ISSN 2524-0056(Print)
ISSN 2519-481X(Online)

**ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА**

ЗБІРНИК НАУКОВИХ ПРАЦЬ

ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Виходить 4 рази на рік

№ 67

КИЇВ – 2020

УДК621.43
ББК 32-26.8-68.49
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2020. № 67. 160 с.

Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень та побажань.

Зареєстровано Міністерством юстиції України, свідоцтво про державну реєстрацію друкованого засобу масової інформації - серія КВ № 11541 – 413Р від 21.07.2006 р.

Відповідно до Наказу МОН України від 16.05.2016 № 515 «Збірник наукових праць ВІКНУ імені Тараса Шевченка» внесено до переліку наукових фахових видань із технічних наук, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук.

Затверджено на засіданні вченої ради ВІКНУ від 23.01.2020р., протокол №. 7

Відповідальні за макет:
Ряба Л.О., Солодєєва Л.В.

Адреса редакції: 03189, м. Київ, вул. Ломоносова,81 тел./факс +38 (044) 521 – 33 – 82
Наклад 300 прим.
Ел.адреса редактора: lenkov_s@ukr.net
Офіційний сайт журналу: http://miljournals.knu.ua/

ЗМІСТ

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ЗАГАЛЬНІ ПИТАННЯ

CONTENTS

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

INFORMATION TECHNOLOGIES

GENERAL QUESTIONS

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕНН

УДК 004.05:004.657

к.т.н. **Гаценко С.С.** (НУОУ)
Писаренко Р.В. (ВІКНУ)
Лук'янчіков І.М. (НУОУ)
Ошкодер С.В. (НУОУ)
Ніколаєнко В.П. (НУОУ)
Приходько О.Г. (НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-01

ІНФОРМАЦІЙНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ РАДІОМОНІТОРИНГОМ

Збройна агресія Російської Федерації проти України, втрата важливих промислових потенціалів, як Державна акціонерна холдингова компанія «Топаз», яка спеціалізувалася на розробці і виробництві складних радіотехнічних систем і комплексів, в тому числі унікальних комплексів дальньої радіотехнічної розвідки та раннього попередження систем протиповітряної оборони, зокрема станції радіотехнічної розвідки «Кольчуга», дала значний поштовх для розвитку нових підходів до ведення радіомоніторингу обстановки, як одного з головних, а іноді єдиного способу добування інформації.

Такий складний вид технічної діяльності, як радіомоніторинг, потребує значних зусиль для його підтримки в готовності. Постійне забезпечення радіомоніторингу необхідною кількістю висококваліфікованих спеціалістів, що мають великий досвід визначення типу джерела радіовипромінювання, потребує значних зусиль для їх пошуку та навчання. Навчання фахівця цього класу займає не менше 1-1,5 років та значні фінансові витрати. Розв'язання наукового завдання автоматизації процесу виявлення та розпізнавання є одним із пріоритетних напрямків розвитку радіомоніторингу.

Сучасний радіомоніторинг характером функціонування поділяється на 2 групи:

активний, що дозволяє розпізнавати та виявляти непрацюючі джерела радіовипромінювання;

пасивні, що дозволяють ідентифікувати та розпізнавати функціонуючі джерела радіовипромінювання.

Основою функціонування пасивних засобів радіомоніторингу є виявлення сигналів, що передають повідомлення (наприклад сигнал управління повітряним рухом) і розпізнавання параметрів потужних сигналів бортових, корабельних та наземних радіолокаційних станцій. Інформативність сигналу джерела радіовипромінювань для засобів радіомоніторингу залежить від того, наскільки надійно цей сигнал виявляється і наскільки достовірно (точно) визначаються його параметри, що несуть корисні для розвідки повідомлення або значення. Оскільки спостереження сигналу завжди відбувається на фоні різного роду перешкод, факт виявлення сигналу, а також помилки вимірювання сигнальних параметрів і виділення повідомлень завжди виявляються випадковими.

У статті розглянуто актуальне наукове завдання автоматизації процесу виявлення та розпізнавання джерел радіовипромінювання, за рахунок розробки системи підтримки прийняття рішень щодо визначення типу джерел радіовипромінювання за параметрами його сигналу в інтересах системи радіомоніторингу держави, яка надає вказівки операторам РТР Кольчуга-КЕ (Кольчуга-М) щодо вибору найбільш ймовірного варіанту рішення, що знизить кваліфікаційні вимоги до операторів, що значно скоротить фінансові та часові витрати на їх підготовку.

Ключові слова: система радіомоніторингу, кризовий регіон, ефективність, ймовірність, об'єкти радіомоніторингу, джерела радіомоніторингу.

Вступ. Такий складний технічний вид діяльності, як радіомоніторинг, потребує значних зусиль по підтримці її у постійній готовності. Окрім забезпечення новітніми засобами та

комплексами важливою частиною є забезпечення висококваліфікованими спеціалістами, що мають великий досвід у визначенні типу ДРВ, що вимагає витрати значних зусиль на їх пошук і підготовку. Підготовка спеціаліста такого класу займає щонайменше 1-1,5 роки та значних фінансових затрат на підготовку [1, 2].

Вирішення наукового завдання автоматизації процесу виявлення та розпізнавання джерел радіовипромінювань є одним з пріоритетних напрямків розвитку радіомоніторингу.

Аналіз останніх досліджень та публікацій. За матеріалами [3, 4] сучасні засоби радіомоніторингу за характером функціонування поділяються на 2 групи:

активні, що дозволяють розпізнавати і виявляти не функціонуючі джерела радіовипромінювання (ДРВ);

пасивні, що дозволяють виявляти і розпізнавати ДРВ, що функціонують.

Основою функціонування пасивних засобів радіомоніторингу є виявлення сигналів, що передають повідомлення (наприклад сигнал управління повітряним рухом) і розпізнавання параметрів потужних сигналів бортових, корабельних та наземних радіолокаційних станцій (РЛС). Інформативність сигналу ДРВ для засобів радіомоніторингу залежить від того, наскільки надійно цей сигнал виявляється і наскільки достовірно (точно) визначаються його параметри, що несуть корисні для радіомоніторингу повідомлення або значення. Оскільки спостереження сигналу завжди відбувається на фоні різного роду перешкод, факт виявлення сигналу, а також помилки вимірювання сигнальних параметрів і виділення повідомлень завжди виявляються випадковими [1, 3, 4].

У [1] зазначено, що корисну інформацію засоби радіомоніторингу отримують, аналізуючи електромагнітні поля $u(t,r)$ на розкриві прийомної антени $r \in L$ протягом часу $t \in [-T/2; T/2]$ на фоні просторово-часових перешкод $n(t,r)$. Якщо вважати, що сигнал і перешкоди адитивні, то:

$$u(t,r,\alpha_i) = s(t,r,\alpha_i) + n(t,r), \qquad (1)$$

де $s(t,r,\alpha_i)$ – сигнал, що залежить від часової t, просторової r координат і параметрів α_i; $n(t,r)$, – сукупність перешкод, що залежать від часової t та просторової r координат.

Просторово-часові перешкоди $n(t,r)$ викликаються спільною дією атмосфери і космічного простору, адитивних шумів антенно-фідерного тракту, інших шумів приймальної апаратури засобу радіомоніторингу.

Саме параметри α_i і просторові параметри r приносять радіомоніторингу корисну для нього інформацію. Обробка сигналу з прийомної антени станції радіомоніторингу майже завжди розділяється на просторову і на часову. Перш за все проводиться обробка сигналу в просторі. Цю операцію виконує антенна система - просторовий фільтр, що проводить селекцію сигналу на фоні перешкод з різних областей простору і визначає просторові параметри сигналу (напрямок на ДРВ). Результатом просторової обробки є, перш за все, оцінки параметрів просторового положення і руху джерела випромінювання. Потім проводиться обробка сигналу приймачем стації радіомоніторингу в часовій області. В результаті часової обробки визначаються несучі частоти, потужності випромінювання, якісні та кількісні характеристики модулюючих функцій і інші параметри сигналів ДРВ об'єктів радіомоніторингу.

Складність структури поля (складної сигнальною обстановки) обумовлюється наявністю багатьох випромінювачів радіосигналів і джерел побічних і ненавмисних випромінювань, зміною геометричних, частотних і часових параметрів випромінюваних сигналів внаслідок маневрування випромінювачів в просторі, в якому функціонують засоби радіомоніторингу (в середовищі інтересів).

Складна сигнальна обстановка є, з одного боку, предметом аналізу для засобів радіомоніторингу, в її створенні беруть участь випромінювання радіоелектронних засобів (РЕЗ) об'єктів радіомоніторингу. Але, з другого боку, складність сигнальної обстановки для засобів радіомоніторингу забезпечує процес виявлення і визначення параметрів сигналів

об'єктів радіомоніторингу на фоні неінформативних для радіомоніторингу випромінювань. Безліч непотрібних випромінювань в основному і створює той завадовий фон $n(t,r)$, який ускладнює роботу операторів станцій радіомоніторингу. Крім цього завдання радіомоніторингу полягає в спостереженні за динамікою змін сигнальної обстановки, тобто фіксації сигнальних ситуацій, що складаються з сигналів в кожен момент часу в області інтересів радіомоніторингу.

Проблема визначення типу сигналу, а отже й джерела, що його випромінює, частково вирішується за рахунок попереднього аналізу ефіру на слух, що проводять оператори станцій РТР "Кольчуга-КЕ" ("Кольчуга-М"). Це дає змогу не відволікатись на неінформативні сигнали, що належать ДРВ, які не представляють інтересу для радіомоніторингу, скоротити час пошуку ДРВ та мінімізувати витрати на амортизацію обладнання, економити технічний та обчислювальний ресурс. Недоліком даного методу можна зазначити необхідність наявності достатньої кількості навчених операторів та постійного підвищення рівня їх підготовки. Враховуючи той факт, що підготовка одного оператора до професійного рівня може тривати 6-12 міс, забезпечити дані вимоги дуже складно.

У [5-7] зазначено, що системи підтримки прийняття рішень являють собою клас комп'ютерних програм, які видають поради, проводять аналіз, виконують класифікацію, дають консультації і визначають типи. Вони орієнтовані на вирішення завдань, що зазвичай вимагають проведення експертизи людиною-фахівцем. Такі системи часто виявляються здатними знайти вирішення завдань, які неструктуровані і неявно визначені. Вони справляються з відсутністю структурованості шляхом залучення евристик, тобто правил, що описані згідно з досвідом використання апаратури, що може бути корисним в тих ситуаціях, коли недолік необхідних знань або часу виключає можливість проведення повного аналізу.

Мета статті. З метою усунення вищенаведених, негативних факторів та приведення оперативності обробки даних операторами станцій РТР "Кольчуга-КЕ" ("Кольчуга-М") до масштабу часу наближеного до реального, на базі автоматизованої системи управління засобами радіомоніторингу (АСУ РМ), метою статті є розроблення системи підтримки прийняття рішень (СППР) по визначенню типу ДРВ за параметрами сигналу.

Виклад основного матеріалу. Для забезпечення функцій СППР визначення типу ДРВ були розроблені програмні засоби реалізації системи.

Одним з ефективних підходів створення систем "запит-відповідь" є веб-служби. Веб-служба, або веб-сервіс (англ. Web service) - програмна система зі стандартизованими інтерфейсами, що ідентифікується веб-адресою.

Веб-служби можуть взаємодіяти одна з одною та зі сторонніми додатками за допомогою повідомлень, заснованих на певних протоколах (SOAP, XML-RPC і т.д.) та угодах (REST). Веб-служба є одиницею модульності при використанні сервіс-орієнтованої архітектури додатку. Основні принципи організації систем, що базуються на веб-службах описано у [8].

Протоколом взаємодії між АСУ РМ та веб-сервісом було обрано протокол SOAP так, як він дозволяє повністю реалізувати всі потреби даної експертної системи. SOAP (від англ. Simple Object Access Protocol - простий протокол доступу до об'єктів) - протокол обміну структурованими повідомленнями в розподіленому обчислювальному середовищі.

SOAP може використовуватися з будь-яким протоколом прикладного рівня: SMTP, FTP, HTTP, HTTPS та ін. Однак його взаємодія з кожним із цих протоколів має свої особливості, які повинні бути визначені окремо. Найчастіше SOAP використовується поверх HTTP.

Слід зазначити, що даний підхід дозволяє перейти до концепції побудови системи з розподіленими обчисленнями та покласти на сервер, який має великі обчислювальні можливостями та локальний доступ до системи управління базами даних СУБД, важкі та затратні по часу виконання обчислювальні завдання.

Після розгортання веб-служби на сервері є можливість перевірити її працездатність за допомогою посилання http://127.0.0.1/Scripts/soapasurtr.exe. Результатом перевірки працездатності веб-служби повинен бути html документ виду, який зображено на рис. 1.

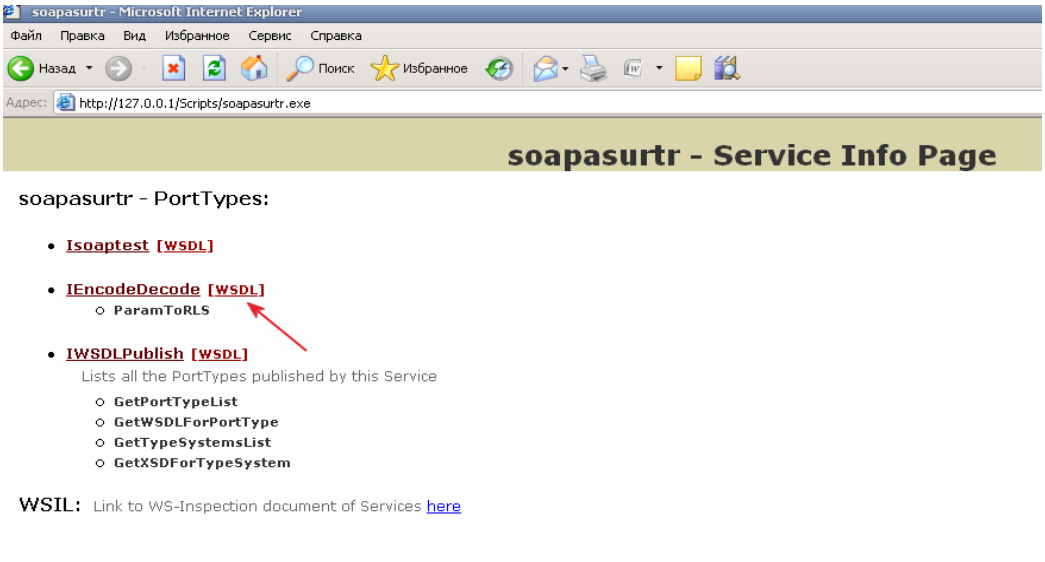

Рисунок 1 – Відповідь веб-служби на запит

Опис будь-якої веб-служби міститься у XML-документі на мові WSDL (Web Services Description Language). Отримати WSDL опис можна за допомогою посилання, що позначене стрілкою. Текст WSDL опису приведено на рис. 2.

```
<?xml version="1.0" encoding="utf-8" ?>
- <definitions xmlns="http://schemas.xmlsoap.org/wsdl/" xmlns:xs="http://www.w3.org/2001/XMLSchema" name="IEncodeDecodeservice"
    targetNamespace="http://tempuri.org/" xmlns:tns="http://tempuri.org/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
    xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/">
  - <message name="ParamToRLS0Request">
      <part name="Param1" type="xs:string" />
      <part name="Param2" type="xs:string" />
      <part name="Param3" type="xs:string" />
    </message>
  - <message name="ParamToRLS0Response">
      <part name="return" type="xs:string" />
    </message>
  - <portType name="IEncodeDecode">
    - <operation name="ParamToRLS">
        <input message="tns:ParamToRLS0Request" />
        <output message="tns:ParamToRLS0Response" />
      </operation>
    </portType>
  - <binding name="IEncodeDecodebinding" type="tns:IEncodeDecode">
      <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http" />
    - <operation name="ParamToRLS">
        <soap:operation soapAction="urn:u_Intrf-IEncodeDecode#ParamToRLS" style="rpc" />
      - <input message="tns:ParamToRLS0Request">
          <soap:body use="encoded" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" namespace="urn:u_Intrf-IEncodeDecode" />
        </input>
      - <output message="tns:ParamToRLS0Response">
          <soap:body use="encoded" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" namespace="urn:u_Intrf-IEncodeDecode" />
        </output>
      </operation>
    </binding>
  - <service name="IEncodeDecodeservice">
    - <port name="IEncodeDecodePort" binding="tns:IEncodeDecodebinding">
        <soap:address location="http://127.0.0.1/Scripts/soapasurtr.exe/soap/IEncodeDecode" />
      </port>
    </service>
</definitions>
```

Рисунок 2 – WSDL опис функції ParamToRLS (SF,ST,STau)

Варто зазначити, що дана веб-служба фізично розташована на ПЕОМ з СУБД MySQL, у контрольованій зоні, без виходу до мережі Internet. Інформація, що циркулює у системі між АСУ РМ та веб-службою, передається по каналам передачі даних АСУ ПД “Дніпро”, над якими побудована підмережа VPN (англ. Virtual Private Network - віртуальна приватна мережа), яка побудована на базі технології OpenVPN та має гарантовану стійкість криптографічного захисту [12]. Загальні принципи передачі даних між складовими АСУ РМ через підмережу OpenVPN, а також принципи побудови останньої наведено у [9].

СППР передбачає введення, накопичення, зберігання та аналіз експертних знань. З метою їх використання, користувач системи повинен мати швидкий та зручний доступ до цих знань. Вищезазначені фактори привели до обрання в якості сховища інформації базу даних. Серед багатьох систем управління базами даних було обрано СУБД MySQL (принципи побудови алгоритмів з використанням баз даних описано у [10], оскільки вона використовується у побудові самої АСУ РМ та для забезпечення програмної сумісності.

Реалізація веб-сервісу була забезпечена за допомогою системи програмування Delphi 7. Дана система підтримує всі необхідні технології, включаючи SOAP та MySQL.

Архітектура СППР визначення типу ДРВ за параметрами

Загальна архітектура СППР визначення типу РЛС зображена на рис. 3. Вона складається з таких складових:

1. "АСУ РМ Карта" – складова АСУ по відображенню картографічної інформації. Вона є ключовим, організуючим елементом у роботі комплексу в цілому.

2. Веб-служба – сервіс, що розгорнутий на базі серверної ПЕОМ. Виконує функції прийому запиту, доступу до СУБД та надання відповіді про результати.

3. СУБД MySQL – база даних, що забезпечує введення, накопичення, зберігання та видачу інформації, яка потрібна користувачу.

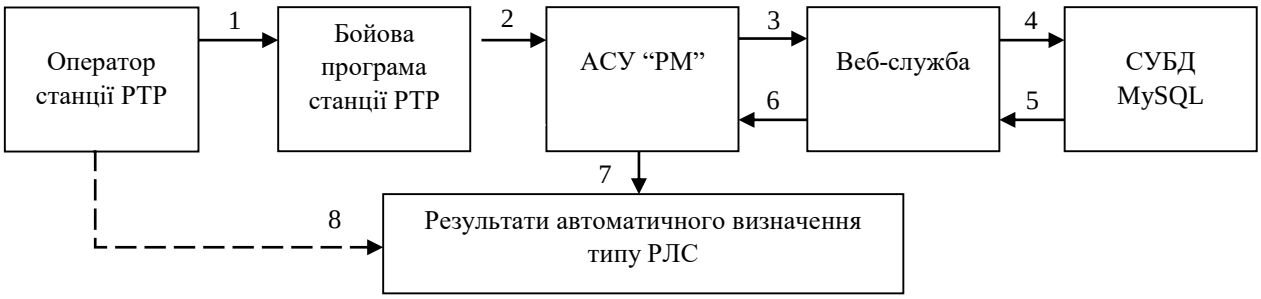

Рисунок 3 – Загальна архітектура СППР визначення типу РЛС

Робота системи у комплексі з АСУ РМ складається з декількох етапів, які позначені стрілками з номерами на рис. 3.

Після попереднього аналізу радіоефіру на слух, оператор приймає рішення про інструментальний аналіз визначеного ним сигналу від джерел розвідувальних відомостей. На **першому етапі** оператор подає команду бойовій програмі станції РТР "Кольчуга-КЕ" ("Кольчуга-М") на вимірювання, зчитування та обробку параметрів сигналу з апаратури. Результатом роботи штатної, бойової програми станції є файл з розширенням ".dat" (далі – dat-файл), що містить у собі сукупність даних про заміри за певний проміжок часу.

На **другому етапі** роботи АСУ завантажує щойно створений бойовою програмою dat-файл та вираховує з нього всі параметри сигналу, а саме: F_H (несучу частоту сигналу), T_i (період слідування імпульсів) та τ_i (тривалість імпульсів). Кожен з цих параметрів може мати декілька значень, як правило від двох до п'яти;

На **третьому етапі** система АСУ РМ формує запит до веб-сервісу у вигляді функції

$$ParamT_0RLS\left(SF, ST, STau\right), \quad (2)$$

де SF – сукупність визначених несучих частот сигналу (до п'яти значень), розділених знаком пробілу; ST – сукупність визначених періодів слідкування імпульсів у сигналі (до п'яти значень), розділених знаком пробілу; $STau$ – сукупність визначених тривалостей імпульсів у сигналі (до п'яти значень), розділених знаком пробілу.

На **четвертому етапі** веб-служба робить сукупність SQL-запитів до СУБД MySQL за визначеним алгоритмом.

На **п’ятому етапі** після отримання даних від СУБД MySQL веб-служба робить висновок про те, які типи РЛС підходять під задані параметри.

На **шостому етапі** веб-служба розставляє визначені типи РЛС у порядку убування ймовірності їх визначення та формує відповідь до АСУ у форматі:

$$N_1;P_1;N_2;P_2;...N_n;P_n, \tag{3}$$

де N_i – назва радіолокаційної станції, що визначена веб-службою; P_i – ймовірнісний коефіцієнт, що має значення в умовних пунктах (чим більше значення коефіцієнту, тим більш імовірно, що сигнал станції відповідає обрахованим параметрам).

На **сьомому** прикінцевому етапі роботи системи АСУ РМ формує інформаційне, інтерактивне табло на екрані монітора, що містить у собі відповідь від веб-служби у табличному варіанті. Вікно результатів роботи СППР на рис. 4.

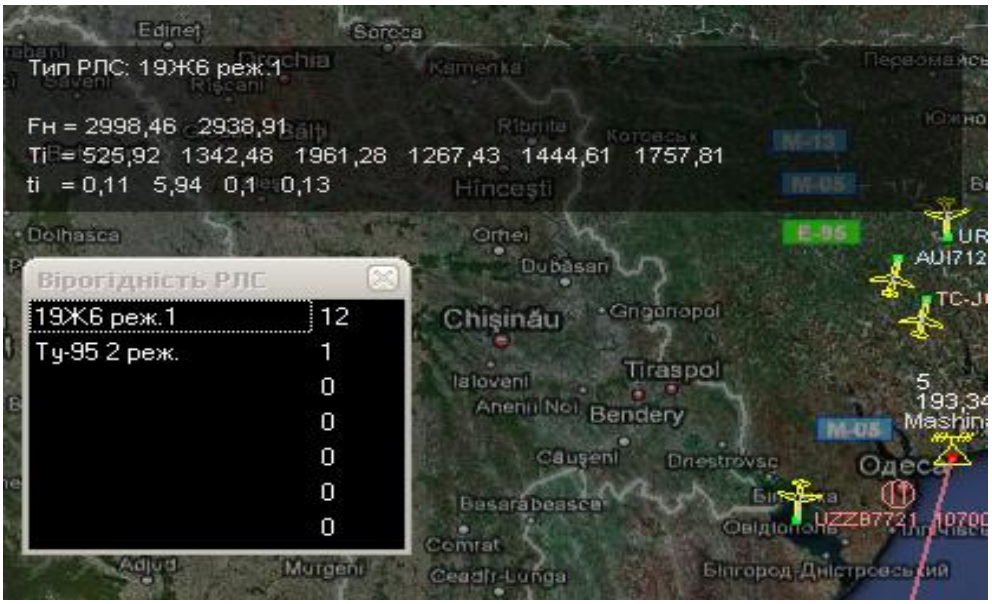

Рисунок 4 – Вигляд результатів роботи СППР визначення РЛС

На кінцевому **восьмому етапі** роботи системи оператор станції РТР “Кольчуга-КЕ” (“Кольчуга-М”) повинен підтвердити той варіант результату системи, який вважає найбільш ймовірним. Дана функція необхідна тому, що інколи ймовірність P двох, або більше РЛС приблизно однакова. В даному випадку оператор робить свій вибір спираючись на інші знання або апріорну інформацію. Підтвердження проводиться подвійним натисненням лівої кнопки маніпулятора типу “миша” на рядку з правильно визначеною РЛС. В результаті підтвердження на карту наноситься пеленг на РЛС, в разі, якщо визначена РЛС є наземною, то інформація про її роботу заноситься у таблицю та графік роботи стаціонарних РЛС. В разі виявлення бортової або корабельної РЛС інформація про неї заноситься у таблицю АСУ моніторингу повітряної (морської) обстановки (АСУ МП (М)О).

