для системи стратегічних комунікацій та реалізувати інтереси держави у вигляді підтримки населенням стратегічного курсу держави на набуття повноправного членства України в ЄС.

Подальший розвиток цього дослідження необхідно проводити на основі сучасних наукових методів теорії соціальних досліджень та теорії інформаційних операцій з метою виявлення часових показників, які характеризують етапи планування та виконання завдань силами і засобами стратегічних комунікацій.

Для забезпечення оптимального сумарного інформаційного впливу доцільно здійснювати науково-обґрунтований розподіл прогнозованого загального об'єму завдань між різними структурними підрозділами системи стратегічних комунікацій з обов'язковим врахуванням особливостей різних цільових аудиторій. Це наддасть можливість не тільки конкретизувати цілі і завдання для кожного структурного підрозділу системи стратегічних комунікацій, але й дозволить розробити дієві та ефективні матеріали інформаційно-психологічного впливу для досягнення результатів.

Література

1. Указ Президента України №121/2021 від 25 березня 2021 року Про рішення Ради національної безпеки і оборони України "Про Стратегію воєнної безпеки України" **2. Солонніков В.Г., Войтко О.В., Пащенко Т.П.** Обґрунтування реалізації стратегічного наративу держави. Сучасні інформаційні технології у сфері безпеки та оборони. 2020. №1 (37). С. 203-212. **3. Войтко О.В., Солонніков В.Г., Полякова О.В.** Особливості застосування методу фрактального аналізу сталості процесу розвитку громадської думки при реалізації стратегічного наративу держави. Сучасні інформаційні технології у сфері безпеки та оборони. 2020. №2(38). С. 145-150. **4. Войтко О.В., Микусь С.А**. Показники розповсюдження інформації серед цільової аудиторії. Proceedings of the 8-th International Scientific and Practical Conference «Challenges in Science of Nowadays» (April 4-5, 2021). Washington, USA: EnDeavours Publisher, 2021. pp.1053-1057.

5. Kermack, W. O.; McKendrick, A. G. (1927). "A Contribution to the Mathematical Theory of Epidemics". Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences. **6. K.Molodetska, V.Solonnikov, O.Voitko, I.Humeniuk, O.Matsko, O.Samchyshyn** Counteraction to information influence in social networking services by means of fuzzy logic system. International Journal of Electrical and Computer Engineering. Vol. 11. № 3 – 2021. – P.2490-2499. **7 Gubanov DA** Review of online reputation / trust systems. Internet conference on governance issues. Moscow: IPP RAS, 2009. 25p**. 8. Gubanov DA, Novikov DA, Chkhartishvili AG** "Social networks: models of information influence, management and confrontation", 2010 - 228 pages. **9. Roberts F.S.** Discrete mathematical models with applications to social, biological and ecological problems. - Moscow: Science, 1986. **10. Михайлов А.П., Петров А.П., Маревцева Н.А., Третьякова И.В.** Разработка модели распространения информации в обществе, 2014, Журнал "Математическое моделирование", с.74. **11. D.V. Lande, V.A. Dodonov,** Fractal Properties of Multiagent News Diffusion Model, 2016, 10p. **12. Болотин А.В.** Разработка модели распространения новостей в социальных сетях на основе SIR – модели эпидемии. М.: Московский институт электроники и математики , 2018. **13.** Візуалізація моделі розповсюдження інформації.

МОДЕЛЬ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ ПРИ РЕАЛИЗАЦИИ СТРАТЕГИЧЕСКОГО НАРРАТИВА ГОСУДАРСТВА

***Александр Владимирович Войтко** (кандидат военных наук)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Изучения и проведения исследований относительно процессов распространения и получения информации из средств массовой информации и информации, циркулирующей в соцсетях остается перспективным научным направлением, как для аналитиков, маркетологов так и для проведения специальных информационных и психологических действий в интересах применения войск (сил).

Анализ социальной сети или нескольких сетей позволяет составить социальный связь между пользователями и контентом социальной сети и определить перспективные направления удовлетворения их интересов к информации, непосредственно используемого для определения целевых аудиторий. Это непосредственно связано с развитием технологического процесса и процесса совершенствования способов коммуникации между людьми, которые в настоящее время охватывают почти каждый угол земного шара, особенно важно стало понимать процессы по распространению информации.

В статье автором проанализированы модель распространения эпидемии SIR, которая была использована для описания распространения слухов от одного пользователя к другому, и ее модификации. По результатам анализа предложено и описано модель распространения информации среди целевых аудиторий при реализации стратегического нарратива государства. Логика функционирования модели базируется на представлении целевой аудитории информационного канала как суммы трех групп людей,

а именно: подписчиков, активных и неактивных фолловеров. Также модель учитывает интенсивность подписки на новостного агента, отписки от него, позволяет рассчитать вероятность прочитывания новости.

С помощью сервиса программного обеспечения Melting Asphalt автором визуализированы процесс распространения информации в соответствии с предложенной моделью.

***Ключевые слова**: модель распространения информации, целевая аудитория, нарратив, подписчики, фолловеры.*

MODEL OF DISSEMINATION OF INFORMATION IN THE IMPLEMENTATION OF THE STRATEGIC NARRATIVE OF THE STATE

***Oleksandr Voitko** (Candidate of Military Sciences)*

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

Studying and conducting research on the processes of disseminating and receiving information from the media and information circulating in social networks remains a promising scientific area, both for analysts, marketers and for conducting special information and psychological actions in the interests of using troops (forces).

The analysis of a social network or several networks makes it possible to compose a social connection between users and the content of a social network and to determine promising directions for meeting their interests in information, which is directly used to determine target audiences. This is directly related to the development of the technological process and the process of improving the methods of communication between people, which now cover almost every corner of the globe, it has become especially important to understand the processes of information dissemination.

In the article, the author analyzed the SIR epidemic spread model, which was used to describe the spread of rumors from one user to another, and its modification. Based on the results of the analysis, a model for disseminating information among target audiences was proposed and described in the implementation of the strategic narrative of the state. The logic of the model's functioning is based on the presentation of the target audience of the information channel as the sum of three groups of people, namely: subscribers, active and inactive followers. The model also takes into account the intensity of subscription to a news agent, unsubscribing from him, and allows calculating the probability of reading the news.