Сервер бази даних. За замовчуванням продукт підтримує базу даних MySQL, яка відноситься до реляційних систем. У даній системі використовується мова SQL-запитів. На рис. 5 представлена схема бази даних АСУ РМ в цілому та СППР про тип РЛС, як її складової частини.

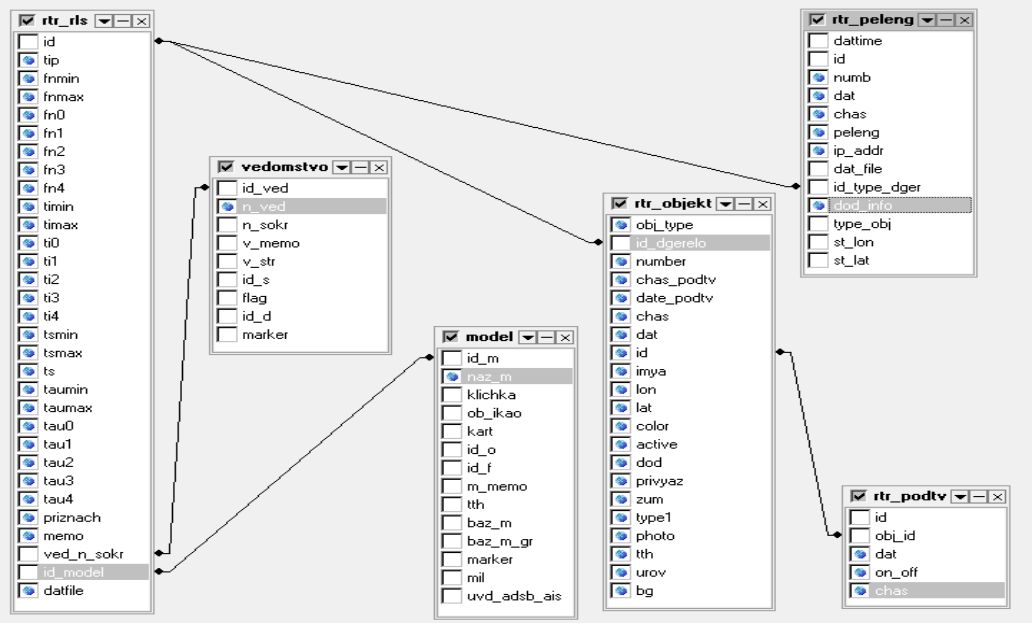

Рисунок 5 – Схема бази даних СППР визначення типу РЛС

СППР визначення типу РЛС використовує наступні таблиці бази даних:

rtr_rls – таблиця, у якій містяться основні назви та параметри сигналів, за цією таблицею проводяться основні обрахунки;

rtr_object – таблиця, що містить у собі дані про об’єкти розвідки;

rtr_peleng – таблиця містить пеленгаційну інформацію;

rtr_podtv – дані про підтвердження роботи об’єктів розвідки;

vedomstvo – таблиця, що містить назви відомств, до яких належать об’єкти розвідки;

model – таблиця типів та характеристик літальних апаратів, кораблів та наземних рухомих об’єктів. Дані у таблицю rtr_rls заносяться після перехоплення сигналу станцією “Кольчуга-КЕ” або “Кольчуга-М” та його ретельної обробки кращими експертами. Під час опису сигналу визначаються параметри та режими роботи РЛС. Після визначення параметрів РЛС дані заносяться у базу даних системи за допомогою зручної для користувача форми, після чого проводиться експериментальна перевірка на правильність надання системою оцінки по визначенню типу РЛС. На даний момент таблиця rtr_rls містить параметри більше 400-т наземних, бортових та корабельних станцій та постійно доповнюється.

Опис алгоритму програмного модуля визначення типів РЛС

Алгоритм роботи СППР визначення типу РЛС зображено на рис. 6. Даний алгоритм є складовою частиною веб-служби, що розміщена на сервері бази даних з метою підвищення швидкості доступу веб-служби до сервера бази даних, уникаючи низькошвидкісні канали передачі даних.

На першому етапі роботи алгоритму проводиться прийом та завантаження параметрів, що виміряні станцією РТР та передані через SOAP від АСУ РМ до веб-служби.

На наступному етапі визначаються допуски по частоті несучій F_H за формулами:

$$F_H max = F_H + (F_H / K_F), \quad (4)$$

$$F_H min = F_H - (F_H / K_F), \quad (5)$$

де K_F – коефіцієнт допуску, що враховує неточність визначення частоти станцією РТР “Кольчуга-КЕ” (“Кольчуга-М”). Коефіцієнт K_F визначено виходячи з міркувань похибки визначення несучої частоти сигналу апаратурою станції “Кольчуга-КЕ”, а саме ± 11 МГц та становить K_F = 2000; $F_H max$, $F_H min$ –максимальне та мінімальне значення несучої частоти з врахуванням коефіцієнту допуску.

Наступним кроком з бази даних вибираються усі можливі ДРВ, що відповідають діапазону $F_H min \geq F_H \leq F_H max)$, після чого їх назви заносяться у проміжний масив типів ДРВ. Кожне співпадіння значення F_H з довідковим додає до сумарної ймовірності вагове значення $P_{F1} = 3$.

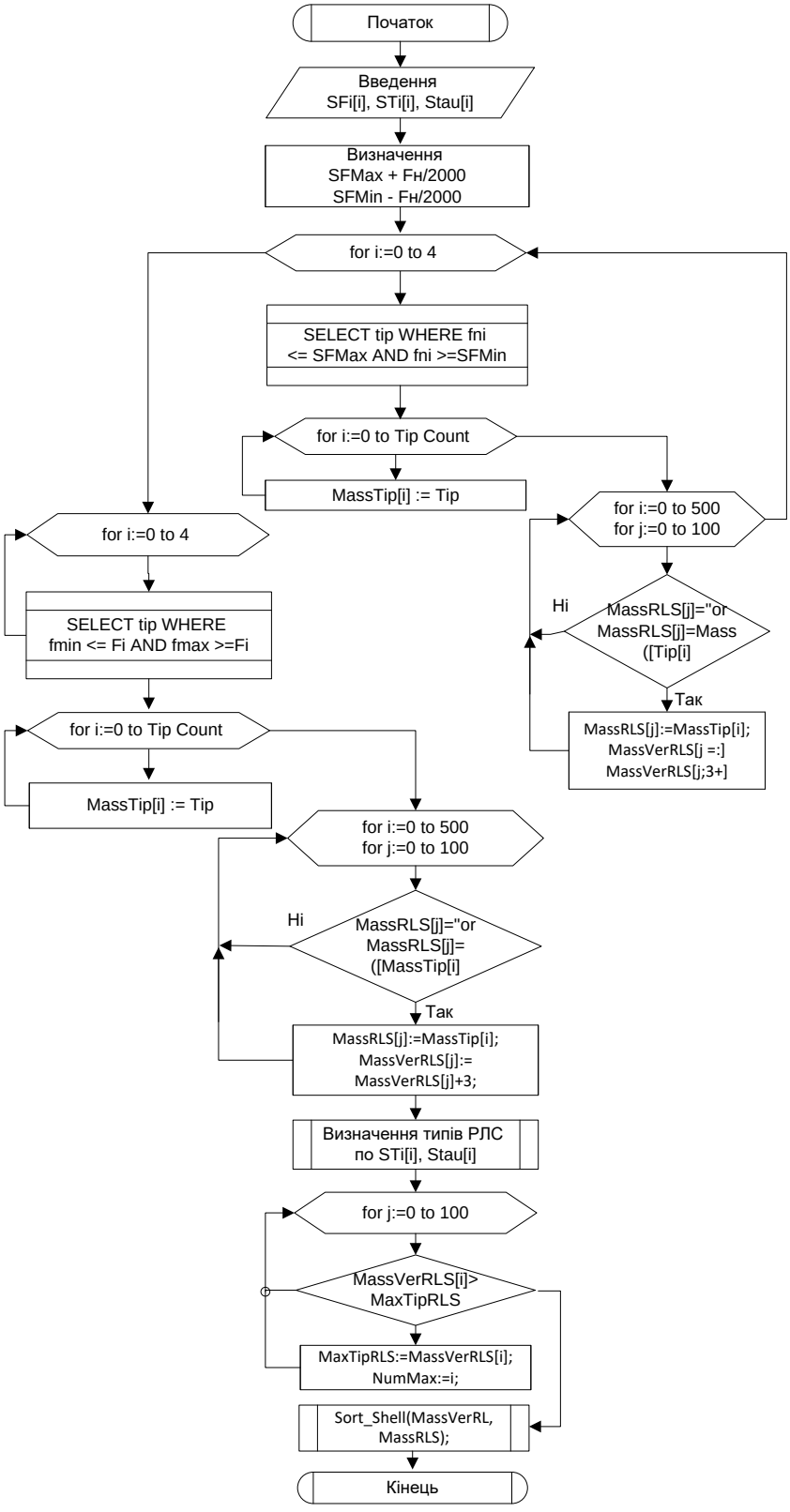

Рисунок 6 – Частковий алгоритм роботи СППР визначення типу РЛС за параметрами сигналу

По закінченню аналізу співпадання виміряних значень F_H зі значеннями у базі даних з врахуванням коефіцієнту допуску K_F запускається алгоритм пошуку ДРВ по f_{nmin} та f_{nmax} таблиці rtr_rls.

У цьому аналізі з бази даних вибираються усі можливі джерела радіовипромінювання, що відповідають діапазону $f_{nmin} \geq F_H \leq f_{nmax}$, після чого їх назви заносяться у проміжний масив типів ДРВ. Оскільки потрапляння несучої частоти у деяку зону значень носить менш інформативний характер ніж відповідність конкретному значенню, то кожне знаходження значення F_H у межах $f_{nmin} \geq F_H \leq f_{nmax}$ додає до значення ймовірності ваговий коефіцієнт $P_{F2} = 1$.

Так само працюють два блоки по пошуку відповідності заміряних значень еталонним по T_i (період слідування імпульсів) та τ_i (тривалість імпульсів). При цьому значення $T_i max$ та $T_i min$ розраховуються за формулами:

$$T_i max = T_i + (T_i / K_T), \quad (6)$$

$$T_i min = T_i - (T_i / K_T), \quad (7)$$

де K_T – коефіцієнт допуску, що враховує неточність визначення періоду слідування імпульсів станцією РТР “Кольчуга-КЕ” (“Кольчуга-М”). Оскільки середня квадратична похибка виміру T_i (періоду слідування імпульсів) не більше 0,1 мкс, а діапазон визначення цього параметру має значення 2-79999, коефіцієнт K_T визначено $K_T = 1000$;

- $T_i max$, $T_i min$ максимальне та мінімальне значення періоду слідування імпульсів з врахуванням коефіцієнту допуску.

Значення $\tau_i max$ та $\tau_i min$ розраховуються за формулами:

$$\tau_i max = \tau_i + (\tau_i / K_\tau), \quad (8)$$

$$\tau_i min = \tau_i - (\tau_i / K_\tau), \quad (9)$$

де K_τ – коефіцієнт допуску, що враховує неточність визначення періоду слідування імпульсів станцією РТР “Кольчуга-КЕ” (“Кольчуга-М”). Оскільки середня квадратична похибка виміру τ_i (тривалість імпульсів) не більше 0,1 мкс, коефіцієнт K_τ визначено та становить $K_\tau = 2000$;

– $\tau_i max$, $\tau_i min$ – максимальне та мінімальне значення тривалості імпульсів з врахуванням коефіцієнту допуску.

Під час сумування вагових коефіцієнтів у випадках з T_i та τ_i значення вагових коефіцієнтів $P_\tau = 1$ та $P_\tau = 1$.

Після створення масиву зі списком ДРВ та їх сумарними ймовірнісними параметрами, параметри яких у більшій або меншій мірі співпадають з еталонними, алгоритм роботи системи відпрацьовує сортування масиву, яке розміщує ДРВ у порядку убування їх ймовірнісних показників.

Останнім етапом роботи веб-сервісу є формування відповіді до АСУ РМ та передача її за протоколом SOAP. Після отримання відповіді від веб-сервісу, АСУ РМ виводить значення таблиці типів ДРВ на підтвердження оператору станції РТР “Кольчуга-КЕ” (“Кольчуга-М”), як показано на рис. 4.

Оцінка підвищення ефективності [13, 14] роботи засобів розвідки у складі АСУ РМ з використанням СППР, проводилась шляхом експерименту під час дослідної експлуатації, у порівнянні з традиційним використанням за призначенням, що наведено у таблиці 1.

Таблиця 1

Оцінка підвищення ефективності роботи засобів розвідки у складі АСУ РМ з використанням СППР

№ з/п	Найменування засобу радіомоніторингу дії по добуванню інформації	Традиційне використання	Використання у складі АСУ РМ	Підвищення ефективності
1	Станція РТР Кольчуга-КЕ (Кольчуга-М)			
1.1	Пеленгування повітряних, надводних та стаціонарних об'єктів за сигналом РЛС	До 5 хв.	5-10 сек.	Так (у %)
1.2	Автоматичне пеленгування та декодування сигналів ADSB, AIS, УВД	Ні	Так	Так
1.3	Можливість автоматичної проводки цілі за інформацією від декількох станцій РТР	Ні	Так	Так
1.4	Наявність системи, що дозволяє застосування оператора з низькою кваліфікацією	Ні	Так	Так
1.5	Відображення на карті стану стаціонарних джерел радіовипромінювання	Ні	Так	Так
2	Пеленгування у КХ діапазоні			
2.1	Запит на пеленгування, отримання результату	1-2 хв	3-5 сек.	Так(у %)
2.2	Візуалізація результатів пеленгування на карті	Ні	Так	Так
2.3	Можливість статистичного аналізу результатів пеленгування	Ускладнено	Так	Так
2.4	Вплив людського фактору під час пеленгування	Так	Ні	Так
3	Пеленгування у УКХ діапазоні			
3.1	Запит на пеленгування, отримання результату	1-2 хв	1-2 сек.	Так (у %)
3.2	Візуалізація результатів пеленгування на карті	Ні	Так	Так
3.3	Можливість статистичного аналізу результатів пеленгування	Ні	Так	Так
3.4	Наявність людського фактору під час пеленгування	Так	Ні	Так
4	Доведення розвідувальної інформації до користувача	До 5 хв.	(близький до реального)	Так
4.1	У таблиці АСУ РМ	(не було)	До 30 сек.	
4.2	По карті АСУ РМ		Миттєво	
5	Потреба у серверному обладнанні та високошвидкісних каналах ПД	Ні	Так	Ні
6	Автоматичне прогнозування майбутніх подій аналізуючи дійсний стан засобів ведення БД	Ускладнено	Так, автоматично	Так

Очевидно, що використання засобів розвідки у складі АСУ РМ з використанням розробленої СППР, значно підвищує ефективність роботи системи радіомоніторингу в цілому. Як недолік такого варіанту використанні засобів радіомоніторингу можна зазначити лише деяке ускладнення комунікацій, а також необхідність наявності серверного обладнання та швидкісних каналів зв'язку. Враховуючи той факт, що в результаті роботи всіх засобів у єдиному інформаційному полі радіомоніторингу, зростає ефективність по всім параметрам, а також з'являються нові можливості, дане ускладнення нівелюється.

Висновки. З метою вирішення наукового завдання автоматизації процесу виявлення та розпізнавання джерел радіовипромінювань, розроблена система підтримки прийняття рішення по визначенню типу ДРВ за параметрами його сигналу для системи радіомоніторингу України. Оскільки система надає рекомендації оператору станції РТР "Кольчуга-КЕ" ("Кольчуга-М") щодо вибору найбільш ймовірного варіанту, вимоги до кваліфікації операторів можуть бути знижені, що суттєво скорочує фінансові та часові затрати на їх підготовку, а сам процес роботи на станції стає частиною навчання оператора.

Напрямки подальших досліджень щодо удосконалення програмного алгоритму оцінки сигналу, за умови глибокої модернізації апаратури, дозволить перейти до напівавтоматичної або цілком автоматичної роботи станції РТР, що відкриє нові можливості та суттєво підвищить ефективність ведення радіомоніторингу за рахунок підвищення оперативності та достовірності прийняття рішень операторами постів РТР.

ЛІТЕРАТУРА:

1. Варламов І.Д., Устименко О.В., Гаценко С.С. Шляхи удосконалення ведення радіоелектронного моніторингу засобів повітряного нападу. Збірник матеріалів 10 наукової конференції "Новітні технології – для захисту повітряного простору". Харків: ХУПС, 2014. С. 232-233.
2. Варламов І.Д., Гаценко С.С. Аналіз проблем інформаційного забезпечення органів військового управління при плануванні оборонної операції за досвідом проведення Антитерористичної операції на сході України. Матеріали науково-практичного семінару "Основні напрямки застосування космічних систем та геоінформаційного забезпечення в інтересах національної безпеки і оборони"/ Київ: НУОУ, 2015. С. 35-41.
3. Максименков А. Современные средства радиотехнической разведки иностранных государств. Зарубежное военное обозрение №6. Москва: 2013. 102с.
4. Смирнов Ю. А. Радиотехническая разведка. М.: Воениздат, 2001. 456 с.
5. Ситник В. Ф. Системи підтримки прийняття рішень: Навч. посіб. К.: КНЕУ, 2004. 614 с
6. Потрашкова Л.В., Комп'ютерна підтримка прийняття рішень у сфері дизайну поліграфічної продукції.: Системи обробки інформації, 2010, випуск 7 (88)
7. Marius Cioca, Florin Filip (2015). Decision Support Systems - A Bibliography 1947-2007
8. Ouzzani, M., Bouguettaya A. Semantic Web Services for Web Databases. Springer Science+Business Media, 2011. 155 c.
9. Beginning OpenVPN 2.0.9 by Markus Feilner and Norbert Graf. Publisher: Packt Publishing, 2009.
10. Фаронов В.В., Шумаков П.В / Delphi 5. Руководство разработчика баз данных. Москва: «Нолидж», 2000. 640 с., ил.
11. Варламов І.Д., Гаценко С.С., Бучинський Ю.А. Особливості побудови та практичної реалізації автоматизованої системи управління розвідкою К., НУОУ, Труди університету. 2017. - № 6(145), С. 44–54.
12. Beginning OpenVPN 2.0.9 by Markus Feilner and Norbert Graf. Publisher: Packt Publishing, 2009.
13. Смірнов Ю. О. Основи радіоелектронної розвідки. Частина 1. Розвідувально-інформаційний процес, основні моделі системи РЕР ефективність і напрями її подальшого розвитку. К.: НДІ ГУР МО України, 2009. 155с.
14. Бакуменко Ф.О. Методика оцінки ефективності воєнної розвідки в операції і бою. К.: НАОУ, 1998. 64 с.

REFERENCES:

1. Varlamov I`.D., Ustimenko O.V., Gaczenko S.S. Shlyakhi udoskonalennya vedennya radi`oelektronnogo moni`toringu zasobi`v povi`tryanogo napadu. Zbi`rnik materi`ali`v 10 naukovoyi konferenczi`yi "Novi`tni` tekhnologi`yi – dlya zakhistu povi`tryanogo prostoru". Kharki`v: KhUPS, 2014. S. 232-233.

2. Varlamov I`.D., Gaczenko S.S. Anali`z problem i`nformaczi`jnogo zabezpechennya organi`v vi`js`kovogo upravli`nnya pri planuvanni` oboronnoyi operaczi`yi za dosvi`dom provedennya Antiteroristichnoyi operaczi`yi na skhodi` Ukrayini. Materi`ali naukovo-praktichnogo semi`naru "Osnovni` napryamki zastosuvannya kosmi`chnikh sistem ta geoi`nformaczi`jnogo zabezpechennya v i`nteresakh naczi`onal`noyi bezpeki i` oboroni"/ Kiyiv: NUOU, 2015. S. 35-41.

3. Maksimenkov A. Sovremenny`e sredstva radiotekhnicheskoj razvedki inostranny`kh gosudarstv. Zarubezhnoe voennoe obozrenie #6. Moskva: 2013. 102s.

4. Smirnov Yu. A. Radiotekhnicheskaya razvedka. M.: Voenizdat, 2001. 456 s.

5. Sitnik V. F. Sistemi pi`dtrimki prijnyattya ri`shen`: Navch. posi`b. – K.: KNEU, 2004. – 614 s

6. Potrashkova L.V., Komp'yuterna pi`dtrimka prijnyattya ri`shen` u sferi` dizajnu poli`grafi`chnoyi produkczi`yi.: Sistemi obrobki i`nformaczi`yi, 2010, vipusk 7 (88)

7. Marius Cioca, Florin Filip (2015). Decision Support Systems – A Bibliography 1947-2007

8. Ouzzani, M., Bouguettaya A. Semantic Web Services for Web Databases. Springer Science+Business Media, 2011. 155 s.

9. Beginning OpenVPN 2.0.9 by Markus Feilner and Norbert Graf. Publisher: Packt Publishing, 2009.

10. Faronov V.V., Shumakov P.V / Delphi 5. Rukovodstvo razrabotchika baz danny`kh. Moskva: «Nolidzh», 2000. 640 s., il.

11. Varlamov I`.D., Gaczenko S.S., Buchins`kij Yu.A. Osoblivosti` pobudovi ta praktichnoyi reali`zaczi`yi avtomatizovanoyi sistemi upravli`nnya rozvi`dkoyu K., NUOU, Trudi uni`versitetu. 2017. - # 6(145), S. 44–54.

12. Beginning OpenVPN 2.0.9 by Markus Feilner and Norbert Graf. Publisher: Packt Publishing, 2009.

13. Smi`rnov Yu. O. Osnovi radi`oelektronnoyi rozvi`dki. Chastina 1. Rozvi`duval`no-i`nformaczi`jnij proczes, osnovni` modeli` sistemi RER efektivni`st` i` napryami yiyi podal`shogo rozvitku. K.: NDI` GUR MO Ukrayini, 2009. 155s.

14. Bakumenko F.O. Metodika oczi`nki efektivnosti` voyennoyi rozvi`dki v operaczi`yi i` boyu. K.: NAOU, 1998. 64 s.

к.т.н. Гаценко С.С., Писаренко Р.В., Лукьянчиков И.М.,
Ошкодер С.В., Николаенко В.П., Приходько О.Г.

ИНФОРМАЦИОННАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ РАДИОМОНИТОРИНГОМ

Вооруженная агрессия Российской Федерации против Украины, потеря важных промышленных потенциалов, как Государственная акционерная холдинговая компания «Топаз», которая специализировалась на разработке и производстве сложных радиотехнических систем и комплексов, в том числе уникальных комплексов дальней радиотехнической разведки и раннего предупреждения систем противовоздушной обороны, в частности станции радиотехнической разведки «Кольчуга», дала значительный толчок для развития новых подходов к ведению радиомониторинга обстановки, как одного из главных, а иногда единственного способа добычи информации.

Такой сложный вид технической деятельности, как радиомониторинг, требует значительных усилий для его поддержания в готовности. Постоянное обеспечение радиомониторинга необходимым количеством высококвалифицированных специалистов, имеющих большой опыт определения типа источника радиоизлучения, требует значительных усилий для их поиска и обучения. Обучение специалиста этого класса занимает не менее 1-1,5 лет и значительные финансовые затраты. Решение научной задачи автоматизации процесса обнаружения и распознавания является одним из приоритетных направлений развития радиомониторинга.

Современный радиомониторинг характером функционирования делится на 2 группы:

активный, что позволяет распознавать и выявлять неработающие источники радиоизлучения; пассивные, позволяющие идентифицировать и распознавать функционирующие источники радиоизлучения.

Основой функционирования пассивных средств радиомониторинга является выявление сигналов, передают сообщение (например сигнал управления воздушным движением) и распознавания параметров мощных сигналов бортовых, корабельных и наземных радиолокационных станций. Информативность сигнала источника радиоизлучений для средств радиомониторинга зависит от того, насколько надежно этот сигнал оказывается и насколько достоверно (точно) определяются его параметры, несущие полезные для разведки сообщение или значение. Поскольку наблюдения сигнала всегда происходит на фоне различного рода помех, факт обнаружения сигнала, а также ошибки измерения сигнальных параметров и выделение сообщений всегда оказываются случайными.

В статье рассмотрены актуальная научная задача автоматизации процесса обнаружения и распознавания источников радиоизлучения, за счет разработки системы поддержки принятия решений по определению типа источников радиоизлучения по параметрам его сигнала в интересах системы радиомониторинга государства, предоставляет указания операторам РТР Кольчуга-КЕ (Кольчуга-М) по выбора наиболее вероятного варианта решения, снизит квалификационные требования к операторам, что значительно сократит финансовые и временные затраты на их подготовку.

Ключевые слова: система радиомониторинга, кризисный регион, эффективность, вероятность, объекты радиомониторинга, источники радиомониторинга.

Ph.D. Hatsenko S.S., Pysarenko R.V., Lukianchykov I.M.,
Oshkoder S.V., Nykolaienko V.P., Prykhodko O.G.

INFORMATION SYSTEM FOR SUPPORTING DECISIONS OF AUTOMATED RADIO MONITORING CONTROL SYSTEM

Armed aggression of the Russian Federation against Ukraine, loss of important industrial potentials, as Topaz state-owned holding company, which specialized in the development and production of complex radio engineering systems and complexes, including unique long-range radio intelligence systems and early warning of air defense systems, Kolchuga radio intelligence has given a significant impetus to the development of new approaches to conducting radio monitoring of the situation, as one of the main tion method of obtaining information.

Such a complex type of technical activity as radio monitoring requires considerable effort to maintain it in readiness. The continuous provision of radio monitoring by the required number of highly qualified specialists with extensive experience in determining the type of radio source requires considerable effort to find and train them. Training of a specialist in this class takes at least 1-1.5 years and significant financial costs. Solving the scientific task of automating the process of detection and recognition is one of the priority areas for the development of radio monitoring.

Modern radio monitoring character of functioning is divided into 2 groups:

active, which allows to identify and detect non-functioning sources of radio emission; passive, allowing you to identify and recognize functioning radio sources.

The basis for the operation of passive radio monitoring is the detection of signal transmitting messages (such as air traffic control signal) and the recognition of the parameters of the powerful signals of onboard, ship and ground radar stations. The informative nature of the radio source signal for radio monitoring facilities depends on how reliably the signal is detected and how accurately (accurately) its parameters are determined, which are useful for the intelligence of the message or value. Since signal monitoring always occurs against a background of all sorts of obstacles, the fact of detecting a signal, as well as errors in measuring signal parameters and message selection are always random.

The article deals with the actual scientific task of automating the process of detection and recognition of radio sources, by developing a decision support system for determining the type of sources of radio radiation by its signal parameters in the interests of the state monitoring system, which provides guidance to the MTS-Kolchuga RTR operators the choice of the most likely variant of the decision that will reduce the qualification requirements for the operators, which will significantly reduce the financial and time costs for their preparation.

Keywords: radio monitoring system, crisis region, efficiency, probability, radio monitoring facilities, sources of radio monitoring.

УДК 004.522

д.т.н., проф. **Мясищев А.А**. (ХмНУ)
д.т.н., проф. **Ленков С.В.** (ВИКНУ)
д.т.н., с.н.с. **Комарова Л.А.** (ОНАЗ им.О.С. Попова)
к.т.н. **Ленков Е.С.** (ЦНИИ ВСУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-02

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ РЕЖИМА RESCUE В ПРОШИВКЕ BETAFLIGHT ДЛЯ БПЛА НА БАЗЕ КОНТРОЛЛЕРА STM32F405

В работе рассматривается практическая возможность реализации режима GPS Rescue для прошивки Betaflight ver.4.1.1 с целью возврата квадрокоптера(БПЛА) в точку, близкой по координатам точке взлета. В связи с этим был построен экспериментальный образец с рамой 250мм, но которой установлен полетный контроллер OMNIBUSF4V3 на базе микроконтроллера STM32F405 с GPS приемником и курсовой видеокамерой для обеспечения полетов по FTP. Для получения полетных данных с целью анализа правильности работы алгоритма возврата коптера был настроен Betaflight OSD. В процессе летных испытаний показано, что режим GPS Rescue позволяет вернуть БПЛА в зону запуска при условии соблюдения представленных в работе настроек на собранном квадрокоптере. При выполнении режима GPS Rescue важным условием является стабильная связь GPS приемника с количеством спутников не меньшим установленных при настройке прошивки. Если количество спутников становиться меньше установленного, то в течении нескольких секунд моторы выключаются и коптер падает.

Показано, что для устойчивой работы режима GPS Rescue коптер при полете должен использовать режим стабилизации(Angle) с включенным акселерометром, выполнять полет с небольшими углами наклона. Установлено, что чем больше угол наклона копрера, тем меньшее число спутником ловит GPS приемник. Поэтому режим GPS rescue не целесообразно использовать в режимах полета Acro, 3D, Horizon при совершении flip-ов.

Практически установлено, что режим GPS Rescue более целесообразно использовать в случае обрыва видео связи с курсовой камерой (FPV полеты) при сохранении связи с пультом управления. В этом случае теряется ориентация полета и коптер в автоматическом режиме необходимо вернуть в зону видеосвязи. Для этого на пульте управления устанавливается режим стабилизации (angle) и включается режим GPS Rescue. При установлении видеосвязи, определении местоположения режим GPS Rescue отключается с пульта и коптер может продолжать полет по FPV.

Было замечено, что при нарушении связи с пультом управления автоматически включается режим GPS Rescue. При этом коптер возвращается в точку старта и в случае восстановления радиосвязи коптер автоматически восстанавливает управление с пультом. Этот момент должен быть отслежен пилотом, в противном случае коптер может потерпеть аварию. Поэтому целесообразно в случае потери связи тумблер на пульте управления установить в режим GPS Rescue. Тогда коптер при восстановлении радиосвязи сработает по режиму GPS Rescue с пульта и автоматически вернется в зону старта и может быть обнаружен визуально с последующим управлением с пульта.

Ключевые слова: OMNIBUSF4V3, OSD Betaflight, INAV, GPS приемник, FPV, STM32F405, GPS Rescue, GLONASS, NEO-6M-0-001, Beitian BN-880.

Постановка задачи. В настоящее время все шире используется класс микрокоптеров с размерами рамы 160x220x250 мм и весом не бодее 400 грамм. Они, как правило используются для полетов от первого лица [1]. Их еще называют First Person View (сокр. FPV). В этом случае осуществляется не только управление квадрокоптером по радиоканалу с помощью системы радиоуправления, но и приём с него видео изображения по дополнительному видео-радиоканалу обычно на частоте 5.8 ГГц в режиме реального времени. Пилот, управляющий квадрокоптером, видит изображение, получаемое с видеокамеры при помощи устройств отображения: мониторов, телевизоров, видео-очков, видео-шлемов. Развитие микроэлектроники позволило резко увеличить зону уверенного приема радиосигнала как

управления коптером, так и видеоизображения. С помощью бюджетных приемопередатчиков зона уверенной связи достигает 5-8 км при полете в зоне прямой видимости, а бортового источника питания для таких микро коптеров хватает на полет со средней скоростью 60-70 км/час на 14-16 минут. Таким образом радиус действия таких летающих устройств составляет до 7-8 км. Это позволяет их использовать в качестве эффективных средств для видеоразведки. На этих коптерах устанавливают кроме курсовой камеры еще пишущую видеокамеру с высоким разрешением, которая позволяет при возврате коптера просматривать маршрут полета с HD качеством. Однако при полете на дальние расстояния особенно через небольшие населенные пункты, где работают, например, системы мобильной связи, возникают сильные помехи особенно по видеопередаче. Поэтому пилот во время таких помех может не сориентироваться на местности и потерять управление коптером, что приводить к его аварии. Для этого необходимо на таких видеоразведчиках использовать систему автоматического возврата в точку старта в случае потери связи. При появлении связи система должна быть способна вернуть пилоту ручное управление с помощью пульта. В работе рассматривается создание экспериментального коптера и его тестирование с размером рамы 250мм, весом не более 400гр, способным на бортовом аккумуляторе пролетать расстояние до 8км и автоматически возвращаться в случае потери радиосвязи с пилотом.

Анализ последних исследований. В настоящее время уделяется большое внимание построению беспилотных летательных аппаратов роторного типа(квадрокоптеров) [1,4,15]. Для них созданы прошивки, которые обеспечивают не только их горизонтальную стабилизацию, но и полет по заданным точкам в автоматическом режиме, удержание позиции, автоматического возврата в точку старта [4,6,15]. Однако эти разработки ведутся для коптеров относительно большого размера (2-5 кг) [15], на которых устанавливается относительно дорогое оборудование и которые летают с небольшими скоростями (20-35 км/час). Для возврата в точку старта в качестве обязательной опции используется магнитометр, являющийся достаточно капризным устройством, который требует установки в вдалеке от моторов для уменьшения магнитного воздействия. Выше отмечено, что в настоящее время появился класс микрокоптеров малого веса с достаточно высокими скоростными характеристиками и дальностью полета. Поскольку в режиме FPV [1,8] для выполнения видеоразведки им достаточно иметь режим возврата в точку старта без обеспечения высокой точности. Она должна быть такой, которая обеспечила бы перехват автоматического возврата коптера пультом управления при восстановлении видеосвязи. В связи с этим в работе рассматривается изготовление и настройка коптера на базе полетного контроллера OMNIBUSF4V3[7] с прошивкой Betaflight [2,3,9] и GPS [4] приемника, что обеспечит возврат коптера в зону радиосвязи в любых аварийных ситуациях. Эта работа связана с практическим исследованием возможности возврата коптера в режиме GPS Rescue [9 - 14] для прошивки Betaflight ver.4.1.1 [2,3], которая является последней и стабильной на момент написания статьи.

Изложение основного материала работы. Ранее было отмечено, что режим GPS Rescue [11,12] предназначен для автономного возвращения беспилотного летательного аппарата, в нашем случае квадрокоптера к месту его запуска в случае возникновения чрезвычайной ситуации, например, при потере видеосигнала или радиосвязи. Однако разработчики прошивки betaflight начиная с версии 3.5 не гарантируют надежный возврат в точку запуска. В дальнейших версиях надежность возврата увеличивается, что требует экспериментальных запусков и настроек параметров для этого режима в обновленных версиях. В данной работе рассматривается тестирование GPS Rescue для версии 4.1.1. GPS Rescue не является полной функцией «Return to home» (RTH). Этот режим не предназначен для того, чтобы быть инструментом самостоятельного полета квадрокоптера, и его не стоит использовать для этих целей. У GPS Rescue нет способности к автоматической посадке, и он намеренно управляет «мягким падением коптера», когда тот приближается к исходной точке. Цель режима - вернуть коптер ближе к точке старта, чтобы пилот БПЛА мог возобновить управление в случае потери

сигнала. Пилот должен возобновить контроль как можно скорее и не допустить, чтобы GPS Rescue выполнил приземление коптера, т.к. это может выполнить его поломку. Эта работа связана с постройкой квадрокоптера и его настройкой для тестирования указанного режима с целью заключения пригодности для надежного возврата в зону уверенной радиосвязи с последующим "мягким" приземлением коптера в ручном режиме.

Для реализации этого режима должны быть выполнены требования:

- наличие приемника GPS. Рекомендуются модели - варианты Ublox m8n u-blox - пример Beitian BN880. Данный приемник может работать одновременно с двумя или тремя из систем BeiDou, Galileo, GLONASS, GPS, что позволяет ему ловить для позиционирования большое количество спутником (14-18), увеличивая при этом точность позиционирования. В работе использован модуль NEO-6M-0-001[4], который поддерживает одновременную работу с одной из систем GNSS (спутниковая система навигации) и поэтому устанавливает связь с меньшим количеством спутников (6-11). В настоящее время реально глобально работающими являются две спутниковые навигационные системы: GLONASS и GPS.

- акселерометр должен быть включен, режиму спасения необходимо, чтобы квадрокоптер был выровнен.

- барометр для работы режима не является обязательным [9,11], но если он установлен на полетном контроллере, то его целесообразно включить. Его также удобно использовать в случае вывода на экран монитора в режиме полета по FPV данных телеметрии. Например - более точного значения высоты полета и скорости подъема и снижения по сравнению с данными GPS приемника.

- этот режим не требует магнитометра, однако при его установке будет использоваться.

- если в прошивке включена функция 3D, то режим GPS Rescue будет отключен. 3D предусматривает полет коптера "вверх ногами" для выполнения пилотажных трюков при быстром прохождении сложных преград. В этом случае ориентация антенны GPS меняется и возможна потеря спутников, что приведет к отключению моторов и падению коптера.

В работе режим GPS Rescue установлен на конкретном экспериментальном коптере, который для полетов использует FPV камеру, видеопередатчик, GPS приемник, полетный контроллер с барометром и обязательно с микросхемой OSD, поддерживаемой прошивкой betaflight ver.4.1.1. На рис. 1 показано фото этого квадрокоптера на раме ZMR250.

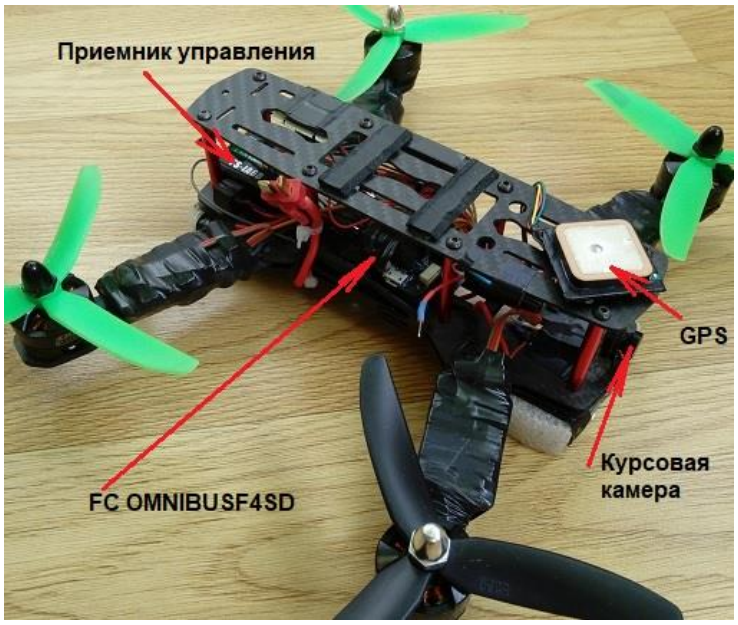

Рисунок 1 – Фото экспериментального квадрокоптера

На рис. 2 представлено схематическое взаимодействие основных элементов квадрокоптера на базе полетного контроллера OMNIBUSF4V3[7]. Необходимо отметить, что

видеопередатчик с курсовой камерой должны быть подключены к аккумулятору через отдельный преобразователь напряжения, например, на 5V. Это связано с большим током потребления во время работы видеопередатчика.

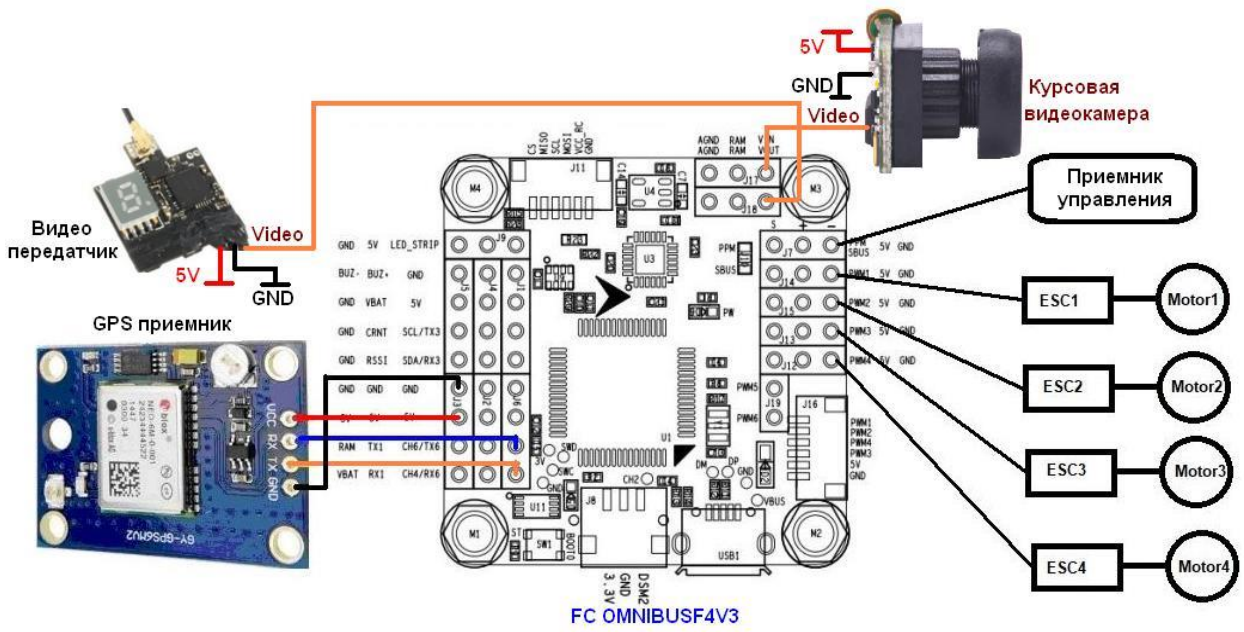

Рисунок 2 – Взаимодействие основных элементов тестируемого квадрокоптера

Рассмотрим настройку установленных основных параметров электронных компонентов исследуемого квадрокоптера в конфигураторе betaflight ver. 10.6.0[3].

Во вкладке "Порты" необходимо настроить полетный контроллер для работы с GPS приемником по UART6. Так как приемник управления работает в режиме PPM в этой вкладке больше ничего не настраивается.

Порты

WIKI

Примечание: не все комбинации этих настроек являются верными и если прошивка контроллера это поймёт, то она сбросит конфигурацию этого порта.
Примечание: **НЕ ОТКЛЮЧАЙТЕ** MSP на первом в списке порту, если вы не знаете, что делаете. Сделав это можно случайно перепрошить и стереть конфигурацию.

Идентификатор	Конфигурация и MSP	Serial Rx	Выход телеметрии	Вход датчиков	Периферия
USB VCP	115200		Отключено AUTO	Отключено AUTO	Отключено AUTO
UART1	115200		Отключено AUTO	Отключено AUTO	Отключено AUTO
UART3	115200		Отключено AUTO	Отключено AUTO	Отключено AUTO
UART6	115200		Отключено AUTO	GPS 38400	Отключено AUTO

В вкладке "Конфигурация" устанавливаются показанные на рис. 3 параметры.

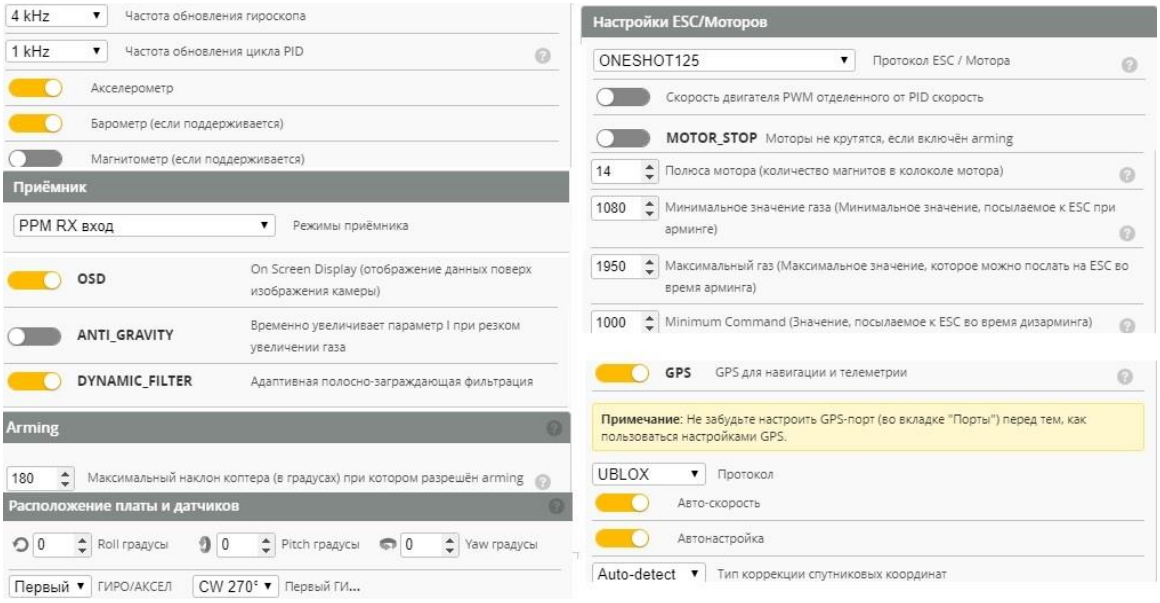

Рисунок 3 – Параметры вкладки "Конфигурация"

Рассмотрим настройку OSD для прошивки betaflight [8]. Betaflight OSD (On Screen Display, экранное меню) – это микросхема в полетном контроллере под управлением Betaflight, которая накладывает полетные данные(телеметрию) на видео, передаваемое с квадрокоптера (высота полета, скорость, расстояние от точки взлета, направление к точке взлета(стрелка), напряжение батареи, число подключенных спутников, режимы полета и т.д.).

OSD можно использовать как меню для изменения настроек коптера: PID, рейты, переключать профилей и т.д. На исследуемом коптере установлен полетный контроллер OMNIBUSF4V3 с OSD микросхемой AT7456.

Для программной настройки OSD в конфигураторе betaflight необходимо войти во вкладку OSD и установить там необходимые параметры, которые должны отображаться на экране видеоприемника для FPV полетов (рис. 4).

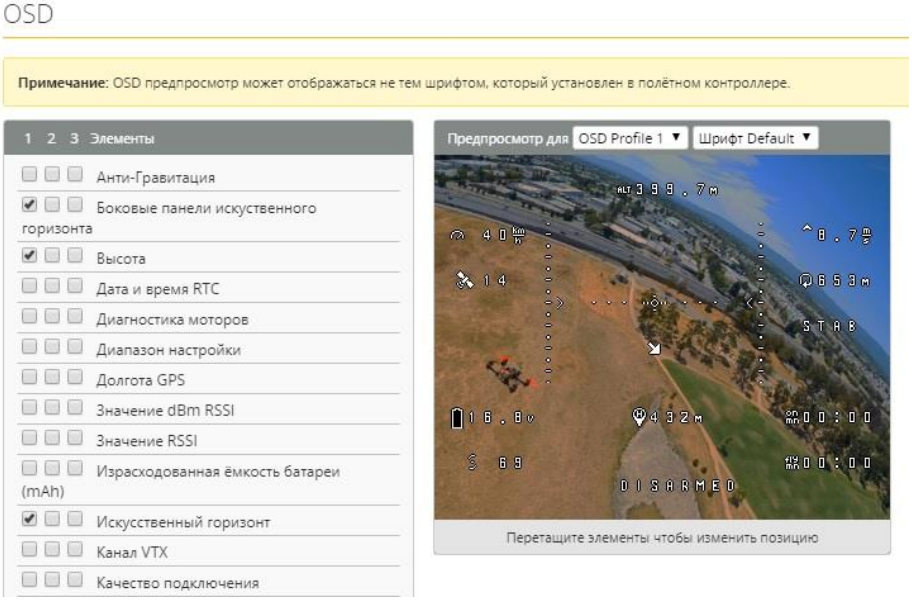

Рисунок 4 – Настройка OSD

Отображаемые параметры выбираются из таблицы слева. В работе выбрано отображение боковых панелей искусственного горизонта, высота полета, искусственный горизонт, стрелка направления домой (обязательна для режима GPS Rescue), напряжение батареи, процентное положение газовой заслонки, прицел полета, расстояние до точки взлета, общее пройденное

расстояние, режим полета (Acro, Horizon), скорость изменения высоты, скорость по GPS, количество пойманных спутников, время работы батареи и полета, Disarmed. Изменение размещения выбранных параметров на экране выполняется перетаскиванием их с помощью мыши. Если параметров много, чтобы они не мешали видеопросмотру, их можно размещать в других профайлах, которые представлены в таблице слева как 1,2,3. В OSD Betaflight имеется возможность входа в встроенное меню для изменения, например, параметров PID регулятора. Для этого на аппаратуре управления необходимо правый стик отклонить до конца вверх, а левый кратковременно с средней позиции влево. После этого появляется новое меню для настоек, для входа в каждое вложенное подменю, а также для изменения параметра. Для изменения параметра (например, PID регулятора) необходимо кратковременно отклонять влево правый стик. Работа с меню OSD возможна лишь в режиме Disarm (не в полете). На рис. 5 показаны примеры работы настроенного OSD. Первые два фото представлены с закрытым объективом камеры. Они отображают параметры во время полета и после приземления. Третье фото отображает параметры PID-регулятора после входа в встроенное меню для установки параметров. В последнем фото объектив камеры в открытом состоянии - параметры OSD наложены на видеоизображение.