With the help of the Melting Asphalt software service, the author visualized the process of information dissemination in accordance with the proposed model.

***Key words:** information dissemination model, target audience, narrative, subscribers, followers.*

References

1. Ukaz Prezydenta Ukrainy №121/2021 vid 25 bereznia 2021 roku Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy “Pro Stratehiiu voiennoi bezpeky Ukrainy” **2. Solonnikov V.H.,** Voitko O.V., Pashchenko T.P. Obgruntuvannia realizatsii stratehichnoho naratyvu derzhavy. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. 2020. #1 (37). S. 203-212. **3. Voitko O.V.,** Solonnikov V.H., Poliakova O.V. Osoblyvosti zastosuvannia metodu fraktalnoho analizu stalosti protsesu rozvytku hromadskoi dumky pry realizatsii stratehichnoho naratyvu derzhavy. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. 2020. №2(38). S. 145-150. **4. Voitko O.V.,** Mykus S.A. Pokaznyky rozpovsiudzhennia informatsii sered tsilovoi audytorii. Proceedings of the 8-th International Scientific and Practical Conference «Challenges in Science of Nowadays» (April 4-5, 2021). Washington, USA: EnDeavours Publisher, 2021. pp.1053-1057. **5. Kermack, W. O.**; McKendrick, A. G. (1927). "A Contribution to the Mathematical Theory of Epidemics". Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences. **6. K.Molodetska,** V.Solonnikov, O.Voitko, I.Humeniuk, O.Matsko, O.Samchyshyn Counteraction to information influence in social networking services by means of fuzzy logic system. International Journal of Electrical and Computer Engineering. Vol. 11. №3 – 2021. – R.2490-2499. **7 Gubanov DA** Review of online reputation / trust systems. Internet conference on governance issues. Moscow: IPP RAS, 2009. 25p. **8. Gubanov DA,** Novikov DA, Chkhartishvili AG "Social networks: models of information influence, management and confrontation", 2010 - 228 pages. **9. Roberts F.S.** Discrete mathematical models with applications to social, biological and ecological problems. - Moscow: Science, 1986. **10. Mykhailov A.P**., Petrov A.P., Marevtseva N.A., Tretiakova Y.V. Razrabotka modely rasprostranenyia ynformatsyy v obshchestve, 2014, Zhurnal “Matematycheskoe modelyrovanye”, s.74. **11. D.V. Lande**, V.A. Dodonov, Fractal Properties of Multiagent News Diffusion Model, 2016, 10p. **12. Bolotyn A.V.** Razrabotka modely rasprostranenyia novostei v sotsyalnыkh setiakh na osnove SIR – modely эpydemyy. M.: Moskovskyi ynstytut эlektronyky y matematyky , 2018. 13. Vizualizatsiia modeli rozpovsiudzhennia informatsii.

DOI:**10.33099/2311-7249/2021-41-2-53-58**

УДК: 355.23(477):378.5

Олександр Віталійович Левченко (*доктор військових наук, професор****)***
Дмитро Леонідович Федорчук (*кандидат технічних наук****)***
Юрій Іванович Міхєєв (*кандидат технічних наук****)***

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

АНАЛІЗ ОСНОВНИХ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ДЕРЖАВ-СУСІДІВ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ АГРЕСІЇ РОСІЇ

У статті розглянуто поняття та сутність загроз національній безпеці держав-сусідів України, спричинених гібридною агресією Російської Федерації. Проаналізовано нормативно-правові акти, які визначають можливі інформаційні загрози для України та держави-сусідів: Польщі, Словаччини, Румунії, Молдови, Угорщини, Білорусі. Основну увагу приділено реальним та потенційним загрозам національній безпеці держави в інформаційній сфері, а саме намаганню маніпулювати суспільною свідомістю, зокрема шляхом поширення пропагандистських повідомлень, недостовірної, неповної або упередженої інформації. Розглянуто Стратегію національної безпеки Російської Федерації, яка визначає причини виникнення загроз національній безпеці держави.

На основі аналізу результатів моніторингу інформаційного простору визначено основну цільову аудиторію, обрану спецслужбами Російської Федерації для поширення пропагандистських повідомлень. При цьому враховано основні цілі пропаганди, яка поширювалася спецслужбами Російської Федерації під час проведення антитерористичної операції та поширюється в умовах проведення операції Об'єднаних сил з метою досягнення стратегічних цілей держави-агресора, а саме: дискредитації держави на міжнародній арені, підриву довіри до неї як до надійного економічного та політичного партнера; дискредитації військово-політичного керівництва держави, керівників органів державної влади усіх рівнів серед українського суспільства; дестабілізації внутрішньополітичної обстановки в державі; зниження морально-психологічного стану особового складу Збройних Сил України; інформаційної підтримки керівництва тимчасово окупованих територій, ватажків незаконно створених збройних формувань, терористичних організацій так званих "ДНР" та "ЛНР"; демонстрації військової могутності Російської Федерації.

За результатами проведеного аналізу задекларованих національних інтересів та загроз національній безпеці держав-сусідів України з'ясовано особливості конфронтації національних інтересів нашої держави: етнічне розмаїття суспільства, ескалація напруженості в зоні територіальних інтересів, агресія Російської Федерації.

Ключові слова*: гібридна агресія, національні інтереси, національна безпека держави, пропаганда, Російська Федерація, держави-сусіди, моніторинг інформаційного простору.*

Вступ

У сучасній геополітиці під національними інтересами (НІ) розуміють стратегічно важливі цілі, які ставить перед собою кожна держава, і засоби, за допомогою яких вона їх досягає [1]. Однією з пріоритетних серед таких цілей є забезпечення інформаційної та кібернетичної безпеки держави як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних та інформаційних заходів [2]. Особливо питання забезпечення інформаційної та кібернетичної безпеки держави зростає, коли проявляються елементи гібридизації – не нові за сутністю але унікальні за узгодженістю цілей, динамічністю їх досягнення, зростанням ролі інформаційної та кібернетичної складової на усіх рівнях [3].