OSD с закрытой камерой при arming | OSD с закрытой камерой после полета (disarming) | Вход в меню OSD для изменения параметров PID регулятора

Рисунок 5 – Пример результата работы настроенного OSD

Рассмотрим настройку режима GPS Rescue. Поскольку режим экспериментальный, то настраивается на только что установленной прошивке в соответствии с четко документированной последовательностью. Необходимо отметить, что в ранней версии betaflight 3.5, где этот режим только появился, использовался только командный режим установки параметров во вкладке cli (командная строка). В рассматриваемой версии betaflight 4.1.1 во вкладке failsafe доступен раздел для настройки GPS Rescue. Для активизации режима необходимо перейти на вкладку Betaflight Modes и добавить переключатель для режима GPS Rescue (рис. 6). Этот режим будет активизирован, если правильно установлен приемник GPS (рис. 3).

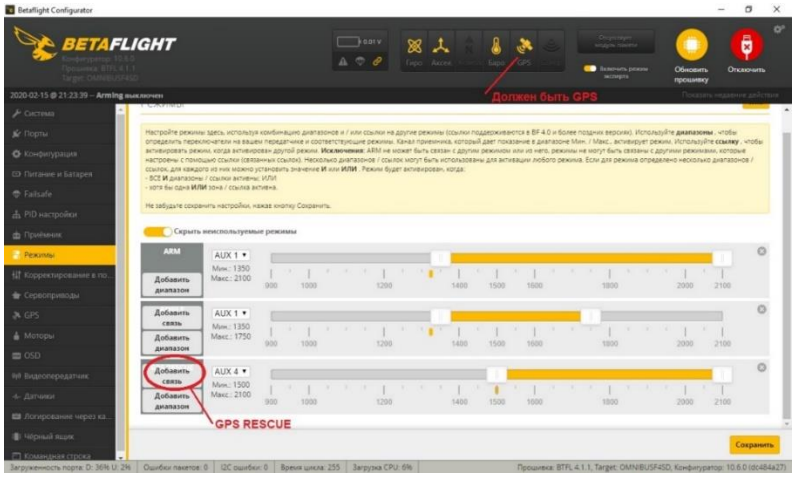

Рисунок 6 – Активизация GPS Rescue

На рис. 7 показана часть вкладки Failsafe для настроенных параметров режима GPS спасения(rescue)

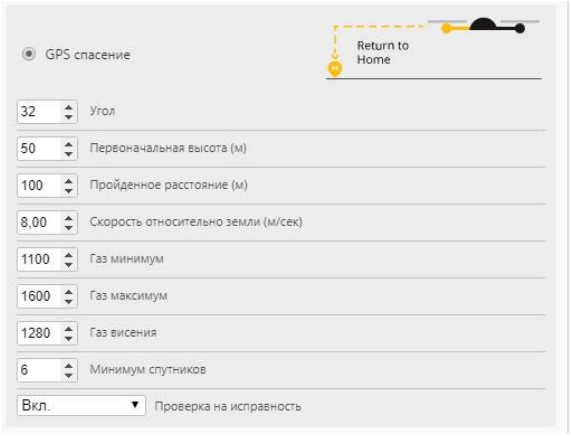

Рисунок 7 – Часть вкладки режима GPS rescue

Параметры устанавливаются во вкладке "командная строка" (cli).

set failsafe_procedure=GPS-RESCUE

Здесь устанавливается для failsafe процедура GPS Rescue.

set gps_rescue_initial_alt=[number] (default is 50)

Когда активирован, Rescue Mode - например, переключателем AUX4 на пульте управления, квадрокоптер развернется передней частью в сторону запуска и попытается подняться на безопасную высоту относительно точки взлета. Эта высота будет либо параметром, соответствующим number, либо максимальной высотой, зарегистрированной во время полета +15 м, в зависимости от того, что больше. На рис. 7 установлена высота 50 метров.

set gps_rescue_ground_speed=800 (default is 2000)

Это скорость, с которой квадрокоптер будет пытаться вернуться, в сантиметрах в секунду. Установлена скорость 8 м/с (около 30км в час - рис. 7).

set gps_rescue_angle=32 (default is 32)

Устанавливает максимально допустимый угол наклона квадрокоптера при возвращении в точку пуска. Этот параметр может помешать достижению полной скорости (8 м/с), если его значение будет слишком малым. Чем выше угол, тем сложнее для регулятора высоты сохранять стабильную высоту. Когда есть вероятность возвращения по встречному ветру, этот параметр можно увеличить до 45 градусов.

set gps_rescue_descent_dist =100 (default is 200)

Это расстояние в метрах, на котором квадрокоптер начнет снижаться от точки взлета с высоты, заданной командой set gps_rescue_initial_alt. Главное, чтобы в пределах этого расстояния не было помех для снижения (например, деревья, возвышенности, здания).

set gps_rescue_min_dth = <meters> (default is 100)

Команда устанавливает минимальное расстояние в метрах от точки взлета, начиная с которого будет работать режим GPS Rescue. Если активизировать режим ближе чем это расстояние, коптер упадет. Значение меньше 100 метров ставить не рекомендуется, так как ближе 100 метров прошивка может не сработать.

set gps_rescue_ascend_rate = 300 (default is 500) (добавлено в betaflight 4.1)

Здесь устанавливается вертикальная скорость, с которой будет подниматься квадрокоптер при возврате в точку пуска, выраженная в сантиметрах за секунду (установлена 3 м/с).

set gps_rescue_descend_rate = 150 (default is 150) (добавлено в betaflight 4.1)

Это вертикальная скорость, с которой квадрокоптер будет опускаться в точку старта, начиная с расстояния по команде gps_rescue_descent_dist выраженная в сантиметрах за секунду.

Установка параметров дроссельной заслонки выполняется по командам

set gps_rescue_throttle_min=1100 и set gps_rescue_throttle_max=1600

Они относятся к версиям betaflight более старым чем 4.1. Например, первый параметр определял скорость вращения моторов при посадке, а второй - при максимальной скорости подъема и возврата в точку пуска. В версии 4.1 и более новых - это диапазон скоростей вращения моторов, который не превышается в режиме GPS Rescue, так как скорости подъема и посадки режима GPS Rescue заданы предыдущими параметрами. Однако разработчики рекомендуют и для этих параметров выполнять тестирование для вновь собранного коптера.

gps_rescue_alt_mode = [MAX_ALT, FIXED_ALT, CURRENT_ALT] (added in betaflight 4.1)

Эта команда с перечисленными параметрами позволяют установить высоту полета коптера в режиме GPS Rescue.

MAX_ALT - для этого параметра высота возврата будет соответствовать высоте, установленной командой set gps_rescue_initial_alt=50 (50м), либо максимальной высотой, зарегистрированной во время полета +15 м, в зависимости от того, что больше.

FIXED_ALT - здесь квадрокоптер будет возвращаться к точке взлета на высоте, установленной командой gps_rescue_initial_alt=50 (50м).

CURRENT_ALT - квадрокоптер будет возвращаться на высоте, которая была установлена во время активации режима спасения (GPS Rescue).

Для работы режима GPS Rescue необходимо установить минимальное количество спутников, с которыми должен установить связь приемник GPS:

set gps_rescue_min_sats=6 (default is 8)

С целью проверки работоспособности режима GPS Rescue, надежности его срабатывания, для построенного квадрокоптера с прошивкой версии 4.1.1. была выполнена последовательность процедур, представленных ниже.

Выполнен пролет на квадрокоптере на расстояние больше чем 100 метров от дистанции, которая указана в команде set gps_rescue_min_dth =100. Здесь начало срабатывания режима GPS спасения указано на расстоянии 100 м от точки старта. Поэтому пролетаем на расстояние примерно 150м. При полете по прямой линии стрелка home должна указывать в направлении точки пуска. На коптере предварительно настраивается OSD [8]. Если стрелка указывает другое направление, режим GPS Rescue не активизируется, например, тумблером с пульта управления. После активизации GPS Rescue при правильной настройке коптер будет лететь в направлении стрелки. При подлете к точке старта и начале снижения с целью исключения падения коптера деактивизировался режим GPS Rescue выключателем на тумблере. Управление переходило в ручной режим, в котором производилась посадка квадрокоптера. При подлете часто коптеру трудно удержать стабильную высоту в случае, если показания высоты по GPS нестабильны, а контроллер коптера движет его к заданной цели - высоте. Однако в случае стабильной высоте по GPS, если коптер не стабилизируется по высоте в пределах десяти метров, проводилось регулирование параметров PID регулятора для дроссельной заслонки:

gps_rescue_throttle_P; gps_rescue_throttle_I; gps_rescue_throttle_D

Или параметров PID регулятора по приросту скорости навигации (версия 4.1.1):

gps_rescue_velocity_P = 80; gps_rescue_velocity_I = 20; gps_rescue_velocity_D = 15

Команда set failsafe_procedure = GPS-RESCUE (указанная ранее) активизирует режим GPS Rescue в случае потери связи с аппаратурой управления. В случае возвращения радиосвязи управление коптером будет возвращено пульту управления. Однако это не всегда удобно, так как коптер в этом случае может находиться за пределами видимости или видеосвязи. Поэтому дальнейший маршрут его полета может быть не определен. В случае обрыва связи при испытаниях на пульте управления тумблером включался режим GPS Rescue

и в этом случае после установления радиосвязи с пультом коптер будет продолжал следовать к месту старта. После появления видеосвязи (полет по FPV) или визуального обнаружения коптера, тумблером выполнялось выключение режима GPS Rescue с последующей посадкой или продолжением полета (по курсовой камере) в ручном режиме.

При использовании GPS rescue была использована команда включения проверки работоспособности этого режима:

set gps_rescue_sanity_checks = RESCUE_SANITY_ON

Эта проверка гарантирует что имеет место:

- постоянное подключение GPS приемника к полетному контроллеру
- GPS-приемник отправляет действительное значение GPS Fix на полетный контроллер
- квадрокоптер не испытал сильных вибраций (например, удар о препятствие)
- количество спутников, с которыми установлена связь, равно или более gps_min_sats
- квадрокоптер приближается к точке взлета после достижения заданной высоты в режиме GPS Rescue

Если любое из этих условий не выполнилось, происходит отключение моторов (disarming). Последние два условия имеют небольшую задержку перед срабатыванием.

При запуске коптера учитывалось следующее. Arming коптера невозможен без GPS Fix, если настроен режим GPS Rescue (даже если он находится в выключенном состоянии на пульте управления). Для полета без GPS Fix в зоне с плохим покрытием спутниками выполняется деактивация режима GPS Rescue с помощью команды:

set gps_rescue_allow_arming_without_fix = ON

GPS Rescue будет недоступен во время полета и на экранном меню появится предупреждение (RESCUE OFF), при работе OSD. Если во время полета получено надлежащее количество спутников, для включения GPS Rescue выполняется приземление, процедуры disarming и arming.

Выводы

1. В процессе летных испытаний показано, что режим GPS Rescue позволяет вернуть БПЛА в зону запуска при условии соблюдения вышеописанных настроек на представленном в работе квадрокоптере.

2. Установлено, что при выполнении режима GPS Rescue важным условием является стабильная связь GPS приемника с количеством спутников не меньшим установленных в параметре gps_min_sats. Если количество спутников во время выполнения режима GPS Rescue становиться меньше установленного, то в течении нескольких секунд моторы выключаются и коптер упадет. Это режим целесообразно использовать в безоблачную погоду.

3. Для устойчивой работы режима GPS Rescue коптер при полете должен использовать режим стабилизации(Angle) с включенным акселерометром, выполнять полет с небольшими углами наклона. Установлено, что чем больше угол наклона копрера, тем меньшее число спутником ловит GPS приемник. Поэтому режим GPS Rescue не целесообразно использовать в режимах полета Acro, 3D, Horizon при совершении flip-ов.

4. При полете на дальние расстояния(4-8км) на небольшом коптере необходимо убедиться, что стрелка в OSD показывает на направление старта. В противном случае режим GPS Rescue не сработает.

5. Практически установлено, что режим GPS Rescue более целесообразно использовать в случае обрыва видео связи с курсовой камерой (FPV полеты) при сохранении связи с пультом управления. В этом случае теряется ориентация полета и коптер в автоматическом режиме необходимо вернуть в зону видеосвязи. Для этого на пульте управления устанавливается режим стабилизации (angle) и включается режим GPS Rescue. При установлении видеосвязи, определении местоположения, режим GPS Rescue отключается с пульта и коптер может продолжать полет по FPV.

6. При нарушении связи с пультом управления автоматически включается режим GPS Rescue. Коптер возвращается в точку старта и в случае восстановления радиосвязи коптер

автоматически восстанавливает управление с пультом. Этот момент должен быть отслежен пилотом, в противном случае коптер может потерпеть аварию. Обычно в случае потери связи тумблер на пульте устанавливается в режим GPS Rescue и коптер автоматически возвращается в точку старта и может быть обнаружен визуально с последующим управлением с пульта.

7. Режим GPS Rescue применяется в FPV полетах с обязательной настройкой OSD. Для этого требуются полетные контроллеры с встроенной микросхемой OSD, которые поддерживаются программным обеспечением Betaflight.

ЛИТЕРАТУРА:

1.First Person View (FPV). [Electronic resource]. – 2019. – Mode of access: https://ru.wikipedia.org/wiki/First_Person_View_(FPV)

2.Maintenance Release Betaflight 4.1. [Electronic resource]. – 2019. – Mode of access: https://github.com/betaflight/betaflight/releases

3.Betaflight Configurator 10.6.0. [Electronic resource]. – 2019. – Mode of access: https://github.com/betaflight/betaflight-configurator/releases/tag/10.6.0

4. Мясищев А.А. Построение БПЛА на базе полетного контроллера АРМ 2.6. / ВІСНИК ХНУ. Технічні науки.-Хмельницький: ХНУ, 2016. №5. С. 225-230.

5. Мясищев А.А. ВОЗМОЖНОСТИ ПОЛЕТНОГО КОНТРОЛЛЕРА CC3D С ПРОШИВКОЙ INAV. / ВІСНИК ХНУ. Технічні науки.-Хмельницький: ХНУ, 2019. №1. С. 129-136.

6. INAV [Electronic resource]. – 2018. – Mode of access: https://github.com/iNavFlight/inav/wiki

7. OMNIBUS F4V3. [Electronic resource]. – 2017. – Mode of access: http://nic.vajn.icu/PDF/radio-controlled/OMNIBUS_F4_V3.pdf

8. BETAFLIGHT OSD SETUP. [Electronic resource]. – 2017. – Mode of access: https://oscarliang.com/betaflight-osd/

9. GPS Rescue Mode. [Electronic resource]. – 2020. – Mode of access: https://github.com/betaflight/betaflight/wiki/GPS-rescue-mode#arm-without-a-gps-fix

10. HOW TO SETUP GPS RESCUE MODE IN BETAFLIGHT. [Electronic resource]. – 2018. – Mode of access: https://oscarliang.com/setup-gps-rescue-mode-betaflight/

11. GPS-Rescue. Как это работает? BF 3.2.5. [Electronic resource]. – 2019. – Mode of access: https://www.youtube.com/watch?v=dsKz01WPppk&t=74s

12.Константинов Э. Betaflight, тесты режима GPS Rescue, Failsafe. [Electronic resource]. – 2019. – Mode of access: https://www.youtube.com/watch?v=PwAaC4EtI64

13. Betaflight GPS Rescue mode - what happens at the end? [Electronic resource]. – 2019. – Mode of access: https://www.youtube.com/watch?v=AZ5UDh7U7QU&t=28s

14. MICRO FPV BETAFLIGHT GPS RESCUE. Electronic resource]. – 2019. – Mode of access: https://www.youtube.com/watch?v=2lePVoK0t1c

15. Мясищев А.А. Использование платы ROBOTDYN MEGA2560 PRO для построения полетного контроллера гексакоптера / А.А. Мясищев // Вісник хмельницького національного університету. Технічні науки. – Хмельницький: ХНУ, 2018. – № 3. – С. 171–179.

REFERENCES:

1.First Person View (FPV). [Electronic resource]. – 2019. – Mode of access: https://ru.wikipedia.org/wiki/First_Person_View_(FPV)

2.Maintenance Release Betaflight 4.1. [Electronic resource]. – 2019. – Mode of access: https://github.com/betaflight/betaflight/releases

3.Betaflight Configurator 10.6.0. [Electronic resource]. – 2019. – Mode of access: https://github.com/betaflight/betaflight-configurator/releases/tag/10.6.0

4. Myasishev A.A. Postroenie BPLA na baze poletnogo kontrollera APM 2.6. / VISNIK HNU. Tehnichni nauki.-Hmelnickij: HNU, 2016. - №5.-s. 225-230.

5. Myasishev A.A. VOZMOZHNOSTI POLETNOGO KONTROLLERA CC3D S PROSHIVKOJ INAV. / VISNIK HNU. Tehnichni nauki. -Hmelnickij: HNU, 2019. - №1.-s. 129-136.

6.INAV [Electronic resource]. – 2018. – Mode of access : https://github.com/iNavFlight/inav/wiki

7.OMNIBUS F4V3. [Electronic resource]. – 2017. – Mode of access : http://nic.vajn.icu/PDF/radio-controlled/OMNIBUS_F4_V3.pdf

8.BETAFLIGHT OSD SETUP. [Electronic resource]. – 2017. – Mode of access: https://oscarliang.com/betaflight-osd/

9.GPS Rescue Mode. [Electronic resource]. – 2020. – Mode of access: https://github.com/betaflight/betaflight/wiki/GPS-rescue-mode#arm-without-a-gps-fix

10.HOW TO SETUP GPS RESCUE MODE IN BETAFLIGHT. [Electronic resource]. – 2018. – Mode of access: https://oscarliang.com/setup-gps-rescue-mode-betaflight/

11. GPS-Rescue. Kak eto rabotaet? BF 3.2.5. [Electronic resource]. – 2019. – Mode of access: https://www.youtube.com/watch?v=dsKz01WPppk&t=74s

12.Konstantinov E. Betaflight, testy rezhima GPS Rescue, Failsafe. [Electronic resource]. – 2019. – Mode of access: https://www.youtube.com/watch?v=PwAaC4EtI64

13.Betaflight GPS Rescue mode - what happens at the end? [Electronic resource]. – 2019. – Mode of access: https://www.youtube.com/watch?v=AZ5UDh7U7QU&t=28s

14.MICRO FPV BETAFLIGHT GPS RESCUE. Electronic resource]. – 2019. – Mode of access: https://www.youtube.com/watch?v=2lePVoK0t1c

15. Myasishev A.A. Ispolzovanie platy ROBOTDYN MEGA2560 PRO dlya postroeniya poletnogo kontrollera geksakoptera / A.A. Myasishev // Visnik hmelnickogo nacionalnogo universitetu. Tehnichni nauki. – Hmelnickij : HNU, 2018. – № 3. – S. 171–179.

д.т.н., проф. Мясіщев О.А., д.т.н., проф. Лєнков С.В.,
д.т.н., с.н.с. Комарова Л.О., к.т.н. Лєнков Є.С.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ РЕЖИМУ RESCUE У ПРОШИВЦІ BETAFLIGHT ДЛЯ БПЛА НА БАЗІ КОНТРОЛЛЕРА STM32F405

У роботі розглядається практична можливість реалізації режиму GPS Rescue для прошивки Betaflight ver.4.1.1 з метою повернення квадрокоптера (БПЛА) в точку, близькою за координатами точки зльоту. У зв'язку з цим був побудований експериментальний зразок з рамою 250мм, але якої встановлено польотний контролер OMNIBUSF4V3 на базі мікроконтролера STM32F405 з GPS приймачем і курсової відеокамерою для забезпечення польотів по FTP. Для отримання польотних даних з метою аналізу правильності роботи алгоритму повернення коптера був налаштований Betaflight OSD. В процесі льотних випробувань показано, що режим GPS Rescue дозволяє повернути БПЛА в зону запуску за умови дотримання представлених в роботі налаштувань на зібраному квадрокоптера. При виконанні режиму GPS Rescue важливою умовою є стабільна зв'язок GPS приймача з кількістю супутників такою ж встановлених під час налаштування прошивки. Якщо кількість супутників ставати менше встановленого, то протягом декількох секунд мотори вимикаються і коптер падає.

Показано, що для стійкої роботи режиму GPS Rescue коптер при польоті повинен використовувати режим стабілізації (Angle) з включеним акселерометром, виконувати політ з невеликими кутами нахилу. Встановлено, що чим більше кут нахилу копрера, тим менше число супутником ловить GPS приймач. Тому режим GPS rescue недоцільно використовувати в режимах польоту Acro, 3D, Horizon при здійсненні flip-ів.

Практично встановлено, що режим GPS Rescue більш доцільно використовувати в разі обриву відео зв'язку з курсовою камерою (FPV польоти) при збереженні зв'язку з пультом управління. В цьому випадку втрачається орієнтація польоту і коптер в автоматичному режимі необхідно повернути в зону відеозв'язку. Для цього на пульті управління встановлюється режим стабілізації (angle) і включається режим GPS Rescue. При встановленні відеозв'язку, визначенні місця розташування режим GPS Rescue відключається з пульта і коптер може продовжувати політ по FPV.

Було відмічено, що при порушенні зв'язку з пультом управління автоматично включається режим GPS Rescue. При цьому коптер повертається в точку старту і в разі відновлення радіозв'язку коптер автоматично відновлює управління з пультом. Цей момент повинен бути відстежено пілотом, в іншому випадку коптер може потерпіти аварію. Тому доцільно в разі втрати зв'язку тумблер на пульті управління встановити в режим GPS Rescue. Тоді коптер при відновленні радіозв'язку спрацює по режиму GPS Rescue з пульта і автоматично повернеться в зону старту і може бути виявлений візуально з подальшим управлінням з пульта.

Ключові слова: OMNIBUSF4V3, OSD Betaflight, INAV, GPS приймач, FPV, STM32F405, GPS Rescue, GLONASS, NEO-6M-0-001, Beitian BN-880

Doctor of Technical Sciences Myasischev A.A., Doctor of Technical Sciences Lienkov S.V.,
Doctor of Technical Sciences Komarova L.O., Ph.D. Lienkov Ye.S.

FEATURES OF USE OF RESCUE MODE IN BETAFLIGHT FIRMWARE FOR UAV ON THE BASIS OF STM32F405 CONTROLLER

The paper considers the practical possibility of implementing the GPS Rescue mode for Betaflight ver.4.1.1 firmware in order to return the quadrocopter (UAV) to a point close to the take-off point coordinates. In this regard, an experimental prototype was built with a 250mm frame, but with which the OMNIBUSF4V3 flight controller was installed based on the STM32F405 microcontroller with a GPS receiver and a directional video camera for FTP flights. Betaflight OSD was configured to receive flight data in order to analyze the correct operation of the copter return algorithm. During flight tests, it was shown that the GPS Rescue mode allows you to return the UAV to the launch zone, subject to the settings presented in the work on the assembled quadcopter. When performing GPS Rescue mode, an important condition is the stable connection of the GPS receiver with the number of satellites not less than those installed when setting the firmware. If the number of satellites becomes less than the set, then within a few seconds the motors turn off and the copter falls.

It is shown that for stable operation of the GPS Rescue mode, the copter during flight should use the stabilization mode (Angle) with the accelerometer turned on, perform a flight with small angles of inclination. It was found that the greater the angle of inclination of the coprera, the smaller the number of satellites the GPS receiver catches. Therefore, the GPS rescue mode is not advisable to use in Acro, 3D, Horizon flight modes when making flip-s.

It has been practically established that the GPS Rescue mode is more appropriate to use in the event of a break in video communication with the heading camera (FPV flights) while maintaining communication with the control panel. In this case, the flight orientation is lost and the copter in automatic mode must be returned to the video communication zone. To do this, the control mode sets the stabilization mode (angle) and turns on the GPS Rescue mode. When establishing a video connection, determining the location, GPS Rescue mode is disabled from the remote control and the copter can continue flying via FPV.

It was noticed that in case of communication failure with the control panel, GPS Rescue mode is automatically turned on. In this case, the copter returns to the starting point and in case of restoration of radio communication, the copter automatically restores control with the remote control. This moment must be monitored by the pilot, otherwise the copter may crash. Therefore, it is advisable in case of loss of communication to set the toggle switch on the control panel to GPS Rescue mode. Then, when the radio is restored, the copter will operate according to the GPS Rescue mode from the remote control and will automatically return to the start area and can be detected visually with subsequent control from the remote control.

Keywords: OMNIBUSF4V3, OSD Betaflight, INAV, GPS receiver, FPV, STM32F405, GPS Rescue, GLONASS, NEO-6M-0-001, Beitian BN-880

УДК 681.3

к.т.н., доц. **Пампуха І.В.** (ВІКНУ)
к.військ.н. **Нікіфоров М.М.** (ВІКНУ)
Комаров В.О. (ЦНДІО і ОВТ ЗСУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-03

РОЗРОБКА МЕТОДИКИ ВИЗНАЧЕННЯ ЗАПАСУ МІЦНОСТІ БОЙОВИХ ЛІТАКІВ НА ОСНОВІ АНАЛІЗУ ДИНАМІЧНИХ ХАРАКТЕРИСТИК З УРАХУВАННЯМ ЕКСПЛУАТАЦІЙНИХ ФАКТОРІВ

У статті розглядаються питання діагностики технічного стану консольно закріплених конструкцій літального апарату (ЛА) на основі аналізу їх динамічних характеристик. Виконання цього завдання передбачає визначення фактичного технічного стану пошкодженої конструкції і, як наслідок, запасу міцності. Основним критерієм є використання якомога меншої кількості інформації для отримання точної об'єктивної оцінки. В якості діагностичних ознак пропонується використовувати динамічні характеристики конструкції, що володіють найбільшою інформативністю - частоти власних коливань (крутильні і вигинних) і положення осі жорсткості (щодо даних свідомо непошкоджених конструкцій, які приймаються за еталонні).

Зазначена методика запатентована. Як технічне рішення вона передбачає проведення частотних випробувань з порушенням вигинних і крутильних коливань, при яких для кожного типу ЛА, а саме, для його частини - крила, оперення (консольно закріплених конструкцій планера) буде встановлюватися мінімальна частота власних коливань, відповідна мінімально-допустимій залишкової міцності. Збільшення кількості аналізованих ЧСК підвищує достовірність оцінки залишкової міцності. Виходячи з цього, розроблено і виготовлено в мобільному варіанті обладнання та апаратура контролю (які також запатентовані), можуть бути ефективно використані при базуванні ЛА в польових умовах. Подібна система контролю, ґрунтуючись на положеннях НІАС, може бути впроваджена в військових частинах Повітряних Сил ЗС України при експлуатації авіаційної техніки за технічним станом.

Ключові слова: діагностика технічного стану, частота власних коливань, залишкова міцність, неруйнівний контроль, крило, силовий набір.

Вступ та аналіз останніх досліджень. В експлуатації авіаційної техніки використовуються різні системи контролю у залежності від прийнятих методів експлуатації - по ресурсу, за технічним станом і суміщений [1,2].

При експлуатації за встановленим ресурсом контроль конструкцій виконується після досягнення обмежень їх ресурсу, але разом з тим перевірки можуть проводитися вибірково там, де вони можливі та ефективні [3]. Такі початкові інтервали контролю встановлюються виробником техніки. При експлуатації за технічним станом плануються періодичні контрольно-перевірочні роботи, за результатами яких приймається рішення про подальшу експлуатацію на підставі визначення залишкової міцності. Інтервали контролю при цьому базуються на досвіді експлуатації і рекомендаціях виробників, а також на припустимості пошкоджень [4]. Повністю перевести авіаційну техніку на експлуатацію за технічним станом не вдається (тільки від 60 до 75 % агрегатів і систем сучасної авіатехніки експлуатуються за станом), тому основним методом експлуатації є суміщений метод.

Перехід на експлуатацію по технічному стану і на суміщений метод експлуатації сприяє підвищенню рівня надійності техніки завдяки впровадженню найбільш ретельного неруйнівного контролю значно більшого числа деталей об’єкта в умовах експлуатації і ремонту. Більша увага при цьому повинна приділятися визначенню стану матеріалу деталей методами дефектоскопії та неруйнівного контролю [2,5].

Порядок проведення робіт по технічному обслуговуванню і контролю визначається типом техніки і може бути різним. Однак, в програмах технічного обслуговування різних об’єктів контролю здійснюються деякі загальні принципи використання засобів дефектоскопії

та неруйнівного контролю.

Наприклад, часті перевірки передбачається виконувати візуально. Перевірки з більшою періодичністю виконують з використанням інструментальних засобів неруйнівного контролю. Найбільш часто перевіряються високонавантажені і відповідальні конструкції планера ЛА, їх деталі та вузли. При великому напрацюванні з появою втомних (експлуатаційних) тріщин і корозії передбачається збільшення кількості методів неруйнівного контролю, ретельності і частоти перевірок. Все це стосується експлуатації ЛА у мирний час.

В умовах же застосування зброї масового ураження або інтенсивних повітряних боїв існує ймовірність того, що практично весь літаковий парк бойового полку буде ушкоджений. Ушкодження літального апарата (ЛА), пов'язані з руйнуванням силових елементів конструкції, змінює (насамперед, зменшує) її міцнісні й жорсткісні властивості, несучу здатність конструкції в цілому.

Тому, задача забезпечення безпеки польотів бойових літаків за умовами міцності при наявності ушкоджень, включаючи бойові, є актуальною. Розв'язання цієї задачі припускає визначення фактичного запасу міцності ушкодженої конструкції для розробки рекомендацій на технічне обслуговування й відновлення. В умовах бойових дій ці задачі повинні вирішуватися в найкоротший термін і з мінімальними працезатратами на діагностичний контроль.

Для підтримання справності парку літаків, що мають експлуатаційні й бойові пошкодженя, і можливості їх подальшого використання при виконанні відповідних ремонтів, необхідно виконання наступних заходів:

оцінка технічного стану силової конструкції крила літака з експлуатаційними пошкодженнями й бойовими ураженнями та після їх усунення;

дослідження напружено-деформованого стану конструкції панелі крила літака з експлуатаційними пошкодженнями й бойовими ураженнями та після проведеного ремонту з метою визначення запасів міцності;

розроблення методичного апарату прогнозування технічного стану силової конструкції та визначення умов безпечної експлуатації силової конструкції літака з експлуатаційними пошкодженнями й бойовими ураженнями;

розроблення методики прогнозування технічного стану силової конструкції літака з експлуатаційними пошкодженнями й бойовими ураженнями.

Основна частина. Для забезпечення технічного обслуговування й відновлення ушкодженої авіаційної техніки (АТ) у найкоротший термін, необхідно для кожного ушкодженого ЛА визначити фактичний технічний стан (залишкову міцність) і на підставі отриманих результатів зробити висновок про можливість його подальшої експлуатації, а також вносити відповідні обмеження в його льотно-технічних характеристик [3,6].

Досвід експлуатації ЛА вказує [1,7], що більшість руйнувань силових елементів (СЕ) планера ЛА має втомний характер. Кількість таких руйнувань складає приблизно 80-90 % від загального числа руйнувань.

При створенні ЛА розробник здійснює прогноз надійності конструкції планера ЛА шляхом розрахунків при використанні результатів лабораторних випробувань СЕ та припущень щодо умов подальшої експлуатації. Аналітичні залежності в математичній моделі розробника побудовано на основі ймовірностної моделі втомної довговічності – двохпараметричного логнормального закону розподілу:

$$F(\lg N) = \frac{1}{\sigma\sqrt{2\pi}} \int_0^{\lg N} e^{-(x-\mu)/(2\sigma^2)} dx, \qquad (1)$$

де: x - втомна довговічність; μ та σ - параметри функції розподілу (μ - математичне очікування, σ - середнє квадратичне відхилення логарифмів довговічностей, при цьому приймається, що $\sigma = 0{,}15$ для алюмінієвих сплавів).

Під руйнуванням конструкції розглядається всяке порушення цілісності СЕ конструкції, при якому поряд із загальними типами руйнування деталей чи агрегатів ЛА до руйнування відноситься також локальні місцеві руйнування: місцевий порив обшивки, зрив та зріз заклепок на значних ділянках крила, оперення чи фюзеляжу, зріз болтів кріплення та інше, включаючи бойові ураження, що призводить до зниження міцності конструкції в цілому.

Рівень міцності, що залишився після появи пошкоджень в силових елементах конструкції $n_{ур}^{Р}$ можна оцінювати відношенням перевантажень, при яких руйнуються ураженні частини високонавантажених конструктивних елементів планера до величини $n^{Đ}$.

$$\overline{n}_{óð}^{ð} = \frac{n_{óð}^{ð}}{n^{ð}} \quad . \tag{2}$$

ЛА може виконати політ на бойове завдання і повернутися на свій аеродром, якщо в результаті наявності експлуатаційного пошкодження чи бойового ураження буде виконуватись умова $n_{óð}^{Đ} = \overline{n}_{óð}^{ð} \cdot n_{ð} \geq n_{áç}$, де $n_{бз}$ – максимальне перевантаження, яке необхідно витримати ЛА.

При експлуатації парку старіючих ЛА виникає науково-технічна проблема підтримання справності та забезпечення довговічності силових елементів (СЕ) планерів ЛА, вирішення якої полягає в пошуку оптимального поєднання методів оцінки ступеню пошкодженості (залишкової міцності) та заходів щодо відновлення технічного стану СЕ.

Оперативність діагностування може бути досягнута шляхом використання методу неруйнівного контролю (МНК), заснованого на зміні частот власних вигинних і крутильних коливань при появі в силових елементах експлуатаційних пошкоджень чи пошкодженні конструкції засобами ураження (щодо свідомо неушкодженої конструкції – еталонні частоти). Прогнозуючими параметрам, що вірогідно відбивають динамічну індивідуальність конструкції, обрані частоти власних коливань (ЧВК). Частоти власних коливань здатні нести максимум необхідної діагностичної інформації.

Суть методу контролю ЧВК полягає в тому, що для кожної конструкції, що характеризується своєю індивідуальністю, періодично заміряються частоти власних коливань – вигинних і крутильних форм. Заміряні частоти рівняються з еталонними, заміряними на свідомо неушкодженій конструкції, переважно на конструкції, яка виходить зі складального цеху [8].

Застосовуваний для частотних випробувань (для діагностики конструкції) метод контролю ЧВК, заснований на застосуванні фізичних коливань із власною частотою, які збуджуються або виникають в об'єкті контролю (крилі або інших консольно закріплених конструкціях планера ЛА), і класифікується по ГОСТ 23829-85, 15467-79 і по керівному документу РД 25.002-80 як резонансний МНК. Резонансний МНК заснований на порушенні авторезонансних пружних коливань в об'єкті контролю або його частини й аналізі параметрів коливань динамічної системи. При застосуванні резонансного МНК реєструються такі параметри авторезонансних коливань, як частота власних (авторезонансних) коливань і амплітуда коливань.

Випробувальне устаткування, що застосовується при цьому методі, повинно забезпечувати:

- стабільність підтримки частоти власних коливань і задану точність випробувань;

- виключити вплив повторних експлуатаційних факторів, що знижують чутливість устаткування;

- можливість ручного й автоматичного керування процесом випробувань;

- можливість оперативного (негайного) одержання інформації під час проведення частотних випробувань;

- можливість багаторазового використання й повторення.

У процесі експлуатації ЛА контролюється зниження частот власних коливань конструкцій. Якщо зниження частот відбувається плавно, то це говорить про деяке старіння конструкції – про появу люфтів у заклепувальних з'єднаннях, корозії на силових елементах, мікротріщин тощо.

На рис. 1 показано зміну частоти консольно закріпленої конструкції літака – крила, залежно від числа польотів (об'єкт контролю до випробувань наробітку не мав, за еталонну частоту fe вигинних коливань прийнята частота f =9,8 Гц).

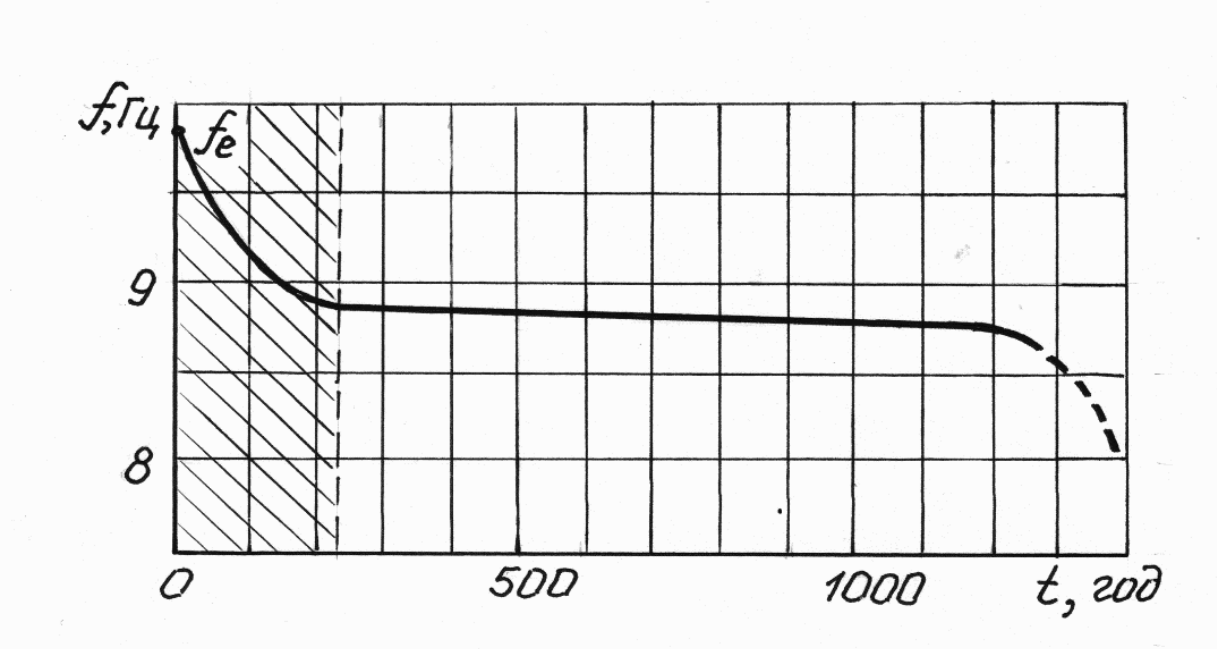

Рисунок 1 – Характер зміни частоти власних коливань консольно закріпленої конструкції літака – крила, залежно від числа польотів (нальоту літака)

Із графіка видно, що в початковій стадії діагностичного контролю спостерігалося помітне (до 1%) зниження частоти власних коливань, пов'язане із приробляннням конструктивних елементів крила, потім частота стабілізувалася. При наробітку від 700 до 1000 годин нальоту (міжремонтний ресурс) пошкоджень у силовому наборі крила не виникало й частота власних коливань за першою формою коливань практично не змінювалася.

При подальшій експлуатації намітилася тенденція до зниження ЧВК. Як видно із графіка, за відносно короткий час ЧВК крила зменшилася не менш, ніж на 2-3 %. Цей період збігається з моментом виникнення й розвитку втомленої тріщини 1 на верхній панелі 2 крила (наприклад, літака Су-25) у районі бортової нервюри 3, що була виявлена візуальним методом (рис. 2).

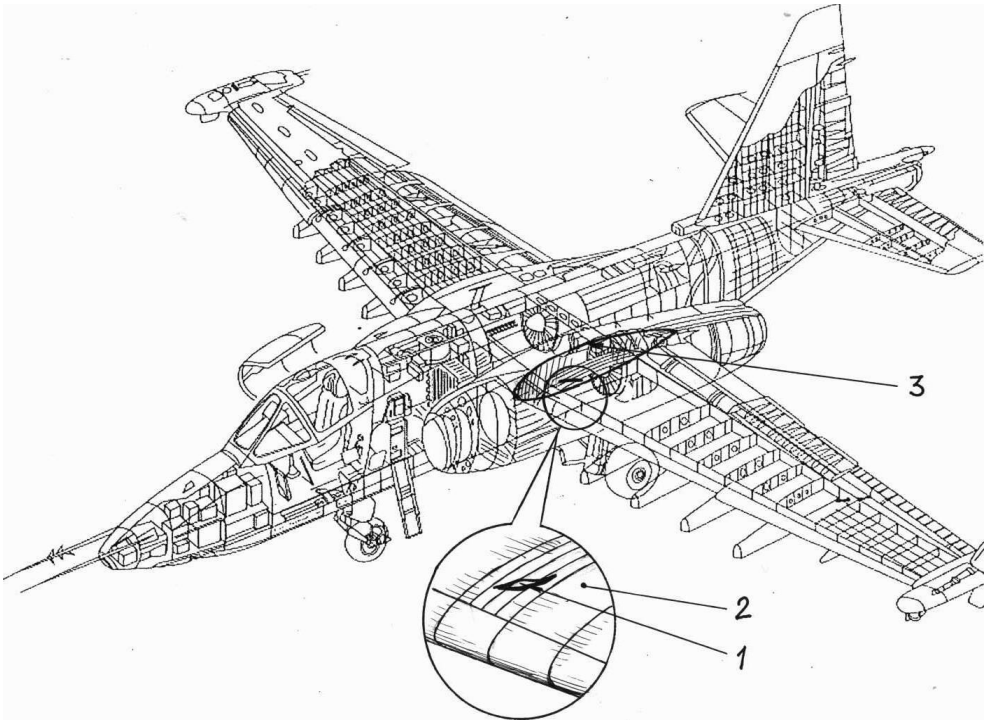

Рисунок 2 – Схема розміщення тріщини на верхній панелі крила літака типу Су-25

Загальний ефект від використання НМК при технічному обслуговуванні авіаційної техніки (АТ) складається з переваг, отриманих в основному в результаті скорочення часу простою АТ при виконанні на ній регламентних робіт, пов’язаних з повним або частковим розбиранням для пошуку дефектів і несправностей, і одержання більш об’єктивних відомостей про технічний стан конструкції.

Зазвичай, профілактичний контроль пов'язаний з повним або частковим розбиранням АТ для доступу до систем і агрегатів, що цікавлять, на предмет появи ушкоджень у силових елементах конструкції. Це суттєво підвищує вартість контролю, збільшує трудовитрати. Профілактичні контрольні операції на новій АТ призначаються, як правило, у великому об’ємі й більш частіше, ніж це дійсно необхідно, із залученням великого числа обслуговуючого персоналу. Забезпечення надійності таким шляхом стає усе більш затратним [9].

На іншому ЛА (літак типу МіГ-29) за допомогою методу ЧВК із збудженням вигинних коливань крила була виявлена тріщина 4 у полиці 5 переднього лонжерона 6 (за фактом різкої зміни частоти власних коливань), а при порушенні крутильних коливань крила було виявлене ушкодження у вигляді поздовжньої тріщини 7 на стінці 8 заднього лонжерона 9 (див., відповідно, схему на рис. 3).

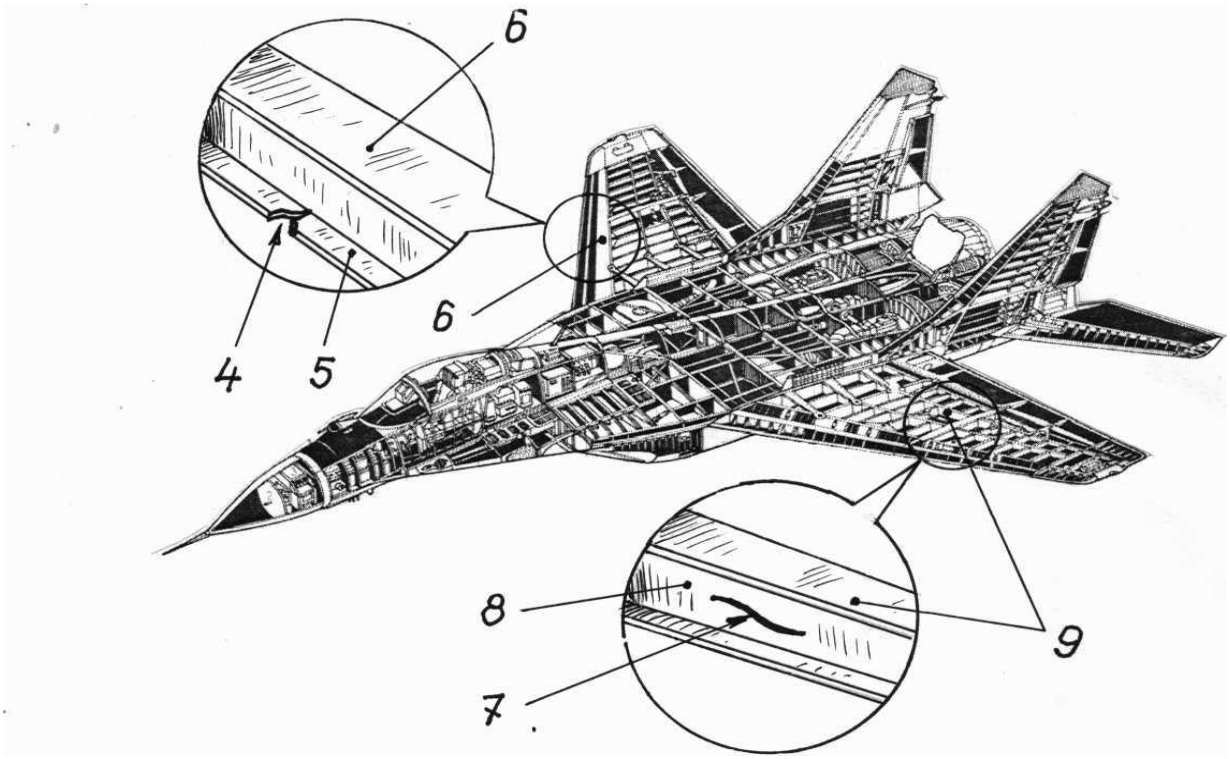

Рисунок 3 – Схема розміщення тріщин у конструктивних елементах лонжеронів крила літака типу МіГ-29

Це говорить про те, що за різким зниженням частоти власних коливань можна з достатньою точністю говорити про появу ушкодження в силовому наборі крила літака, що особливо важливо, якщо ці ушкодження невидимі (знаходяться під обшивкою) при зовнішньому огляді конструкції – крила.

У таблиці 1 показані порівняльні характеристики трудовитрат існуючих МНК і перспективного МНК (методу контролю ЧВК), заснованого на контролі динамічних властивостей конструкції за допомогою обладнання [10,11], що встановлюється на закінцівках консолей крила літака (рис. 4).

Таблиця 1

Порівняльні характеристики трудовитрат існуючих МНК і перспективного МНК (методу контролю ЧВК)

Об’єкт контролю	Мета контролю	Трудовитрати, людино/год		
		Візуальний	Рентгенографія	Метод ЧВК
Стерно висоти	Стан обшивки і силового набору,	80	14	2-3
Стерно повороту		15	4	2-3
Закрилки		75	15	до 2
Елерон		20	7	до 2
Крило	Наявність пошкоджень	90	12	до 2

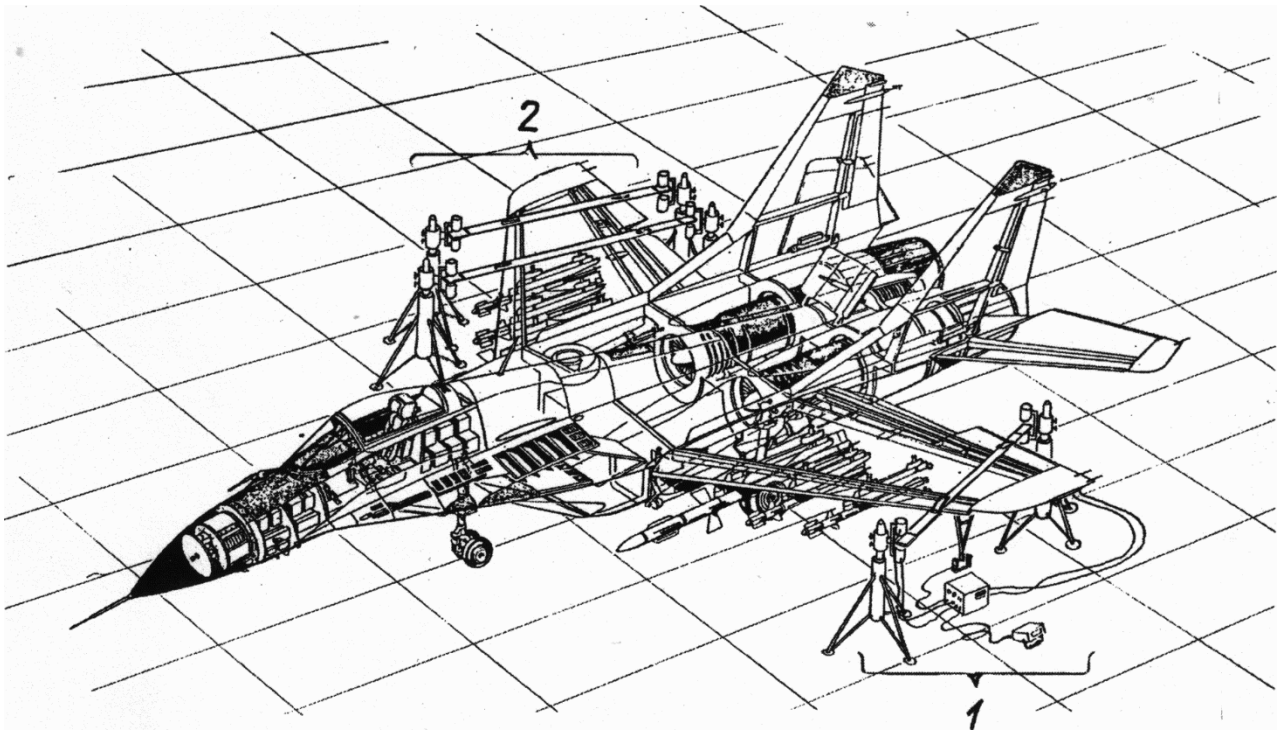

Рисунок 4 – Схема розміщення обладнання, призначеного для збудження в комплексі вигинних і крутильних форм коливань з власною частотою, на крилі літака типу МіГ-29

З табл. 1 видно, що метод контролю ЧВК, забезпечуючи одержання об’єктивної інформації про стан закритих під обшивкою елементів конструкції (лонжеронів, стрингерів, нервюр), при значному виграшу в часі, що витрачається на контроль, дає значний економічний ефект при використанні порівняно дешевої контрольно-записуючої та діагностичної апаратури (зразок конструктивного виконання якої показано на рис. 4), де, відповідно, на лівій консолі крила літака (типу МіГ-29) показано схему закріплення обладнання 1 для збудження у комплексі вигинних і крутильних коливань по першому тону коливань, а на правій консолі – обладнання 2 для багатоточечного збудження зазначених форм коливань.