Постановка проблеми. Відповідно до Стратегії воєнної безпеки України [4] визначено, що агресивна зовнішня і воєнна політика Російської Федерації (РФ) загрожує національній безпеці України та інших держав Балтійського і Чорноморського регіонів, може призвести до подальшої ескалації збройної агресії проти України та спровокувати міжнародний збройний конфлікт у Європі. На національному рівні РФ залишається воєнним противником України, який здійснює збройну агресію проти України, тимчасово окупував територію Автономної Республіки Крим та міста Севастополь, території у Донецькій та Луганській областях, системно застосовує воєнні, політичні, економічні, інформаційно-психологічні, космічні, кібер- та інші засоби, що загрожують незалежності, державному суверенітету і територіальній цілісності України. Для реалізації державної політики у воєнній сфері передбачається створення системи комплексного стратегічного аналізу воєнних загроз національній безпеці України.

Географічно Україна межує по суходолу із сімома державами, які, виходячи з їх задекларованих законодавчо НІ, можна умовно поділити на дві групи: держави проєвропейського спрямування та держави проросійського спрямування. До першої групи відносимо Польщу, Словаччину, Румунію, Молдову, Угорщину; до другої – Білорусь і, власне, Росію. Для розуміння точок розходження інтересів України, а, отже, і потенційних цілей пропаганди проти нашої держави, з інтересами держав-сусідів необхідно проаналізувати послідовно їх НІ, геостратегічні цілі та основні загрози НБ.

Аналіз останніх досліджень і публікацій. Аналіз наукових досліджень за тематикою свідчить про те, що у своїх публікаціях автори розглядають тільки деякі сфери забезпечення національної безпеки окремої держави, які спричинені різними факторами (загрозами), у тому числі, й гібридною агресією Росії проти України [5–8]. Так, у [5] на основі аналізу перебігу процесів анексії РФ Автономної Республіки Крим та сучасних збройних конфліктів авторами визначено особливості прояву інформаційних загроз та їх розвиток у воєнній сфері.

У [6] автором розглянуто передумови та причини розроблення керівництвом Республіки Польща нової редакції Стратегії національно безпеки. Особливу увагу приділено оцінці безпекового середовища Республіки Польща, загроз і викликів, що стоять перед країною та Європейським регіоном.

У [7] автор розглядає вплив російської агресії проти України на зовнішню політику і національну безпеку Румунії. Визначені основні загрози й ризики, а також ключові напрями політики Бухареста за для їх мінімізації і посилення своєї ролі на східному фланзі НАТО та ЄС і в ареалі регіону Чорного моря. Ключовими загрозами визначаються загроза енергетичній сфері та кібербезпеці.

У [8] визначено засади та здійснено поелементний аналіз національної безпеки Республіки Білорусь. Аналізуються фактори, що справляють як безпосередній, так і опосередкований вплив на національну безпеку країни. Акцентується увага на появі нових загроз у інформаційній сфері.

З огляду на це, виникає необхідність у визначенні основних загроз національній безпеці України з боку держав-сусідів. Тому обраний напрям досліджень є актуальним.

Метою статті є дослідження умов появи основних загроз національній безпеці держав-сусідів України, що спричинені гібридною агресією Росії проти України.

Виклад основного матеріалу дослідження

Проєвропейська спрямованість напрямів розвитку першої групи держав визначена у відповідних нормативно-правових та стратегічних документах у сфері національної безпеки (НБ) та оборони, що в загальному аргументується форматом їх участі в міжнародних системах колективної безпеки, інтеграційних процесах, пов'язаних з вступом до Європейського союзу, прагнення до енергетичної незалежності від Росії як найбільшого виробника та постачальника енергоносіїв у регіоні тощо.

Окрему увагу слід приділити деяким специфічним моментам, притаманним НІ держав, що розглядаються. Так, Словаччина та Угорщина наголошують на всебічній підтримці своїх етнічних меншин на територіях інших держав, проводячи послідовну, а подекуди й наполегливу (Угорщина) зовнішню політику, яка на сьогоднішній день уже призводить до певних непорозумінь, напруженостей як в України, так і в її відносинах із зазначеними державами. Яскравим прикладом пропагандистської інформаційної кампанії, основаної на реалізації НІ Угорщини, стала нещодавня критика щодо внесення змін до законодавства України про освіту [9].

Агресивні дії збоку РФ у 2014 році щодо України змусили проєвропейських сусідів переглянути власні переліки загроз НБ та оборони. Результатом стало внесення змін у існуючі нормативно-правові та стратегічні документи у сфері НБ. Усі вони мають декілька схожих положень. Отже, серед загроз НБ Польщі, Угорщини, Румунії, Словаччини та Молдови основними визначені такі:

експансія РФ поблизу кордонів;

конфлікти (зокрема, призупинені) у Чорноморському регіоні;

залежність енергетичної безпеки від РФ.

Причому, якщо Словаччина дипломатично формулює мілітарні дії РФ як "…головний виклик безпеці євроатлантичного простору" [10], то Польща відверто фіксує "…дії РФ щодо відновлення позицій наддержави за рахунок сусідів" [11].

Примітним є визначення країнами Вишеградської четвірки (Польща, Словаччина, Угорщина, Чехія) серед основних завдань з забезпечення НБ: виявлення та моніторинг фактичних або потенційних викликів, ризиків та загроз у кіберпросторі; посилення захисту державних інформаційно-комунікаційних систем, національної критичної інформаційної інфраструктури, секретної інформації та національних інформаційних активів, а також посилення міжнародного співробітництва з кібербезпеки [12]. Причому на думку Угорського керівництва слід активно розвивати наступальні можливості відповідних підрозділів для кібернетичних операцій. Також наголошується на призупиненні військової співпраці з Росією. Але разом з тим, Угорщина прагне зниження ризиків, викликаних напруженістю між НАТО та РФ та зацікавлена у прагматичному розвитку угорсько-російських відносин. Подібні побоювання опосередковано у свої Стратегіях і Доктринах висловлюють й інші проєвропейські держави [13–14], що, у свою чергу, сприяє проведенню

Україною послідовної антиросійської інформаційної політики.