Апаратуру для контролю ЧВК можуть обслуговувати два-три фахівці, що мають середній рівень підготовки. Для двох інших, зазначених вище методів, необхідно мати висококваліфікований обслуговуючий персонал з великим досвідом експлуатації.

Час на отримання цієї інформації склав не більше 20 хвилин з урахуванням часу встановлення спеціального обладнання. У загальний час проведення випробувань входить час на: - підготовку об'єкта випробувань, - установку на контрольований об'єкт (крило) випробувального устаткування і монтаж допоміжного обладнання, - настройку на режим, - контроль визначальних параметрів, - проведення випробувань, - демонтаж допоміжного обладнання та апаратури контролю, - аналіз результатів і постановка діагнозу [12].

Висновки. Сучасні системи неруйнівного контролю авіаційних конструкцій передбачають із збільшенням напрацювання та вірогідності виникнення втомних тріщин і корозії зменшення міжконтрольних інтервалів. Для реалізації цих принципів визначення періодичності контролю необхідно знати вірогідність появи дефектів в критичних деталях у різні часові проміжки експлуатації ЛА і швидкість розвитку дефектів в силових елементах високонавантажених конструкцій, якими є крило та хвостове оперення. Так, коли дефект виявляється у великій кількості екземплярів об'єктів контролю при значному напрацюванні, то необхідно суттєво змінити принципи та періодичність контролю.

Застосування методу контролю ЧВК при визначенні технічного стану пошкоджених конструкцій ЛА, дозволяє об'єктивно підходити до вирішення питання вибору методів їх

відновлення і скорочення часу нормативної тривалості ремонту. При цьому необхідно враховувати працевитрати і час на різні види ремонту, розрахункових моделей, які є вихідними даними для розрахунку моделей методів ремонту.

На підставі вищевикладеного можна зробити висновки, що незначні за величиною зміни ЧВК за часом наробітку конструкції слід уважати старінням конструкції й пов'язані із цим зміни динамічних характеристик консольно закріплених конструкцій таких, як крило, стабілізатор, кіль. Стрибкоподібна ж зміна ЧВК вказує про появу тріщини в силовому наборі крила, яка в більшому або меншому ступені впливає на зміну ЧВК вигинної або крутильної форм коливань.

ЛІТЕРАТУРА:

1. Бурлаков В.І., Лєнков С.В., Салімов Р.М. Основи теорії надійності повітряних суден та авіаційних двигунів: Навч. посіб. – К.: НАУ, 2004. – 172с.

2. Forecasting reliability of complex technology objects. Parameters optimization of their technical exploitation: [monography] in English / Sergey Lenkov, Igor Tolok, Vadim Tsitsarev, Genadiy Zhyrov, Evgen Lenkov, Yurii Khlaponin, Bohdan Borowik; under edition S.V. Lenkov. – Poland, Bielsko-Biala: Publishing house «BEL », 2018. – 253 p.

3. Ямпольский В.И., Белоконь Н.И., Пилопосян Б.Н. Контроль и диагностирование гражданской авиационной техники. М.: Транспорт, 1990. – 184 с.

4. Лєнков С.В., Толок І.В., Лєнков Є.С., Банзак Г.В., Жиров Г.Б., Цицарєв В.М. Імітаційна статистична модель процесу технічного обслуговування і ремонту складної військової техніки. Частина 1. / Монографія на укр.м. – Одеса: изд. Бондаренко М.О., 2019. – 132 с.

5. Стрельников В.П., Федухин А.В. Оценка и прогнозирование надежности электронных элементов и систем. – К.: Логос, 2002. – 486 с.

6. Положение о комплексной системе диагностирования изделий авиационной техники с применением обмена информацией между эксплуатацией и ремонтом. М.: МГА, 1989. – 121 с.

7. Барзилович Е.Ю., Савенков М.В. Статистические методы анализа состояния авиационной техники. М.: Транспорт, 1996. – 364 с.

8. Комаров, В. О. Про використання методу контролю частоти власних коливань при виборі методу відновлення авіаційної техніки [Текст] / В. О. Комаров, О. О. Растригін // Проблеми координації військово-технічної та оборонно промислової політики в Україні. Перспективи розвитку озброєння та військової техніки : тези доповідей на VII науково-практичній конференції / Міністерство оборони України. Міністерство освіти і науки України. Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України. – Київ, 2019. – С. 350-352.

9. Садых Г.С. Показатель остаточного ресурса и его свойства. Известия АН СССР, Техническая кибернетика. 1995, № 4, с. 98-102.

10.Пат. 127849 Україна, МПК (2018.01) B 64 C 3/00, G 01 M 7/00, G 01 B 11/26. Пристрій для визначення просторово-частотних характеристик коливань консольно закріплених елементів літальних апаратів при їхніх випробуваннях на утомлену міцність [Текст] / Комаров В. О. ; заявники і патентовласники Комаров В. О., Расстригін О. О. – № u 2018 02126 ; заявл. 01.03.18 ; опубл. 27.08.18, Бюл. № 16. – 4 с. : іл..

11.Пат. 109226 Україна, МПК (2016) G 01 M 5/00, G 01 N 3/00. Спосіб визначення характеристик жорсткості крила літака неруйнівним методом в умовах експлуатації та ведення бойових дій [Текст] / Комаров В.О.; заявники і патентовласники Комаров В. О., Ткаченко В. А., Галушка В. І. – № u 2016 02602 ; заявл. 16.03.16 ; опубл. 10.08.16, Бюл. № 15. – 6 с. : іл..

12.Барзилович Е.Ю., Мезенцев В.Г., Савенков М.В. Надежность авиационных систем. М.: Транспорт, 1982. – 175 с.

REFERENCES:

1. Burlakov V.I., Ljenkov S.V. and Salimov R.M. (2004). Osnovy teorii' nadijnosti povitrjanyh suden ta aviacijnyh dvyguniv. Kyi'v: NAU, 172p.

2. Forecasting reliability of complex technology objects. Parameters optimization of their technical exploitation: [monography] in English / Sergey Lenkov, Igor Tolok, Vadim Tsitsarev, Genadiy Zhyrov, Evgen Lenkov, Yurii Khlaponin, Bohdan Borowik; under edition S.V. Lenkov. Poland, Bielsko-Biala: Publishing house «BEL », 2018. 253 p.

3. Jampol'skij V.I., Belokon' N.I. and Piloposjan B.N. (1990). Kontrol' i diagnostirovanie grazhdanskoj aviacionnoj tehniki. Moscow: Transport, 181 p.

4. Ljenkov S.V., Tolok I.V., Ljenkov Je.S., Banzak G.V., Zhyrov G.B. and Cycarjev V.M. (2019). Imitacijna statystychna model' procesu tehnichnogo obslugovuvannja i remontu skladnoi' vijs'kovoi' tehniky. Chastyna 1. / Monografija na ukr.m. – Odesa: yzd. Bondarenko M.O., 132 p.

5. Strel'nikov V.P. and Feduhin A.V. (2002). Ocenka i prognozirovanie nadezhnosti jelektronnyh jelementov i sistem. Kyi'v: Logos, 486 p.

6. Polozhenie o kompleksnoj sisteme diagnostirovanija izdelij aviacionnoj tehniki s primeneniem obmena informaciej mezhdu jekspluataciej i remontom. Moscow: MGA, 1989, 121 p.

7. Barzilovich E.Ju. and Savenkov M.V. (1996). Statisticheskie metody analiza sostojanija aviacionnoj tehniki. Moscow: Transport, 365 p.

8. Komarov, V.O. (2019). Pro vykorystannja metodu kontrolju chastoty vlasnyh kolyvan' pry vybori metodu vidnovlennja aviacijnoi' tehniky Problemy koordynacii' vijs'kovo-tehnichnoi' ta oboronno promyslovoi' polityky v Ukrai'ni. Perspektyvy rozvytku ozbrojennja ta vijs'kovoi' tehniky : tezy dopovidej na VII naukovo-praktychnij konferencii' / Ministerstvo oborony Ukrai'ny. Ministerstvo osvity i nauky Ukrai'ny. Central'nyj naukovo-doslidnyj instytut ozbrojennja ta vijs'kovoi' tehniky Zbrojnyh Syl Ukrai'ny. Kyi'v, pp. 350-352.

9. Sadyh G.S. (1995). Pokazatel' ostatochnogo resursa i ego svojstva. *Izvestija AN SSSR, Tehnicheskaja kibernetika*, no 4, P. 98-102.

10. Komarov V.O., Rasstrygin O.O., inventors (2018). Prystrij dlja vyznachennja prostorovo-chastotnyh harakterystyk kolyvan' konsol'no zakriplenyh elementiv lital'nyh aparativ pry i'hnih vyprobuvannjah na utomlenu micnist'. Ukrainian patent, no. 127849.

11. Komarov V.O.; Komarov V.O., Tkachenko V.A., Galushka V.I., inventors (2016). Sposib vyznachennja harakterystyk zhorstkosti kryla litaka nerujnivnym metodom v umovah ekspluatacii' ta vedennja bojovyh dij. Ukrainian patent, no. 109226.

12. Barzylovych E.Ju., Mezencev V.G. and Savenkov M.V. (1982). Nadezhnost' avyacyonnыh system. Moscow: Transport, 175 p.

Ph.D. Pampukha I.V., Ph.D. Nikiforov M.M., Komarov V.O.

DEVELOPMENT OF METHODOLOGY TO DETERMINE THE RESERVE FACTOR OF COMBAT AIRCRAFT BASED ON THE DYNAMIC RESPONSE ANALYSIS WITH REGARD FOR OPERATIONAL FACTORS

The article considers the issues of diagnostics of the technical condition of cantilevered aircraft structures based on the dynamic response analysis.

This task provides for determining the real technical condition of the damaged structure and, as a result, the reserve factor. The main criterion is to use as little information as possible to obtain a precise objective assessment. It is suggested to use the structural dynamics being the most informative as diagnostic features. These are natural oscillation frequencies (torsional and flexural) and zero-twist axis position (according to the data from volitionally undamaged structures taken as reference).

The methodology has been patented. As a technical solution, the methodology provides for frequency tests with dysfunction of flexural and torsional oscillation frequencies under which a minimum frequency of natural oscillations corresponding to the minimum residual strength shall be set for each type of aircraft, namely, for its part - wings, fins (cantilevered structures of the glider).

The increased number of analysed natural oscillation frequencies increases the reliability of the residual strength estimation. Based on this, the developed and produced equipment and monitor equipment as a mobile version (which are also patented), can be effectively used when basing aircraft in the combat theatre.

Based on the provisions of the NIAS similar monitoring system can be implemented in military units of the Air Force of the Armed Forces of Ukraine during the operation of aircraft according to the technical condition.

Keywords: diagnostics of technical condition, natural oscillation frequency, residual strength, non-destructive testing, wing, structural frame.

УДК 004.421

д.т.н., проф. **Пархомей І.Р.** (КПІ)
д.т.н., проф. **Дружинін В.А.** (КПІ)
к.т.н. **Цьопа Н.В.** (КПІ)
к.т.н., с.н.с. **Жиров Г.Б.** (КНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-04

ВИКОРИСТАННЯ НАНОБОТІВ У ДІАГНОСТУВАННІ СТАНУ ЖИВОГО ОРГАНІЗМУ

На сьогоднішній день швидкими темпами розвивається новий напрямок у медичній науки - наномедицина. Велика частина методів даного напрямку поки існує тільки у вигляді проектів. Однак більшість експертів вважає, що саме ці методи стануть основними в XXI столітті. Так, наприклад, Національні інститути охорони здоров'я США включили наномедицину в п'ятірку найбільш пріоритетних областей розвитку медицини в XXI столітті, а Національний інститут раку США збирається застосовувати досягнення наномедицини при лікуванні раку. Ряд зарубіжних наукових центрів вже продемонстрували дослідні зразки в областях діагностики, лікування, протезування та імплантації. Наномедицина прагне надати значний набір дослідницьких інструментів і клінічно корисних пристроїв в найближчому майбутньому.

У даній роботі розглядається методика застосування робототехнічних систем нанорозмірів для точного діагностування стану організму. Запропонована тематика поєднує в собі два аспекти: суто технічний і біологічний, а саме стан організму. Ці аспекти самі по собі є достатньо важливими науковими проблемами, а їх поєднання потребує створення техніко-біологічної концепції діагностування, без пошкодження функцій живого організму та його тканин.

Запропонована методика діагностування живого організму за допомогою наноботу включає три основні складові, які наведені в роботі, а саме: послідовність дій щодо маніпуляцій наноботом в організмі; розрахунок кількісних характеристик процесу діагностування та схемну реалізацію відповідного діагностуючого сканеру. Практична реалізації запропонованого сканера є нескладною у реалізації і експлуатації, а логічність наведеної методики дозволяє сформулювати загальний підхід (концепцію) в подальшому при створенні новітніх засобів діагностики. Проведений аналіз попередніх результатів дослідження дозволяє стверджувати, що введення, виведення і використання наноботу в живій тканині є безпечним.

Ключові слова: наноботи, нано-робототехнічна система, ізотоп, іонізуюче поле, валентна зона, потужність опромінення.

Вступ та аналіз останніх досліджень. Актуальність запропонованого дослідження викликано необхідністю швидкого, а головне точного діагностування стану живого організму.

Запропонована тематика поєднує в собі два аспекти: суто технічний (функціонування наноботів) і біологічний – стан організму.

Ці аспекти самі по собі є важливими науковими проблемами, а їх поєднання потребує вирішення третьої наукової проблеми – створення техніко-біологічної концепції діагностування, без пошкодження функцій живого організму та його тканин. У роботі досліджується процес поєднання технічних систем в інтересах діагностування та розробляється методика отримання інформації про стан організму.

Зрозуміло, що така складна проблема може бути досліджена з низкою обмежень, а саме:

- засобом діагностування може бути над мала робототехнічна система;
- нанобот повинен випромінювати інформативний сигнал, який здатна приймати та обробляти сучасна радіосистема;
- наслідки функціонування наноботу не повинні негативно впливати на живі тканини;
- доставка до місця призначення повинна бути максимально точною.

Складність і разом з цим актуальність запропонованої тематики підтверджується сучасними науковими і технічними тенденціями. У працях [1-3] наведені напрямки доставки

та націлювання фармацевтичних, терапевтичних і діагностичних засобів. Вони включають визначення точних цілей (клітин і рецепторів), пов'язаних з конкретними клінічними станами, і вибір відповідних наноносітелей для досягнення необхідних відповідей при мінімізації побічних ефектів. Мононуклеарні фагоцити, дендритні клітини, ендотеліальні клітини і ракові пухлини (пухлинні клітини, а також новоутворення пухлини) є ключовими мішенями. Також у [3] висвітлені раціональні підходи до проектування і конструювання поверхонь нанорозмірних транспортних засобів та об'єктів для доставки ліків по конкретних ділянок і медичної візуалізації після парентерального введення. Обговорюються також потенційні пастки або побічні ефекти, пов'язані з наночастинками.

У працях [4-5] розроблено інтерактивну карту нуклідів, яка надає дані про структуру і розпад ядра. У працях [6] проаналізовані різні ізотопи та період їх існування з метою їх використання в якості нанобота доставки діагностуючого сигналу до місця призначення.

Постановка завдання. В даній роботі запропонована методика застосування робототехнічних систем нанорозмірів до безпосереднього місця діагностування. Також у роботі поставлені та вирішені наступні завдання: обрання і обґрунтування місця введення наноботу в живий організм і шляхів його доставки до місця призначення; обґрунтування вимог до діагностуючого сигналу та способів його обробки; визначення способу безпечного виведення наноботу з організму.

Результати дослідження. Як було обумовлено спочатку – застосування наноботів у сфері діагностування жорстко пов’язано із забороною пошкодження тканин під час введення або виведення такої робото технічної системи з організму. Таким вимогам, за своїми розмірами, задовольняє або молекула або молекулярний комплекс, який виконує діагностуючу функцію в живій системі. Здійснювати таку функцію можна завдяки наявності джерела енергії і ця функція супроводжується дисипацією енергії.

Крім того робототехнічна система повинна правильно і точно обрати місце призначення. Як правило така нано-робототехнічна система буде знаходитися о двох станах [4,5]: передстаном – високоенергетичний стан, в якому нанобот знаходиться під час руху до місця призначення; після станом – низько енергетичний стан наноботу після прибуття до місця призначення та передачі сигнальної інформації.

Тобто діагностуючий нанобот – це робототехнічна система, якій надано запас енергії для руху та передачі інформації. Але в умовах живого організму без механічних та біологічних пошкоджень це майже неможливо. Якщо використовувати молекулярний комплекс то досягнення місця призначення буде супроводжуватися швидким розсіюванням (дисипацією) наданої енергії. Хоча явна перевага введення в організм нанобота шляхом ін'єкції присутня. Тобто існує висока ймовірність невчасного переходу наномолекулярного роботу з передстану в післястсан.

Виходячи з цього, пропонується в якості нанобота доставки діагностуючого сигналу до місця призначення ще менший за лінійними розмірами об’єкт – ізотопну атомарну систему. Досить гарні результати можуть бути отримані при використанні ізотопів кальцію. Це група ізотопів кальцію: ^{45}Ca, ^{47}Ca.

Найбільшу цікавість викладає ^{45}Ca, ^{47}Ca з періодом існування від 15,3 до 47 годин (інші ізотопи, наприклад кремнію, існують до декількох хвилин) [5,6]. Рух такого ізотопу до місця призначення в живому організмі в наслідок природних біохімічних процесів відбувається від 3 до 12 годин [7]. Після переходу в післястан ^{47}Ca втрачає свою енергетичну активність (W = 6.12еВ). Виведення наноботу на основі ^{47}Ca здійснюється шляхом природного використання його в якості будівельного клітинного матеріалу після втрати енергетичної активності. Виведення ^{45}Ca, який має великий напіврозпад, здійснюється шляхом природного його сполучення з водою [8]:

$$^{45}Ca + 2H_2O \rightarrow Ca(\mathrm{OH})_2 + H_2 \ . \qquad (1)$$

Випромінювання ізотопу ^{45}Ca носить природу γ - випромінювання з енергетикою W = 5.62еВ, що в деяких випадках, за впливом на тканини носить обмежений характер і може бути використаний не як діагностуючий робото технічний засіб, а як терапевтичний.

Тому доцільно зосередити увагу на ізотопі ^{47}Ca, тому що інші ізотопи зазначеного ряду або нестабільні або надто активні при взаємодії з живими тканинами. Зазначені підходи до терапевтичного використання інших хімічних елементів звичайно здійснюються але без складової радіотехнічної обробки сигналу робототехнічного носія.

З огляду на викладене пропонується мнемонічна схема методики використання наноботів при діагностуванні живого організму, яка наведена на рис. 1.

Наступним кроком методики, що розроблюється є отримання і обробка діагностуючого сигналу ізотопного наноботу. Напіврозпад ізотопів супроводжується, як відомо, α, β, γ - випромінюваннями [9].

З точки зору отримання і обробки діагностуючого сигналу пропонується використання γ - випромінювання, яке супроводжується електромагнітними сигналами нанометровому діапазону хвиль. В зазначеному випадку отримання карти місце призначення діагностуючого наноботу, який випромінює, може бути отримане шляхом радіолокаційного сканування поверхні організму.

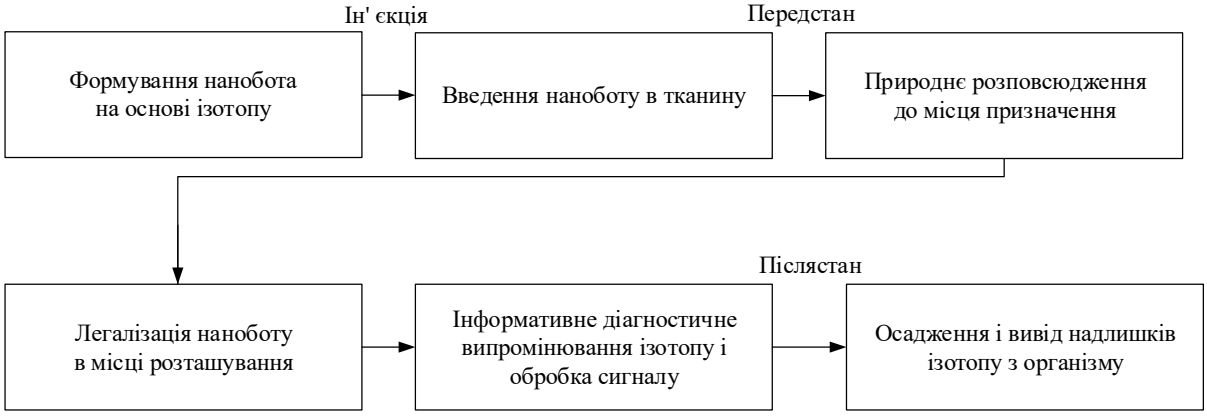

Рисунок 1 – Мнемонічна схема методики використання ізотопних наноботів

Інша справа, якщо використати ефект вторинної радіоактивності, яка спричиняє утворення локальних зон провідності і може бути зафіксовано як джерело надвисокочастотного струму на імпедансній поверхні.

Важливою обставиною, яка сприяє створенню локальної провідності, є наявність у атомів, в зоні провідності електронів, що характерно для провідників.

У напівпровідників та діелектриків, до яких відноситься ^{47}Ca, зона провідності і валентна зони розділені забороненими зонами.

Так у кальцію ширина забороненої зони складає 4.65 - 5еВ [11].

Якщо припустити, що за певних умов, електрони з валентної зони атома будуть переміщені до зони провідності, то зазначена речовина буде виявляти властивості провідника. Це надасть змогу змінити погляди на застосування деяких діелектриків. Як відомо, перехід електронів у зону провідності відбувається у збудженому стані атому. Збудження атому можливо здійснити за умови впливу зовнішнього джерела енергії – наприклад іонізуючого поля. Потрібна потужність поля опромінення P для переводу одного електрону з валентної зони у зону провідності визначається залежністю [12]:

$$P = \frac{W}{\tau}, \tag{2}$$

де W- ширина забороненої зони (для $Ca \prec 5eB$); τ - час знаходження електрона у зоні провідності збудженого атома ($\tau \approx 10^{-5}...10^{-6} c$).

Для *Ca* і його сполук потрібна потужність складає $8.6 \cdot 10^{-13}$Вт. Враховуючи закон Авогадро, створення локальної зони провідності для сполук кальцію потребує потужності опромінення до 10^4 Вт, що не має практичного змісту. Але якщо зважити на те, що передача енергії для збудження атома буде відбуватися за умови досягнення частотного та фазового резонансу зовнішнього джерела опромінення і власних коливань атома, тоді енергії на утворення вторинної радіації і локальної зони провідності потрібно суттєво менше.

Вторинна радіація здатна утворити струм з напругою в зоні локальної провідності на резонансній частоті коливання атома, яка визначається залежністю:

$$U_p = 2U_m \omega_p \tau \left| \frac{\sin\left(\frac{\omega_p}{2} \cdot \tau\right)}{\left(\frac{\omega_p}{2} \cdot\right)\tau} \right|,$$

де: U_m - амплітуда власних коливань атома Ca на частоті ω_p; ω_p - частота гармоніки спектру сигналу, який виникає в наслідок опромінення ізотопом ^{47}Ca з довжиною хвилі $4700\dot{A}$.

Відповідно потужність збудженого сигналу на дистанції *D* до 10 метрів складатиме $P = 2,5 \cdot 10^{-16} Bm$, виходячи з виразу

$$P = \frac{2P_1 G_T \sigma}{\left(4\pi D^2\right)^2}, \tag{4}$$

де: G_T - коефіцієнт підсилення приймача; σ - площа датчика; P_1 - потужність електромагнітного випромінювання.