Якщо проєвропейські держави-сусіди України єдині у своєму тлумаченні дій РФ щодо України, що підкріплено відповідним супроводом в інформаційному полі, то проросійська Білорусь подекуди утримується від різких заяв та на офіційному рівні не визнає цієї агресії. Керівництво Республіки у своїй Концепції національної безпеки, яка не зазнала змін з 2010 року, серед основних НІ держави в воєнній сфері визначає "послідовний розвиток та зміцнення воєнного та воєнно-технічного співробітництва з РФ" [15]. Білорусь позиціонує себе на міжнародній арені незалежною державою, яка тримає нейтралітет на тлі конфлікту Україна – РФ, виступаючи в деякому сенсі дипломатичним представником між конфліктуючими державами, надаючи майданчик для переговорів у форматі Нормандської четвірки. Такі дії Білорусі не суперечать її НІ та всебічно підтримуються інформаційними кампаніями, де гарантом достовірності заявлених напрямів співпраці виступає глава держави [16]. Проте, як показує аналіз новинних повідомлень у засобах масової інформації, у таких заявах мають місце певні маніпулювання фактами, де миролюбні заяви "дружньої" сусідньої держави вступають у протиріччя з діями щодо надання можливостей РФ з нарощування воєнної присутності на своїй території поблизу кордонів нашої держави [17]. Зважаючи на поступове та неухильне слідування заявленим НІ Республіки Білорусь, ця держава є потенційним противником України в інформаційному просторі як ретранслятор наративів Росії. Зважаючи на таке, ймовірними цілями пропаганди з боку цієї держави можуть бути:

підтримка російської інформаційної політики;

приховування воєнної активності збройних сил (ЗС) РФ на своїй території поблизу кордонів з Україною;

створення враження нейтральної позиції щодо конфлікту РФ – Україна, РФ – НАТО.

Останнє потребує особливої уваги з боку України в розрізі завдань із забезпечення заявлених НІ та стратегічних національних пріоритетів РФ, серед яких зазначено [18, 19]:

розвиток інформаційних, комунікативних та когнітивних технологій;

застосування інформаційних технологій в інтересах збереження культурних, історичних та духовно-моральних цінностей багатонаціонального народу РФ;

удосконалення форм і способів застосування ЗС РФ з врахуванням тенденцій змін характеру сучасних війн і збройних конфліктів;

розвиток інтеграційних процесів на пострадянському просторі та засобів задоволення мовних та культурних потреб співвітчизників за кордоном шляхом реалізації програм підтримки вивчення російської мови та культури в Співдружності Незалежних Держав.

У той же час, серед загроз НБ Росії визначено:

поширена практика повалення легітимних політичних режимів, провокування внутрішньодержавних нестабільності і конфліктів, особливо поблизу кордонів РФ;

прагнення деяких держав використовувати інформаційні та комунікаційні технології для досягнення своїх геополітичних цілей, зокрема шляхом маніпулювання суспільною свідомістю і фальсифікацією історії;

спроби інших держав щодо протидії Росії як центру впливу в світі, та послаблення її позицій;

розвиток озброєнь у сусідніх державах.

Ці пункти, зафіксовані на рівні законодавства, стали основою для провадження агресивної інформаційної політики РФ на міжнародному рівні та щодо України.

Крім того, РФ визначає як негативний вплив на реалізацію НІ "…позицію Заходу, спрямовану на протидію інтеграційним процесам і створення вогнищ напруженості в Євразійському регіоні..." [19]. Загрозою НБ – "підтримка США і Європейським союзом антиконституційного державного перевороту в Україні". Факторами виникнення нестабільності в Україні визначені "зміцнення ультраправої націоналістичної ідеології, цілеспрямоване формування в українського населення образу ворога в особі Росії, неприкрита ставка на силове вирішення внутрішньодержавних протиріч, глибока соціально-економічна криза".

Україна визначена як "…довгострокове вогнище нестабільності в Європі і безпосередньо біля кордонів Росії...", а Росія при цьому "…зберігає прихильність використанню, насамперед, політичних і правових інструментів, механізмів дипломатії і миротворчості. Застосування військової сили для захисту НІ можливо тільки в тому разі, якщо всі вжиті заходи ненасильницького характеру виявилися неефективними…" [19].

Аналіз загроз інформаційній безпеці табл.1 свідчить про наявність у кожному джерелі воєнної складової, яка формує джерело загрози інформаційній безпеці у воєнній сфері.

Таблиця 1

Загрози інформаційній безпеці

Зовнішні джерела загроз інформаційної безпеки
Вплив технічних засобів іноземної розвідки на політичні, економічні, військові структури
Концепції окремих держав щодо інформаційної та психологічної війни
Міжнародні терористичні організації та комп'ютерна злочинність
Міжнародна конкуренція за володіння інформаційними ресурсами й технологіями
Ініціювання порушення інформаційної сфери на території противника

Порівнюючи воєнну та інформаційну сферу можна окреслити варіанти джерел загроз інформаційній безпеці у воєнній сфері: дискредитація органів управління; провокування

сутичок між органами управління воєнної організації держави; утруднення прийняття органами управління воєнної організації держави важливих рішень; підрив авторитету воєнної організації держави; нанесення втрат життєво важливим інтересам держави в оборонній сфері.

Для запобігання таких загроз та досягнення стратегічних цілей керівництво РФ використовує відповідні спецслужби, які поширюють пропагандистські повідомлення в інформаційному просторі. Аналіз результатів моніторингу інформаційного простору свідчить про те, що основною цільовою аудиторією для пропагандистських повідомлень РФ проти України виступають:

політичне керівництво та населення України на підконтрольних територіях;

керівництво та особовий склад ЗС України;

населення та військові формування на окупованих територіях;

населення РФ;

міжнародна спільнота.

Як засіб маніпуляції суспільною свідомістю РФ використовує різні технології пропаганди, основними цілями якої є:

дискредитація держави на міжнародній арені, підрив довіри до неї як до надійного економічного та політичного партнера;

дискредитація політичного керівництва держави, керівників органів державної влади державного та регіонального рівнів серед українського суспільства;

дестабілізація внутрішньополітичної обстановки в Україні;

дискредитація та зниження довіри до військового керівництва серед особового складу ЗС України та населення прилеглих до лінії розмежування територій та всередині держави, створення негативного образу українського воїна;

зниження морально-психологічного стану особового складу ЗС України;

зниження боєздатності частин і підрозділів через підбурювання до внутрішніх конфліктів та розколу військових колективів за політичними, релігійними, етнічними, службовими та іншими мотивами;

формування спотвореного сприйняття військовослужбовцями ЗС України наявних загроз НБ, справжніх планів і намірів противника.

інформаційна підтримка окупаційної влади на території анексованої АР Крим, керівників терористичних організацій "ДНР" та "ЛНР", ватажків незаконних збройних формувань, героїзація терористів та окупаційних військ на непідконтрольних Україні територіях та серед населення РФ;

спотворене подання ситуації в Україні серед населення РФ задля утвердження думки щодо правильності дій воєнно-політичного керівництва Росії;

демонстрація військової могутності ЗС РФ.

Висновки і перспективи подальших досліджень

Отже, проведений аналіз задекларованих державами-сусідами України НІ та загроз НБ показав, що конфронтація нашої держави можлива за такими напрямами:

етнічне розмаїття суспільства (національні меншини через пропаганду в електронних засобах масової інформації та соціальних мережах можуть підбурюватися до порушення територіальної цілісності держави);

нестабільність у Чорноморському регіоні (деякі держави можуть використовувати маніпулятивні впливи задля ескалації напруженості в цій зоні з метою задоволення власних економічних і територіальних інтересів);

енергетична залежність (ціллю пропаганди може бути дискредитація України як надійного транзитера енергоносіїв);

неспроможність держави протистояти збройній агресії РФ (залучення військових, політичних експертів для висвітлення невтішних прогнозів стосовно України).

Загрози в інформаційній сфері та кібернетичному просторі визначаються як найбільш небезпечніші для будь-якої з держав в умовах гібридної агресії Росії проти України.

В найближчій перспективі серед загроз основними визначені такі, що пов'язані із зовнішньою політикою РФ:

експансія РФ поблизу кордонів;

конфлікти (зокрема, призупинені) у Чорноморському регіоні;

залежність енергетичної безпеки від РФ.

Перспективним напрямом подальших наукових досліджень може бути завдання з удосконалення заходів протидії зовнішнім інформаційним загрозам України з огляду на концепції забезпечення НБ провідних держав світу.

Література

1. Горбулін В. П. Пріоритетність національних інтересів у світлі національної безпеки України / Горбулін В. П., Качинський А. В. // Стратегічна панорама. – 2005. – № 3. – С. 11–18. **2.** Закон України **"**Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. **3. Грищук Р. В.** Інформаційна та кібернетична безпека: роль та місце в умовах гібридної війни / Р.В. Грищук // Кібербезпека в Україні: правові та організаційні питання. URL:http://oduvs.edu.ua/wp-content/uploads/2017/01/Hryshchuk_R.V._Informatsiyna_ta_kibernetichna_bezpeka_rol-_ta_mistse_v_uslovyyakh_hibridnoyi_Viyny.pdf. **4.** Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України": Указ Президента України від 25 березня 2021 року № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#n8. **5. Левченко О. В.** Інформаційні загрози як різновид воєнних загроз державі / О. В. Левченко, Ю. І. Міхєєв // Наука і техніка Повітряних Сил Збройних Сил України. – 2018. – № 3(32). – С. 14–19. **6. Александров О. С.** Нова

стратегія національної безпеки Польщі – відповідь на європейські виклики та загрози сьогодення / О. С. Александров // Стратегічні пріоритети. – 2015. – № 1 (34). – С. 131–138. **7. Златін О.** Зовнішня політика й національна безпека Румунії у контексті агресії Росії проти України / О. Златін // Міжнародні зв'язки України: наукові пошуки і знахідки. – 2016. – Вип. 25. – С. 324–334. **8. Курас А. І.** Національна безпека Білорусі: військово-політичні парадигми / А. І. Курас // наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. – 2015. – Вип. 2. – С. 184–196. **9.** Новий український Закон про освіту: чому законотворчий процес має значення. Юридична газета online. URL: https://yur-gazeta.com/golovna/noviy-ukrayinskiy-zakon-pro-osvitu-chomu-zakonotvorchiy-proces-mae-znachennya.html. **10**. Bezpečnostná stratégia Slovenskej Republiky 202. URL: https://www.vlada.gov.sk/data/files/8048_bezpecnostna-strategia-sr-2021.pdf. **11.** Новая Стратегия национальной безопасности Польши четко определяет угрозы. URL: https://www.polskieradio.pl/397/7839/Artykul/2515179/. **12. Котух Є. В.** Основні підходи до забезпечення кібербезпеки: досвід країн вишеградської четвірки. **13.** Проект Концепции национальной безопасности Республики Молдова. URL: http://iep.md/analytic/0362-Proekt-Koncepcii-nacionalnoj-bez.phtml. **14.** Strategia naţională de apărare a ţării din 30 iunie 2020. **15.** Указ Президента Республики Беларусь от 9.11.2010 № 575 "Об утверждении Концепции национальной безопасности Республики Беларусь". URL: https://pravo.by/document/?guid=2012&oldDoc=2010-276/2010-276(005-026).pdf&oldDocPage=1. **16.** Батька всіх врятує. План Лукашенка для Донбасу. URL: https://ua.korrespondent.net/ukraine/4028177-batka-vsikh-vriatuie-plan-lukashenka-dlia-donbasu/. **17.** Військові маневри "Захід-2017": у НАТО дорікнули Росії та Білорусі за ухилення від прозорості. URL: https://www.unian.ua/world/2095069-viyskovi-manevri-zahid-2017-u-nato-doriknuli-rosiji-ta-bilorusi-za-uhilennya-vid-prozorosti.html. **18.** Доктрина информационной безопасности Российской Федерации. URL: http://kremlin.ru/acts/bank/41460/page/1. **19.** Указ Президента Российской Федерации от 31 декабря 2015 года № 683 "О Стратегии национальной безопасности Российской Федерации" URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=0&nd=102385609&firstDoc=1.