Якщо припустити, що на деякій відстані відбувається співпадання по фазі на частоті або їх різниця є ціла постійна величина сигналу опромінення та коливань атомів Ca датчика, то таку взаємодію слід розглядати як когерентну. При цьому відбувається збудження атома датчика за рахунок передачі енергії поля опромінення від ізотопу. У цьому випадку електрони з валентної зони переходять до зони провідності, що супроводжується випромінюванням радіохвилі. Тривалість випромінювання визначається часом знаходження електронів у забороненій зоні після приведення атому із стану рівновагив збуджений стан і дорівнює $(0,5-1)мкс$ [13].

Результуюча енергія випромінювання визначається залежністю

$$E_p = \left(\left(E_{Ca}\right)^2 + \left(E_{^{47}Ca}\right)^2 + 2E_{Ca} \cdot E_{^{47}Ca} \cdot \cos\Delta\varphi\right)^{\frac{1}{2}}, \tag{5}$$

де: E_{Ca} - енергія електрона датчика; $E_{^{47}Ca}$ - енергія опромінення ізотопу; $\Delta\varphi$ - різниця фаз зазначених коливань.

Розрахунки показують, що на відстані до 10 метрів при опроміненні датчика полем ізотопу потужність діагностуючого сигналу із місця призначення в організмі становитиме $1,602 \cdot 10^{-7} Bm$. Тобто в локальній області провідності датчика можливо фіксувати діагностуючий сигнал на протязі $1,7мкс$.

Наявність цієї області пояснюється виходом електронів в зону провідності, тобто виникає вторинне статичне електричне поле. Зважаючи на викладене, практичний інтерес викликає інтенсивність випромінювання датчика у випромінюючому полі ізотопу.

Дані розрахунки можна виконати за формулою:

$$I = \frac{\rho V U^2}{2}, \tag{6}$$

де: ρ - густина матеріалу датчика (Ca); V - швидкість розповсюдження поля; U - амплітуда коливань атома датчика.

У випадку, який розглядається, інтенсивність випромінювання у збудженому стані складає $16,2 \cdot 10^{-15}\, Вт \cdot м^3$.

Зазначений підхід щодо дистанційного сканування діагностуючого сигналу має практичну значимість, оскільки може бути реалізований у вигляді технічного пристрою з доволі простою побудовою рис. 2.

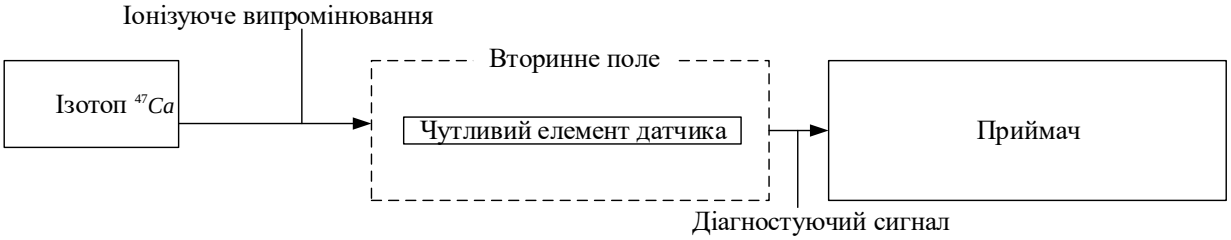

Рисунок 2 – Схема елементарного датчика-сканера місцезнаходження нанобота в живій тканину

Слід відзначити, що наведені елементарні датчики повинні бути згрунтовані в скануючи решітку, яка за площею поверхні повинна перекривати площу живого організму, що діагностується.

Висновки. Таким чином запропонована методика діагностування живого організму за допомогою наноботу включає три основні складові, які наведені в роботі, а саме: послідовність дій щодо маніпуляцій наноботом в організмі; розрахунок кількісних характеристик процесу діагностування та схемну реалізацію відповідного діагностуючого сканеру.

Проведений аналіз попередніх результатів дослідження дозволяє стверджувати, що введення, виведення і використання наноботу в живій тканині є безпечним.

Наведена схема практичної реалізації запропонованого сканера є нескладною у реалізації і експлуатації, а логічність наведеної методики дозволяє сформулювати загальний підхід (концепцію) в подальшому при створенні новітніх засобів діагностики.

ЛІТЕРАТУРА:

1. Drexler K. Eric.: Radical Abundance: How a Revolution in Nanotechnology Will Change Civilization 1st edn. Publisher, PublicAffairs (US), 2013.

2. Kimball N.: Glossary of Biotechnology & Agrobiotechnology Terms 5th edn. Publisher, CRC Press, 2016.

3. Moghimi S.M., Hunter A.C., Murray J.C.: Nanomedicine: Current status and future prospects. FASEB Journal 19(3), 2005, pp. 311-330.

4. Nanomeficine glossary, Homepage http: // www.nanocarbontech-nology.com/nanotech-glossary.htm.

5. Sonzogni, A.: NNDC Chart of Nuclides. International Conference on Nuclear Data for Science and Technology 2007, vol. 41(2), Published online (2008).

6. Jerschow A. Interactive NMR Freguency Map, Homepage http://www.nyu.edu/projects/jerschow/NMRmap/NMRmap_deployed.html

7. Parkhomei I., Parkhomey A., Otychenko O. Modeling the influence of a nanomagnet on the properties of a biogenic hydroxyomagnet. Interdepartmental scientific technical journal «Adaptive systems of automatic control» 1 (28), 2016, pp.83-90.

8. Audi G., Bersillon O. The NUBASE evaluation of nuclear and decay properties. Nuclear Physics A 729, 2003, pp. 3 – 128.

9. Bruining H., Fry D.W. Physics and Applications of Secondary Electron Emission 2nd edn. Publisher: Pergamon, 2016.

10. Cetnar J., General solution of Bateman equations for nuclear transmutations. Annals of Nuclear Energy, 2006? №33 (7), pp. 640-645.

11. Housecroft C. E.: Inorganic Chemistry 5th edn. Publisher: Pearson (2018).

12. Parkhomey I., Humenyi D, Tkach M. Structural model of robot-manipulator for capture. Conf. ICC SEEA, January, 2018.

REFERENCES:

1. Drexler K. Eric.: Radical Abundance: How a Revolution in Nanotechnology Will Change Civilization 1st edn. Publisher, PublicAffairs (US), 2013.

2. Kimball N.: Glossary of Biotechnology & Agrobiotechnology Terms 5th edn. Publisher, CRC Press, 2016.

3. Moghimi S.M., Hunter A.C., Murray J.C.: Nanomedicine: Current status and future prospects. FASEB Journal 19(3), 2005, pp. 311-330.

4. Nanomeficine glossary, Homepage http: // www.nanocarbontech-nology.com/nanotech-glossary.htm.

5. Sonzogni, A.: NNDC Chart of Nuclides. International Conference on Nuclear Data for Science and Technology 2007, vol. 41(2), Published online (2008).

6. Jerschow A. Interactive NMR Freguency Map, Homepage http://www.nyu.edu/projects/jerschow/NMRmap/NMRmap_deployed.html

7. Parkhomei I., Parkhomey A., Otychenko O. Modeling the influence of a nanomagnet on the properties of a biogenic hydroxyomagnet. Interdepartmental scientific technical journal «Adaptive systems of automatic control» 1 (28), 2016, pp.83-90.

8. Audi G., Bersillon O. The NUBASE evaluation of nuclear and decay properties. Nuclear Physics A 729, 2003, pp. 3 – 128.

9. Bruining H., Fry D.W. Physics and Applications of Secondary Electron Emission 2nd edn. Publisher: Pergamon, 2016.

10. Cetnar J., General solution of Bateman equations for nuclear transmutations. Annals of Nuclear Energy, 2006? №33 (7), pp. 640-645.

11. Housecroft C. E.: Inorganic Chemistry 5th edn. Publisher: Pearson (2018).

12. Parkhomey I., Humenyi D, Tkach M. Structural model of robot-manipulator for capture. Conf. ICC SEEA, January, 2018.

д.т.н., проф. Пархомей І.Р., д.т.н., проф. Дружинин В.А., к.т.н. Цьопа Н.В., к.т.н., с.н.с. Жиров Г.Б.

ИСПОЛЬЗОВАНИЕ НАНОБОТОВ ПРИ ДИАГНОСТИРОВАНИИ СОСТОЯНИЯ ЖИВОГО ОРГАНИЗМА

На сегодняшний день быстрыми темпами развивается новое направление в медицинской науки - наномедицина. Большая часть методов данного направления пока существует только в виде проектов. Однако большинство экспертов полагает, что именно эти методы станут основополагающими в XXI веке. Так, например, Национальные институты здравоохранения США включили наномедицину в пятёрку самых приоритетных областей развития медицины в XXI веке, а Национальный институт рака США собирается применять достижения наномедицины при лечении рака. Ряд зарубежных научных центров уже продемонстрировали опытные образцы в областях диагностики, лечения, протезирования и имплантации. Наномедицина стремится предоставить значительный набор исследовательских инструментов и клинически полезных устройств в ближайшем будущем.

В данной работе рассматривается методика применения робототехнических систем наноразмеров для точного диагностирования состояния организма. Предложенная тематика сочетает в себе два аспекта: чисто технический и биологический - состояние организма. Эти аспекты сами по себе являются достаточно важными научными проблемами, а их сочетание требует технико-биологической концепции диагностирования, без повреждения функций живого организма и его тканей. Предложенная методика диагностирования живого организма с помощью наноботов включает три основные составляющие, которые приведены в работе, а именно: последовательность действий по манипуляции наноботом в организме; расчет количественных характеристик процесса диагностирования и схемную реализацию соответствующего диагностирующего сканера. Практическая реализации предложенного сканера является несложной в реализации и эксплуатации, а логичность приведенной методики позволяет сформулировать общий подход (концепцию) для дальнейшего создания новейших

средств диагностики. Проведенный анализ предыдущих результатов исследования позволяет утверждать, что введение, выведение и использования наноботов в живой ткани организма является безопасным.

Ключевые слова: наноботы, нано-робототехнические системы, изотоп, ионизирующее поле, валентная зона, мощность облучения.

Doctor of Technical Sciences Parkhomey I.R, Doctor of Technical Sciences Druzhynin V.A., Ph.D. Tsopa N.V., Ph.D. Zhyrov G.B.

USE OF NANOBOTS IN DIAGNOSIS THE STATE OF THE LIVING ORGANISM

Today, a new direction in medical science is developing rapidly - nanomedicine. Most of the methods in this area so far exist only in the form of projects. However, most experts believe that these methods will become fundamental in the 21st century. For example, the National Institutes of Health of the United States included nanomedicine in the top five areas of medical development in the 21st century, and the National Cancer Institute of the United States intends to apply the achievements of nanomedicine in the treatment of cancer. A number of foreign research centers have already demonstrated prototypes in the areas of diagnosis, treatment, prosthetics and implantation. Nanomedicine seeks to provide a significant set of research tools and clinically useful devices in the near future.

This paper discusses the technique of using nanoscale robotic systems to accurately diagnose the condition of an organism. The proposed topic combines two aspects: purely technical and biological - the state of the organism. These aspects in themselves are important scientific problems, and their combination requires the creation of a technical and biological concept of diagnosis, without damaging the functions of the living organism and its tissues. The proposed technique for diagnosing a living organism by means of a nanobot includes three main components that are presented in the work, namely: the sequence of actions for manipulation of the nanobot in the body; calculation of quantitative characteristics of the diagnosis process and schematic implementation of the appropriate diagnostic scanner. The practical implementation of the proposed scanner is easy to implement and operate, and the logic of the above methodology allows us to formulate a common approach (concept) in the future when creating the latest diagnostic tools. The analysis of preliminary results of the study suggests that the introduction, removal and use of nanobots in living tissue is safe.

Keywords: nanobots, nano-robotics system, isotope, ionizing field, valence band, irradiation power.

УДК 621.396.600

д.військ.н., с.н.с. **Семененко О.М.** (ЦНДІ ЗСУ)
Каблуков О.А. (ЦНДІ ЗСУ)
к.т.н., с.н.с. **Краснік А.В.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-05

УДОСКОНАЛЕНИЙ МЕТОД МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ФУНКЦІОНУВАННЯ БОРТОВИХ РАДІОЛОКАЦІЙНИХ СТАНЦІЙ УПРАВЛІННЯ ЗБРОЄЮ В УМОВАХ АКТИВНОЇ ПРОТИДІЇ СТАНЦІЯМ ПЕРЕШКОД ПРОТИВНИКА

У статті описано удосконалений метод математичного моделювання функціонування бортових радіолокаційних станцій в умовах активної протидії станціям перешкод противника.

Проведено аналіз сучасних бортових радіолокаційних систем та станцій активних перешкод як об'єктів математичного моделювання, а також існуючих способів активної протидії бортовим станціям перешкод противника та методів математичного моделювання функціонування бортових радіолокаційних станцій.

Сформовані вихідні дані щодо моделювання функціонування бортових радіолокаційних станцій в умовах перешкод та активної протидії станціям перешкод противника, наведено визначену ситуацію повітряного бою, яка підлягає математичного опису.

Було обрано показники та критерії, які характеризують ефективність функціонування бортових радіолокаційних станцій основним з яких є обмеження по дальності їх використання в залежності від способу протидії, що застосовується. Проведені попередні розрахунки щодо застосування зазначених способів активної протидії. Враховуючи особливості застосування способів активної протидії станціям перешкод противника, запропоновано поділити цикл повітряного бою між літаками на 5 етапів в залежності від дальності між ними.

Розроблено алгоритм обґрунтування вибору способів протидії станціям перешкод противника з урахуванням дальності між літаками для безперервного супроводження цілі та визначені ймовірності супроводження цілі з урахуванням застосування різних комбінацій способів протидії.

Для якісної та повної оцінки ефективності функціонування бортових радіолокаційних станцій запропоновано використовувати нечіткі множини та теорію ігор, за допомогою чого побудована математична модель оцінювання ефективності функціонування бортових радіолокаційних станцій в умовах протидії станціям перешкод противника, яка застосовувалась також під час розроблення алгоритму та вибору найефективнішій комбінації способів протидії.

Ключові слова: методи математичного моделювання, алгоритм, модель, станція активних перешкод індивідуального захисту, бортова радіолокаційна станція управління зброєю, способи контррадіоелектронної протидії.

Вступ та постановка задачі. Досвід локальних війн і конфліктів показує, що авіація без засобів радіоелектронної боротьби має дуже низьку живучість. Застосування станцій активних перешкод індивідуального захисту літаків доводить ймовірність неураження літака в повітряному бою до 0,45–0,75, а комплексне застосування засобів радіоелектронної боротьби (РЕБ) дозволяє довести цю ймовірність до 0,8–0,95. Таким чином в зв'язку з важливістю завдань виконуваних бортовими засобами РЕБ та їх ефективністю останнім часом все більше активно стали досліджуватися питання радіоелектронної протидії самим засобам РЕБ так звана контррадіоелектронна протидія (КРЕП) [1-4].

Сьогодні для протидії станціям активних перешкод індивідуального захисту (САП ІЗ) є ряд способів протидії їм, використання яких має випадковий характер. Проте проведений аналіз їх застосування свідчить, що більшість способів активної протидії мають різні умови їх застосування, які пов'язані із змінами роботи бортової радіолокаційної станції (БРЛС), що накладає на них обмеження по дальності їх використання.

Розвиток та практична реалізація нових способів активної протидії станціям перешкод противника в повітряному бою створює умови щодо необхідності урахування їх впливу на загальну ефективність функціонування БРЛС управління зброєю, що в свою чергу, викликає

необхідність удосконалення існуючих методів опису функціонування БРЛС управління зброєю (БРЛ УЗ) в умовах перешкод та одночасної активної протидії їм.

Тому подальший розвиток способів радіоелектронної протидії САП ІЗ противника створює необхідність удосконалення математичних моделей опису функціонування БРЛС в повітряному бою як в умовах перешкод так і одночасної протидії їм з метою формування чітко визначеного алгоритму застосування розроблених та практично реалізованих на борту способів протидії.

Вирішення цього наукового завдання можливе в удосконаленні існуючих методів математичного моделювання функціонування БРЛС УЗ. Тому метою статті є розроблення удосконаленого методу математичного моделювання функціонування БРЛС УЗ в умовах активної протидії станціям перешкод противника у повітряному бою.

Аналіз останніх досліджень і публікацій. Проведений аналіз останніх досягнень і публікацій [1–13] з тематики, що розглядалась, показує, що переважна більшість математичних моделей, які описують процеси взаємодії засобів РЕБ та радіолокації, призначені для оцінювання ефективності функціонування бортових радіолокаційних станцій в умовах перешкод [1, 3, 4].

Роботи [2, 5] присвячені способам активної протидії КРЕП, які мають різні умови їх застосування та пов’язані із змінами роботи БРЛС, що накладає на них обмеження по дальності їх використання.

Окремими випадками є моделі, які дозволяють оцінювати ефективність застосування тих чи інших пасивних засобів захисту бортової радіолокаційної станції від окремих видів перешкод [9, 10].

У роботі [12] автори зазначають, що процес протистояння в повітряному бою БРЛС УЗ та САП ІЗ протікає в умовах стохастичної невизначеності прешкодової обстановки в силу відсутності повної інформації про ведення КРЕП, про характеристики САП ІЗ противника, невідомих умов ведення повітряного бою, відсутності практичних оцінок перешкодозахищеності БРЛС при веденні КРЕП на певних етапах бою.

Виклад основного матеріалу дослідження. Математичний опис застосування удосконаленого методу математичного моделювання функціонування БРЛС УЗ поділено на п’ять етапів. Структурно-логічна схема удосконаленого методу складається з п’яти етапів.

На першому етапі (рис. 1) сформовані вихідні дані щодо моделювання функціонування БРЛС УЗ в умовах перешкод та протидії САП ІЗ противника, основні з яких: потужність передавачів БРЛС та САП ІЗ; коефіцієнти підсилення антен БРЛС та САП ІЗ; коефіцієнт подавлення БРЛС; потужність перешкоди та сигналу на вході антени; кут зміни площини поляризації перешкоди при прийомі від ортогонального положення; дальність від винищувача до цілі.

У блоці 1.1 (рис. 1) наведена ситуація повітряного бою, яка підлягає математичного опису та розкриті напрями КРЕП. У блоці 1.2 (рис. 1) наведено у загальному вигляді алгоритм застосування способів протидії станціям активних перешкод індивідуального захисту противника з урахуванням етапів повітряного бою та режимів пеленгації.

Слід зазначити, що під час опису протидії станціям перешкод противника використовується чотири способи КРЕП: 1 та 2 способи – Здійснення протидії станції активних перешкод противника шляхом зміни поляризації сигналу на прийомі БРЛС УЗ; 3-ій спосіб – Здійснення протидії станції активних перешкод противника шляхом зміни потужності опромінюючого сигналу БРЛС УЗ; 4-ий спосіб – Здійснення протидії станції активних перешкод противника шляхом порушення регулярності опромінення.

На другому етапі (рис. 2)обрано показники та критерії, які характеризують ефективність функціонування бортових радіолокаційних станцій управління зброєю. У блоці 2.1 (рис. 2) визначено показники функціонування БРЛС УЗ в умовах перешкод без урахування протидії, а у блоці 2.3 (рис. 2) – в умовах перешкод та протидії їм, а саме: дальність виявлення цілі; дальність застосування режиму безперервної пеленгації; відношення сигнал / шум на вході

приймача БРЛС УЗ; потужність корисного сигналу на вході приймача БРЛС УЗ; коефіцієнт подавлення БРЛС.

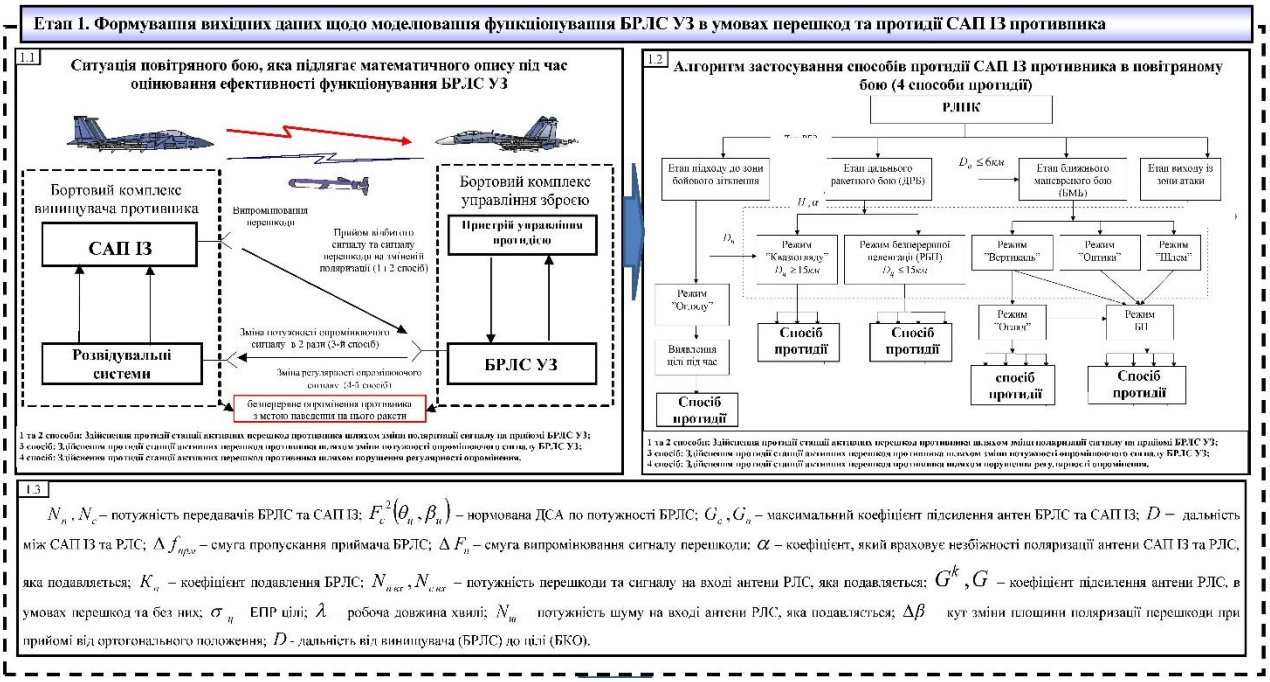

Рисунок 1 – Удосконалений метод етап 1

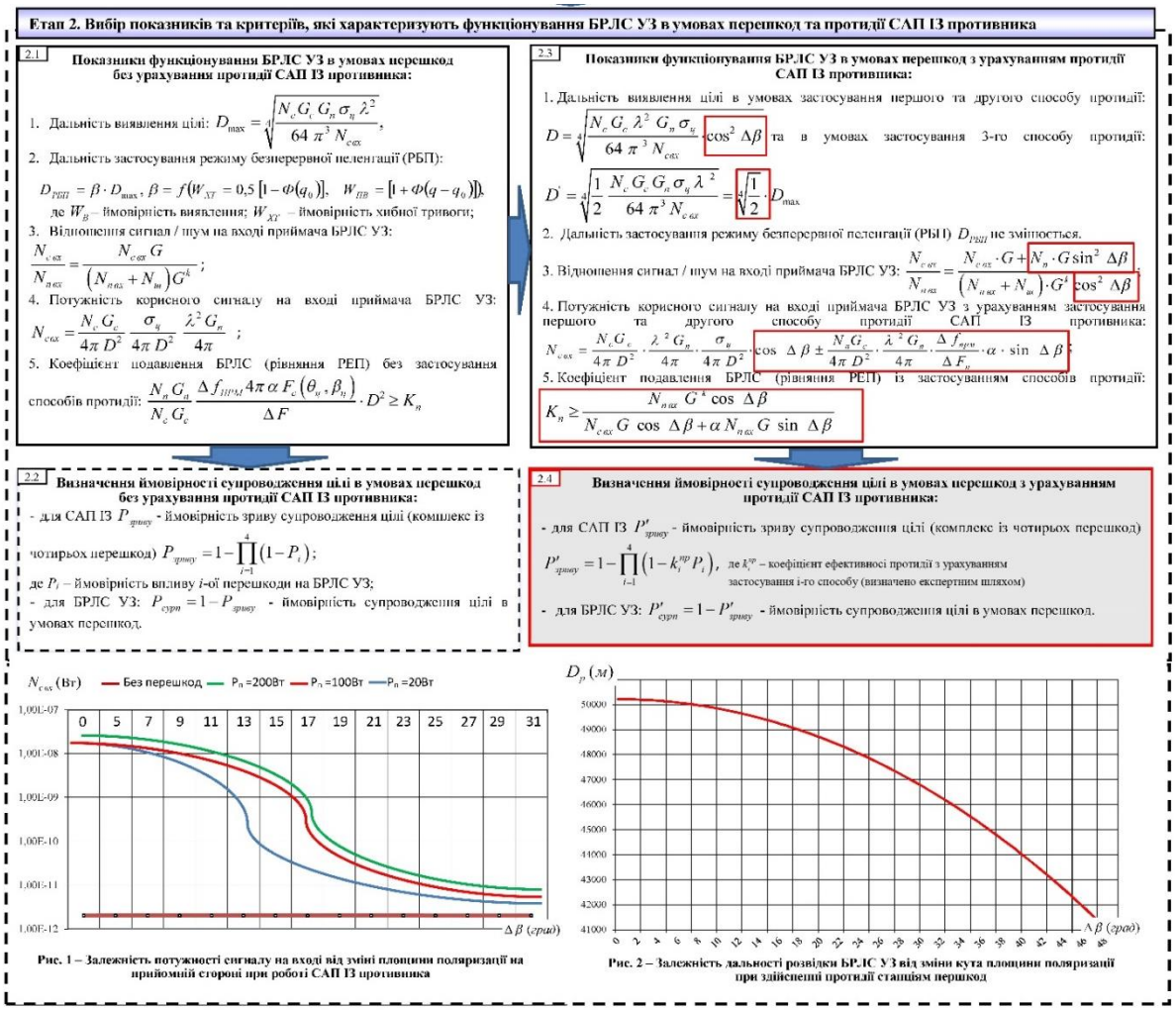

Рисунок 2 – Удосконалений метод етапи 2

Також розраховано обмеження щодо застосування обраних способів активної протидії, основним критерієм обмеження є дальність їх використання за формулами (1) та (2) в залежності від способу КРЕП, який застосовується.

$$D = \sqrt[4]{\frac{N_c G_c \lambda^2 G_n \sigma_ц}{64 \pi^3 N_{c\,вх}} \cdot \cos^2 \Delta\beta} \ , \tag{1}$$

$$D^{'} = \sqrt[4]{\frac{1}{2} \frac{N_c G_c G_n \sigma_ц \lambda^2}{64 \pi^3 N_{c\,вх}}} = \sqrt[4]{\frac{1}{2}} \cdot D_{\max} \ . \tag{2}$$

де N_c ($N_{c\ вх}$) – потужність сигналу передавача та сигналу на вході антени, G_c (G_n) – максимальний коефіцієнт підсилення антен БРЛС та САП ІЗ, λ – робоча довжина хвилі, $\sigma_ц$ – ефективна площина розсіювання цілі, $\Delta\beta$ – кут зміни площини поляризації.