АНАЛИЗ ОСНОВНЫХ УГРОЗ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ-СОСЕДЕЙ УКРАИНЫ В УСЛОВИЯХ ГИБРИДНОЙ АГРЕССИИ РОССИИ

Александр Витальевич Левченко (доктор военных наук, профессор)
Дмитрий Леонидович Федорчук (кандидат технических наук)
Юрий Иванович Михеев (кандидат технических наук)

Житомирський военный институт имени С.П. Корольова, Житомир, Украина

В статье рассматривается концепция и суть угроз национальной безопасности стран, которые граничат с Украиной, вызванных гибридной агрессией России. Анализируются нормативные правовые акты, определяющие возможные информационные угрозы Украине и странам-соседям: Польше, Словакии, Румынии, Молдове, Венгрии, Беларуси. Основное внимание уделяется реальным и потенциальным угрозам национальной безопасности государства в информационной сфере, а именно попытке манипулирования общественным сознанием, в частности путем распространения пропагандистских сообщений, ложной, неполной или предвзятой информации. Рассматривается Стратегия национальной безопасности Российской Федерации, которая определяет причины угроз национальной безопасности государства.

На основе анализа результатов мониторинга информационного пространства определяется основная целевая аудитория, выбранная спецслужбами Российской Федерации для распространения пропагандистских сообщений. В то же время основные цели пропаганды, распространяемой спецслужбами Российской Федерации в ходе антитеррористической операции и распространяемой в условиях операции Объединенных сил в целях достижения стратегических целей страны-агрессора, а именно: дискредитация государства на международной арене, подрыв доверия к нему как к надежному экономическому и политическому партнеру; дискредитация военно-политического руководства государства, глав органов государственной власти всех уровней украинского общества; дестабилизация внутриполитической ситуации в государстве; снижение морально-психологического состояния личного состава Вооруженных Сил Украины; информационная поддержка руководства временно оккупированных территорий, лидеров незаконно созданных вооруженных формирований, террористических организаций так называемых "ДНР" и "ЛНР"; демонстрация военной мощи Российской Федерации.

По результатам анализа заявленных национальных интересов и угроз национальной безопасности стран-соседей Украины выясняются особенности противостояния национальных интересов нашего государства: этническое разнообразие общества, эскалация напряженности в зоне территориальных интересов, агрессия Российской Федерации.

Ключевые слова: *гибридная агрессия, национальные интересы, национальная безопасность государства, пропаганда, Российская Федерация, страны-соседи, мониторинг информационного пространства.*

ANALYSIS OF THE MAIN THREATS TO THE NATIONAL SECURITY OF THE JUDICIAL COUNTRIES OF UKRAINE DURING HYBRID AGGRESSION IN RUSSIA

Oleksandr Levchenko (Doctor of military sciences, professor)
Dmytro Fedorchuk (Candidate of technical sciences)
Yurii Mikhieiev (Candidate of technical sciences)

Zhytomyr Military Institute named after S.P. Korolev, Zhytomyr, Ukraine

The article examines the concept and the essence of threats to the national security of Ukraine's neighboring countries caused by Russia's hybrid aggression. Also analyzes the normative legal acts that determine possible information threats to Ukraine and neighboring countries: Poland, Slovakia, Romania, Moldova, Hungary, Belarus. The main attention is paid to real and potential threats to the national security of the state in the information sphere, namely the attempt to manipulate the public consciousness, in particular by disseminating propaganda messages, false, incomplete or biased information. The article also revues the National Security Strategy of the Russian Federation, which determines the causes of threats to the national security of the state.

Based on the analysis of the results of monitoring of the information space, the main target audience is chosen by the special services of the Russian Federation for the dissemination of propaganda messages. At the same time, the main goals of propaganda, which were disseminated by the special services of the Russian Federation during the anti-terrorist operation. His is still distributed in the conditions of the Joint Forces operation in order to achieve the strategic goals of the aggressor country, namely: discrediting the state on the international stage, losing trust as to reliable economic and political partner; discrediting the military and political leadership of the state, heads of state authorities at all levels among Ukrainian society; destabilization of the internal political situation in the state; reducing the moral and psychological state of the personnel of the Armed Forces of Ukraine; information support of the leadership of the temporarily occupied territories, leaders of illegally created armed groups, terrorist organizations of the so-called "DNR" and "LNR"; demonstration of military power of the Russian Federation.

The peculiarities of confrontation of the national interests of our state are found out according to the results of the analysis of the declared national interests and threats to the national security of the neighboring countries of Ukraine. Among them: ethnic diversity of society, escalation of tension in the zone of territorial interests, aggression of the Russian Federation.

Key words: *hybrid aggression, national interests, national security of the state, propaganda, Russian Federation, neighboring countries, monitoring of information space.*

References

1. Ghorbulin V. P., Kachynsjkyj A. B. (2005), Priorytetnistj nacionaljnykh interesiv u svitli Strateghiji nacionaljnoji bezpeky Ukrajiny // Strateghichna panorama. Problemy nacionaljnoji ta strateghichnoji bezpeky, №3. **2.** Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" vid 05.10.2017 № 2163-VIII. **3. Ghryshhuk R. V.** Informacijna ta kibernetychna bezpeka. **4.** Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 25 bereznia 2021 roku "Pro Stratehiiu voiennoi bezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 25 bereznia 2021 roku № 121/2021. **5. Levchenko O. V.** (2018), Informatsiini zahrozy yak riznovyd voiennykh zahroz derzhavi / O. V. Levchenko, Yu. I. Mikhieiev // Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy. – 2018. – № 3(32). – S. 14–19. **6. Aleksandrov O. S.** (2015), Nova stratehiia natsionalnoi bezpeky Polshchi – vidpovid na yevropeiski vyklyky ta zahrozy sohodennia / O. S. Aleksandrov // Stratehichni priorytety. – 2015. – № 1 (34). – S. 131–138. **7. Zlatin O.** (2016), Zovnishnia polityka y natsionalna bezpeka Rumunii u konteksti ahresii Rosii proty Ukrainy / O. Zlatin // Mizhnarodni zviazky Ukrainy: naukovi poshuky i znakhidky. – 2016. – Vyp. 25. – S. 324–334. **8. Kuras A. I.** (2015), Natsionalna bezpeka Bilorusi: viiskovo-politychni paradyhmy / A. I. Kuras // naukovi zapysky Instytutu politychnykh i etnonatsionalnykh doslidzhen im. I. F. Kurasa NAN Ukrainy. – 2015. – Vyp. 2. – S. 184–196. **9.** Novyi ukrainskyi Zakon pro osvitu: chomu zakonotvorchyi protses maie znachennia. **10.** Security strategy of the Slovak Republic 2021. **11.** Novaya Strategiya nacional'noj bezopasnosti Pol'shi chetko opredelyaet ugrozy. **12. Kotukh Ye.** V. Osnovni pidkhody do zabezpechennia kiberbezpeky: dosvid krain vyshehradskoi chetvirky. **13.** Proekt Koncepcii nacional'noj bezopasnosti Respubliki Moldova. **14.** National heating strategy from June 30, 2020. **15.** Ukaz Prezidenta Respubliki Belarus' ot 9.11.2010 № 575 "Ob utverzhdenii Koncepcii nacional'noj bezopasnosti Respubliki Belarus". Nacional'nyj pravovoj Internet-portal Respubliki Belarus. **16.** Batka vsikh vriatuie. Plan Lukashenka dlia Donbasu. Portal "Korrespondent.net" / Polityka. **17.** Viiskovi manevry "Zakhid-2017": u NATO doriknuly Rosii ta Bilorusi za ukhylennia vid prozorosti. Informatsiine ahentstvo "UNIAN". **18.** Doktrina informacionnoj bezopasnosti Rossijskoj Federacii. **19.** Ukaz Prezidenta Rossijskoj Federacii ot 31 dekabrya 2015 goda № 683 "O Strategii nacional'noj bezopasnosti Rossijskoj Federacii".

Шановні колеги!

Запрошуємо до участі в науковому журналі
"Сучасні інформаційні технології у сфері безпеки та оборони",
Видавець: Національний університет оборони України імені Івана Черняховського
Наказом Міністерства освіти і науки України №409 від 17.03.2020 р. та №886 від 02.07.2020 р.
журнал включено до Переліку наукових фахових видань України категорії "Б" в галузях
"технічні науки" та "військові науки", спеціальності – 122, 124, 253, 254"
Наклад – 100 примірників, відкрите видання.

Основні тематичні напрями журналу:

1. Військова кібернетика та системний аналіз
2. Протиборство у кібернетичному просторі
3. Військово-космічні та геоінформаційні технології
4. Інтелектуальні інформаційні технології та робототехніка у сфері безпеки та оборони
5. Інформаційно-аналітична діяльність у сфері безпеки та оборони
6. Розвиток теорії та практики створення інформаційно-телекомунікаційних систем
7. Стратегічні комунікації та когнітивні системи спеціального призначення
8. Інтерактивні моделі розвитку науково-освітнього простору;
9. Високотехнологічні аспекти воєнного мистецтва
10. Історичний дискурс розвитку високих оборонних технологій

Схема оформлення статей

DOI (*Arial*, *кегль – **11** пт.*)

←— *1 пустий рядок – **6** пт.*

УДК (*Arial*, *кегль – **11** пт.*)

←— *1 пустий рядок – **10** пт.*

[1]Анатолій Анатолійович Іванов ***(д-р техн. наук, професор)***
[2]Іван Іванович Петров ***(канд. техн. наук, доцент, доцент кафедри)***

←— *(кегль – **11** та **8** пт.)*

←— *1 пустий рядок – **6** пт.*

[1]Університет…, Київ, Україна
[2]Інститут…, Київ, Україна ←— *(кегль – **11** пт.)*

←— *1 пустий рядок – **10** пт.*

НАЗВА СТАТТІ (*Arial, кегль – **14** пт.*; *накреслення – "напівжирне", по правому краю)*

←— *1 пустий рядок – **10** пт.*

Текст анотації мовою тексту статті (в даному випадку – українською). Зміст анотації має стисло і достатньо інформативно підсумовувати основні ідеї та отримані результати дослідження. Розмір анотації повинен становити не менше 250 слів. Зверніть увагу на те, що дані про авторів, назва, ключові слова та анотація будуть використані як метадані для опису Вашої статті, тому вони повинні максимально чітко описувати її зміст. Для більш якісного пошуку даного контенту в мережі, будь ласка, уникайте занадто узагальнених та складних формулювань, використовуйте тільки загальновідомі абревіатури. ***(Обсяг анотації – не менше 250 слів.)***

Ключові слова: *поняття1; поняття 2; поняття3.* (*кегль – **10** пт.*)

Вимоги до набору

Формат аркуша: А4 (21 × 29,7 см).

Параметри сторінки (відступи від краю): зліва – 3 см.; справа – 2 см.; зверху – 2 см.; знизу – 2 см.

Шрифт статті – *Times New Roman*; накреслення – пряме; кегль – 10 пт.; міжрядковий інтервал – одинарний.

Текст статті розташовується у два стовпчики однакової ширини – 7,75 см.; відстань між стовпчиками – 0,5 см.; відступ першого рядка абзацу – 0,5 см.; вирівнювання – за шириною.

Підзаголовок – кегль – 12 пт.; накреслення – напівжирне; відступів немає; вирівнювання – центроване.

Не використовуйте для форматування тексту пропуски, табуляцію тощо. Не встановлюйте ручне перенесення слів, не використовуйте колонтитули. Між значенням величини та одиницею її вимірювання ставте нерозривний пропуск (Ctrl + Shift + пропуск).

УВАГА! Остання сторінка статті заповнюється не менше 3/4, рекомендована парна кількість аркушів.
Кількість авторів – не більше трьох.

Набір формул: редактор формул *MS Equation*.

Забороняється використовувати для набору формул графічні об'єкти, кадри й таблиці.

В меню "*Размер* → *Определить*" ввести такі розміри:
Обычный – 10 пт.; Крупный индекс – 8 пт.;
Мелкий индекс – 7 пт.; Крупный символ – 15 пт.;
Мелкий символ – 9 пт.

Стиль формул – "прямий", тобто в меню "*Стиль* → *Определить"* поля "Формат символов" – пусті.

Табличний заголовок (10 пт.) – **обов'язковий**.

Рисунки **обов'язково** супроводжуються центрованими підрисунковими підписами (кегль – 10).

Не допускаються кольорові та фонові рисунки.

Допускається розташування великих рисунків, формул та таблиць в одну колонку (до 16 см.).

Список літератури виділяється підзаголовком "***Література***"та оформлюється згідно з міждержавним стандартом ДСТУ 8302:2015 "(кегль – 9 пт.).

Структура рукопису

Відповідно до постанови ВАК України від 15.01.2003 № 7-05/1 текст статті повинен мати таку структуру: ***постановка проблеми*** *у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями*; ***аналіз останніх досліджень і публікацій***, *на які спирається автор*; ***формулювання мети статті*** (*постановка завдання*); ***виклад основного матеріалу*** *дослідження з повним обґрунтуванням отриманих*

наукових результатів; ***висновки*** *з даного дослідження і перспективи подальших досліджень у даному напрямку.*

Текст статті розбивається на відповідні розділи з підзаголовками, які виділені напівжирним шрифтом.

Робочі мови – українська, російська, англійська.

На останньому аркуші статті після списку літератури наводяться: назва статті, прізвище, ім'я, по батькові, науковий ступінь та вчене звання автора (співавторів), назва організації, у якій працює автор (співавтори), анотація та ключові слова українською, російською та англійською мовами (крім основної мови статті) за нижченаведеним зразком (10 кегль (8 для наукового ступеня, звання, посади), міжрядковий інтервал – 1,0, вирівнювання – по центру). ***Обсяг анотації – не менше 250 слів.***

НАЗВАНИЕ СТАТЬИ

[1]***Анатолий Анатолиевич Иванов*** ***(д-р техн. наук, профессор)***
[2]***Иван Иванович Петров*** ***(канд. техн. наук, доцент, доцент кафедры)***

[1]***Университет…, Киев, Украина***
[2]***Институт…, Киев, Украина***

Перевод текста аннотации и ключевых слов

ARTICLE TITLE

[1]***Anatolii Ivanov*** ***(Doctor of technical sciences, professor)***
[2]***Ivan Petrov*** ***(Candidate of technical Sciences, associate professor)***

[1]***University…, Kyiv, Ukraine***
[2]***Institute…, Kyiv, Ukraine***

Translation of the abstract and keywords

англійською мовою за зразком (9 кегль):

Після цього наводиться список літератури

References

1. Koncepcija rozvytku telekomunikacij v Ukrajini, skhvalena Rozporjadzhennjam Kabinetu Ministriv Ukrajiny vid 7 chervnja 2006 r. № 316-r. **2. A.O. Moskalenko, Gh.V. Sokol.** Pereshkodostijkistj syghnaliv moduljaciji cyklichnym zsuvom kodu z adaptacijeju po shvydkosti peredachi informaciji. *Systemy upravlinnja, navighaciji ta zv'jazku.* Kyjiv. 2018. № 3(49). S. 175-180. **3. A.O. Moskalenko, S.V. Voloshko, I.I. Sljusarj** Pereshkodostijkistj syghnaliv udoskonalenoji moduljaciji cyklichnym zsuvom kodu z adaptacijeju po shvydkosti peredachi informaciji v umovakh baghatopromenevogho rozpovsjudzhennja radiokhvylj. *Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony*. Kyjiv. 2015. № 2 (23). S. 35–39. **4. A.A. Moskalenko, Gh.V. Sokol** Metod synteza syghnalov usovershenstvovannoj moduljacyy cyklycheskym sdvyghom koda s adaptacyej po skorosty peredachy ynformacyy. *Informacijno kerujuchi systemy na zaliznychnomu transporti.* Kharkiv. №3 (100).2013.S.71-75. **5. G.M. Dillard et all**., Cyclic Code Shift Keying: A Low Probability of Intercept Communication Technique // IEEE Trans. Aerosp. Electron. Systems., vol. AES-39, July 2003, pp. 786 -798.

Корисні посилання для здійснення транслітерації:

http://translit.kh.ua/?passport – автоматична транслітерація з української мови
http://translate.meta.ua/ua/translit/ – автоматична транслітерація з російської мови

На окремому аркуші наводяться відомості про авторів.

Автор*:* Прізвище, ім'я та по-батькові; посада; вчена ступінь та вчене звання; адреса електронної поштової скриньки; контактний телефон; ORCID ID в форматі: http://orcid.org/0000-0001-9037-787X

Подання матеріалів

Обсяг рукопису – від 4 до 20 аркушів українською або англійською мовами.

Для публікації необхідно надіслати статтю у електронній формі **doc**.

Подані матеріали автору не повертаються.

Матеріали просимо подавати через сайт журналу (sit.nuou.org.ua) або на e-mail: sitnuou@ukr.net.

З питань оплати звертатись до редакції (sitnuou@ukr.net).

Редколегія залишає за собою право відмови у публікації статей, що не відповідають проблематиці журналу, умовам оформлення матеріалів та за результатами незалежного рецензування.

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) 271-07-31.
Підписано до друку 28.09.2021. Формат 60×84 ⅛. Ум. друк. а. 7,5. Тираж 100 прим.
Надруковано у друкарні Національного університету оборони України імені Івана Черняховського.