Розрахунки свідчать, що при застосуванні 1 та 4 способів максимальна дальність зменшується на 4 %; при застосуванні 2-го або 3-го способів максимальна дальність зменшується на 16 %, а під час застосуванні всіх чотирьох способів – на 20 %.

Критерієм ефективності функціонування БРЛС в умовах перешкод та одночасної протидії їм обрано ймовірність супроводження цілі, тому у блоках 2.2 та 2.4 (рис. 2) визначено ймовірності супроводження цілі в умовах перешкод з урахуванням протидії та без неї, де додатково застосовано коефіцієнт ефективності протидії.

Далі відповідно проведених розрахунків для прикладу графічно наведені залежність потужності сигналу на вході від зміні площини поляризації на прийомній стороні при роботі САП ІЗ противника та залежність дальності розвідки БРЛС УЗ від зміни кута площини поляризації при здійсненні протидії станціям перешкод.

На третьому етапі (рис. 3) розроблено Алгоритм обґрунтування вибору способів протидії станціям перешкод противника з урахуванням дальності до цілі та відповідній комбінації способів протидії для безперервного супроводження цілі.

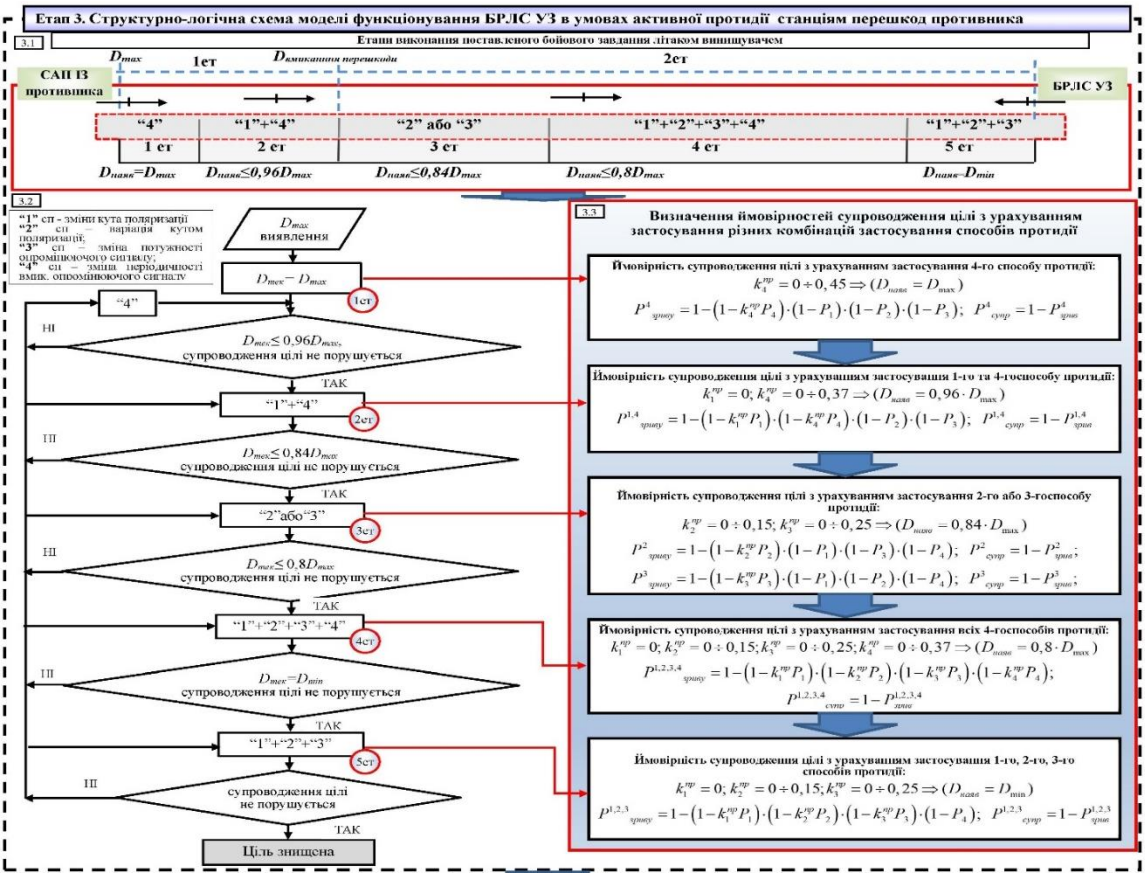

Рисунок 3 – Удосконалений метод етап 3

Розроблення алгоритму передбачало необхідність перегляду послідовності ведення повітряного бою із урахуванням особливостей застосування запропонованих способів радіоелектронної протидії станціям перешкод противника

У блоці 3.1 (рис. 3) запропоновано поділити етапи виконання поставленого бойового завдання літаком винищувачем на 5 етапів в залежності від дальності до цілі (розрахованих вище) на відміну від існуючих етапів на сьогодні.

У блоці 3.3 (рис. 3) визначаються ймовірності супроводження цілі з урахуванням застосування різних комбінацій способів протидії з урахуванням відповідних коефіцієнтів протидії.

Розроблений алгоритм удосконалює існуючий підхід функціонування бортової РЛС УЗ за показником ймовірності супроводження цілі в умовах застосування запропонованих способів протидії станціям перешкод враховуючи обмеження їх застосування.

На етапі 4 (рис. 4) проведено оцінювання ефективності функціонування БРЛС УЗ в умовах протидії станціям перешкод противника та без протидії

У блоці 4.1 (рис. 4) відбувається формування нечітких оцінок ймовірності супроводження БРЛС УЗ в умовах перешкод та протидії САП ІЗ противника у разі застосування усіх способів протидії.

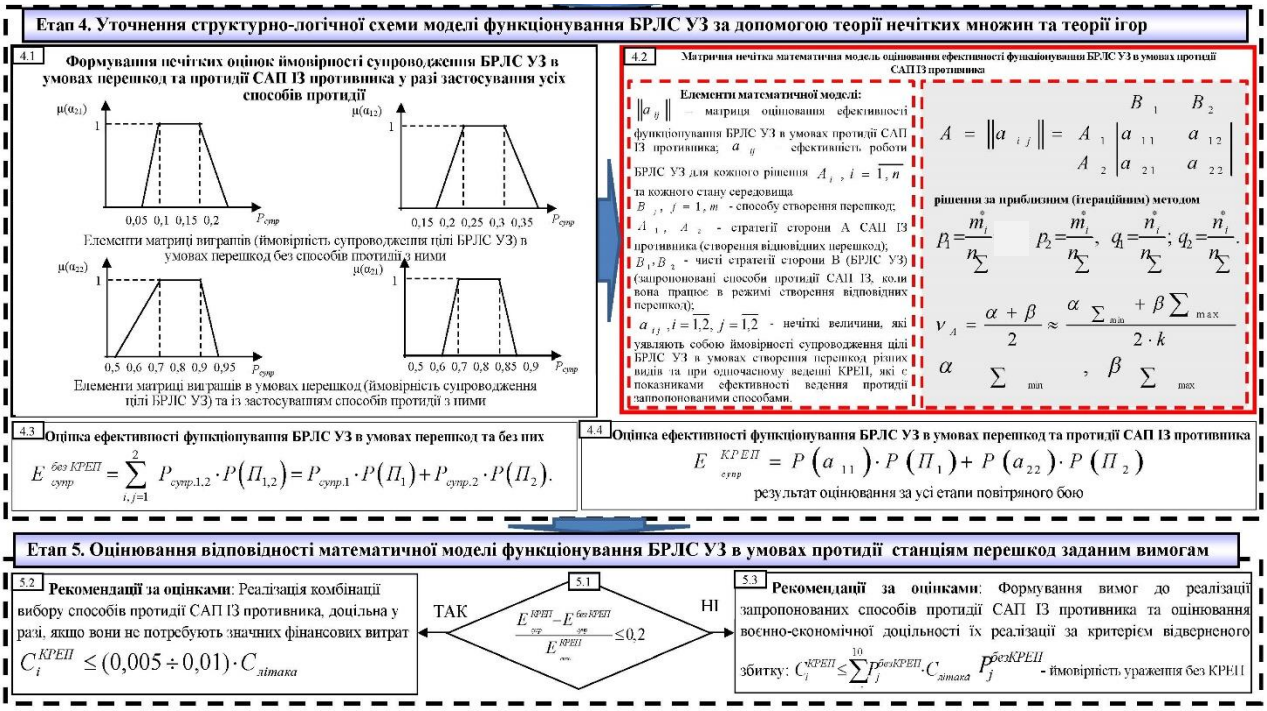

Рисунок 4 – Удосконалений метод етапи 4 – 5

Застосування нечітких шкал оцінювання викликано фактором відсутності чітких оцінок ефективності застосування різних видів перешкод та способів протидії їм, а також природною невизначеністю повітряного бою. У повітряному бою можливі ситуації в яких відомі можливі стратегії застосування САП ІЗ противника, але невідомо, яка з відомих стратегій має місце у даний час, тобто можуть бути відомими дані про типи літаків-винищувачів та засоби протидії, які встановлені на цих літаках та варіанти їх застосування, але невідомо у даний час які види перешкод він зараз створює чи ввімкнена взагалі САП ІЗ на випромінювання та подальші варіанти продовження бою.

У блоці 4.2 (рис. 4) наведена математична модель оцінювання ефективності функціонування БРЛС УЗ в умовах протидії САП ІЗ противника, яка застосовувалась під час розроблення алгоритму та вибору найефективнішій комбінації способів протидії. Було запропоновано математичну модель опису оцінювання ефективності функціонування БРЛС УЗ в умовах перешкод та одночасної протидії станції активних перешкод противника

представити у вигляді нечіткої матричної гри. На нашу думку ця модель є найбільш адекватною для описання такої ситуації щодо БРЛС УЗ літака-винищувача та САП ІЗ противника в умовах здійснення їх активної протидії. Ця математична модель дозволить оцінити ефективність роботи БРЛС УЗ в умовах перешкод та одночасної протидії їм. Запропонована модель має вид матриці ефективності $|a_{ij}|$, де елементами матриці є a_{ij} – нечіткі оцінки ефективності роботи БРЛС УЗ, а саме показники ймовірності супроводження цілі для кожного її рішення щодо застосування способів протидії A_i та кожного стану середовища B_j щодо випромінювання перешкод САП ІЗ.

Результатами рішення матричної гри на кожному етапі запропонованого алгоритму застосування способів протидії САП ІЗ противника є оцінки ефективності БРЛС УЗ на визначених етапах ведення повітряного бою за різних умов застосування БРЛС УЗ, як в умовах перешкод так і в умовах одночасної протидії їм. Загальна оцінка за різного стану середовища повітряного бою розраховується за формулою повної ймовірності розраховано оцінка ефективності функціонування БРЛС УЗ в умовах перешкод без протидії САП ІЗ противника та з урахуванням протидії цим станціям (блоки: 4.3 та 4.4. (рис. 4)).

На п’ятому етапі (рис. 4) проведено оцінювання відповідності удосконаленого методу математичного моделювання заданим вимогам щодо доцільності реалізації запропанованих способів протидії САП ІЗ противника за критерієм воєнно-економічної доцільності та критерієм відверненого збитку.

Висновки. Таким чином удосконалений метод дозволить здійснити обґрунтований опис оцінювання ефективності функціонування БРЛС УЗ в умовах перешкод та одночасної активної протидії станціям перешкод противника, що дозволить за попередніми (рис. 4) розрахунками підвищити ефективність функціонування БРЛС УЗ на 14–33 відсотка, а також враховувати невизначеність ситуації, яка складається під час ведення повітряного бою.

Розроблений алгоритм удосконалює існуючий підхід функціонування бортової РЛС УЗ за показником ймовірності супроводження цілі в умовах застосування запропонованих способів протидії станціям перешкод враховуючи обмеження їх застосування.

Подальші дослідження доцільно спрямувати на надання рекомендацій до впровадження удосконаленого методу під час модернізації винищувачів Повітряних Сил Збройних Сил України з урахуванням різних видів перешкод та появі нових способів протидії.

REFERENCES:

1. Androsov V.A., Kutakhov V.P. Architecture hardware integrovaneho electronic complex // technology, 1996. №. 9. P. 48-52.

2. Semenenko O.M. Analysis of existing methods of active electronic counteraction to onboard stations of active obstacles of individual protection. DNDIA. Kyiv: 2015. №11 (18). P. 120–129.

3. Perunov, Y.M., Matsukevitch V.V., Vasiliev A.A. Foreign electronic warfare / ed. by Perunova Y.M.: 4 kN. KN. 1. The radar system. Moscow: Radio Engineering, 2010. 336 p.

4. Fighter-bomber, the Jaguar. Systems and equipment: [Electron. resource]. – Mode of access: http://aviac.ru/fighters/8-mnogocelevoj-istrebitel-mirazh-f-i.html.

5. Semenenko O.M., Vodchyts O.G., Dobrovolsky Y.B. Method of counterradioelectronic counteraction to the aircraft station of enemy obstacles during its creation of the induced polarization obstacle / ZNP Central Research Institute of the Armed Forces of Ukraine. Kyiv: 2011. №4 (58). P.123–134.

6. Vasilevich L. F. radio-Electronic suppression. Kyiv: KWAI, 1989. 243 p.

7. Multirole fighter Mirage F-I: [Electron. resource]. – Mode of access: http://aviac.ru/fighters/8-mnogocelevoj-istrebitel-mirazh-f-i.html.

8. Lockheed-Boeing-General Dynamics F-22 Raptor, Multirole fighter: [Electron. resource]. – Mode of access: http://www.paralay.com/f22.html.

9. Semenenko O.M., Kablukov O.A., Dobrovolsky Y.B. Analysis of onboard stations of active obstacles of individual protection of enemy aircraft as possible objects of electronic counteraction // Central Research Institute of the Armed Forces of Ukraine. Kyiv: 2019. № 1 (87). P. 98–109.

10. Semenenko OM, Kablukov OA, Chernega VM Ways to create an integrated radar interference system on fighter jets of the Armed Forces of Ukraine. Scientific journal: “Modern Information Technologies in the Field of Security and Defense” №2 (35). Kyiv: 2019. P. 43–48.

11. Handbook of methods of jamming and anti-jamming systems, radar control. Volume 2. Chapter 5. Encyclopedia of anti-jamming methods and techniques of their application. ed Latkina Y. S. – Moscow: vvia im. Zhukovsky, 1987. 620 p.

12. Semenenko O.M., Sorokin D.M., Dobrovolsky Y.B., Kablukov O.A. Recommendations for choosing a mathematical model for evaluating the effectiveness of counterradioelectronic counteraction to the onboard station of enemy interference in air combat. ZNP DNDIA №15 (22). Kyiv: 2019. P. 181–188.

13. Vasilevich L. F. game Theory – Kiev: Our right, 2000. 147 p.

д.воен.н., с.н.с. Семененко О.М., Каблуков О.А., к.т.н., с.н.с. Красник А.В.

УСОВЕРШЕНСТВОВАННЫЙ МЕТОД МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ФУНКЦИОНИРОВАНИЯ БОРТОВЫХ РАДИОЛОКАЦИОННЫХ СТАНЦИЙ УПРАВЛЕНИЯ ОРУЖИЕМ В УСЛОВИЯХ АКТИВНОГО ПРОТИВОДЕЙСТВИЯ СТАНЦИЯМ ПОМЕХ ПРОТИВНИКА

В статье описан усовершенствованный метод математического моделирования функционирования бортовых радиолокационных станций в условиях активного противодействия станциям помех противника.

Проведен анализ современных бортовых радиолокационных систем и станций активных помех как объектов математического моделирования, а также существующих способов активного противодействия бортовым станциям помех противника и методов математического моделирования функционирования бортовых радиолокационных станций.

Сформированы исходные данные по моделированию функционирования бортовых радиолокационных станций в условиях помех и активного противодействия станциям помех противника, приведена выбранная ситуация воздушного боя, которая подлежит математическому описанию.

Были выбраны показатели и критерии, характеризующие эффективность функционирования бортовых радиолокационных станций, основным из которых является ограничение по дальности их использования в зависимости от применяемого способа противодействия. Проведены предварительные расчеты относительно применения указанных способов активного противодействия. Учитывая особенности применения способов активного противодействия станциям помех противника, предложено поделить цикл воздушного боя между самолетами на 5 этапов в зависимости от дальности между ними.

Разработан алгоритм обоснования выбора способов противодействия станциям помех противника с учетом дальности между самолетами для непрерывного сопровождения цели и определены вероятности сопровождения цели с учетом применения различных комбинаций способов противодействия.

Для качественной и полной оценки эффективности функционирования бортовых радиолокационных станций предложено использовать нечеткие множества и теорию игр, с помощью чего построена математическая модель оценки эффективности функционирования бортовых радиолокационных станций в условиях активного противодействия станциям помех противника, которая применялась во время разработки алгоритма и выбора самой эффективной комбинации способов противодействия.

Ключевые слова: методы математического моделирования, алгоритм, модель, станция активных помех индивидуальной защиты, бортовая радиолокационная станция управления оружием, способы контррадіоелектронного противодействия.

Doctor of Military Sciences Semenenko O.M.,
Kablukov O.A., Ph.D. Krasnik A.V.

AN IMPROVED METHOD FOR MATHEMATICAL MODELING OF THE FUNCTIONING OF AIRBORNE RADAR WEAPON CONTROL STATIONS IN THE FACE OF ACTIVE OPPOSITION TO ENEMY INTERFERENCE STATIONS

The article describes an improved method for mathematical modeling of the functioning of the onboard radar in conditions of active opposition to the jammers of the enemy.

The analysis of modern airborne radar systems and stations of active hindrances as objects of mathematical modeling, and existing methods of active resistance to the on-Board jammers of the enemy and methods of mathematical modeling of the functioning of the onboard radar.

Generated input data for the modeling of the performance of airborne radars in noisy environments and active opposition to the jammers of the enemy, given a selected situation of air combat, which is subject to mathematical description.

Were the selected indicators and criteria, characterizing efficiency of functioning of the onboard radar, the main of which is the restriction on the range of their use, depending on the applied method of resistance. Preliminary calculations regarding the application of these methods is active opposition. Given the peculiarities of application of active methods of combating enemy jamming stations, it is proposed to divide the cycle of air combat between aircraft on 5 stages, depending on the distance between them.

The algorithm justify the selection of methods of countering enemy jamming stations taking into account the distance between the aircraft for continuous tracking and determined the probability of target tracking with the use of different combinations of ways of counteraction.

For proper and complete evaluation of the performance of airborne radars is proposed to use fuzzy sets and the theory of games, by means of what a mathematical model of evaluating the performance of airborne radars in the conditions of active opposition to the jammers of the enemy, which was used during development of the algorithm and selecting the most efficient combination of ways to counter.

Keywords: mathematical modeling, algorithm, model, jammer for personal protection, airborne radar weapons control, methods contrarian counter.

УДК 355. 53

к.пед.н., доц. **Толок І.В.** (ВІКНУ)
к.військ.н., доц. **Зайцев Д.В.** (ВІКНУ)
к.військ.н., доц. **Швалючинський В.В.** (НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-06

ВПРОВАДЖЕННЯ ДЕЯКИХ ТЕХНОЛОГІЙ ПОДВІЙНОГО ПРИЗНАЧЕННЯ ПРИ ДИСТАНЦІЙНОМУ ВИКЛАДАННІ ВІЙСЬКОВИХ ДИСЦИПЛІН: ПЕРЕВАГИ ТА ПРОБЛЕМИ

У статті розкриваються деякі технології подвійного призначення при дистанційному викладанні військових дисциплін.

Визначено роль впровадження деяких технології подвійного призначення при дистанційному навчанні в системі підготовки курсантів та офіцерів запасу. Перелічені основні переваги та проблеми щодо розробки й впровадження в освітній процес технологій подвійного призначення при дистанційному викладанні військових дисциплін.

Дистанційне навчання будується відповідно до тієї самої мети та змісту, що і очне навчання, але форми подачі матеріалу і форми взаємодії суб'єктів освітнього процесу між собою суттєво відрізняються. Дидактичні принципи організації дистанційного навчання (принципи науковості, системності і систематичності, активності, принципи розвивального навчання, наочності, диференціації та індивідуалізації навчання) аналогічні очному навчанню, але специфічною є їх реалізація.

Визначені характерні риси дистанційного навчання при викладанні військових дисциплін, а саме: інтерактивність навчання; гнучкість навчання; модульний принцип за відповідною військової спеціальністю; індивідуалізація навчання на основі індивідуального графіку; економічність дистанційного навчання; відсутність проблеми придбання навчальних матеріалів та підручників; інформаційна забезпеченість; паралельність дистанційного навчання; відкритість і об'єктивність оцінки знань громадян; висока самоорганізація громадян.

Визначені деякі підходи вирішення проблем впровадження технологій подвійного призначення при викладання дисциплін: розробка концепції дистанційної освіти за всіма розділами військової підготовки; подальший розвиток і адаптація корпоративної мережі Військового інституту; розробка, розміщення електронних підручників і навчально-методичних матеріалів на сайті Військового інституту та створення бази даних дистанційної освіти; організація взаємодії між всіма учасниками освітнього процесу; створення єдиної корпоративної системи дистанційної освіти і єдиних методичних ресурсів; організація підготовки та підвищення кваліфікації викладачів і технічного персоналу в галузі інформаційних технологій подвійного призначення з врахуванням поетапного переходу у викладанні на стандарти НАТО тощо.

Ключові слова: технології подвійного призначення, дистанційне навчання, дистанційний курс, риси дистанційного навчання, переваги та недоліки технологій подвійного призначення при викладанні військових дисциплін.

Вступ. Підготовка нової генерації офіцерів запасу тактичної ланки з творчим, нестандартним мисленням, спроможним негайно усвідомити завдання, оцінити обстановку, прийняти нестандартне рішення за ситуацією, що склалася, є потребою в комплектуванні Збройних сил в умовах гібридної війни. Реформування системи військової вищої освіти України в напрямку визнання курсанта та громадянина, який навчається за програмою підготовки офіцерів запасу центральною фігурою в навчальному процесі з одночасним розвитком його тактичної грамотності є обґрунтованою необхідністю.

Необхідність у комплектуванні Збройних сил сучасними, навченими за новими стандартами та підходами офіцерами, передбачає також часткову перебудову процесу навчання (впровадження нових форм та способів), кінцевою метою якого має стати максимальне розкриття індивідуальних можливостей та саморозвиток особистості майбутніх офіцерів. Чим це обумовлюється?

По-перше, вимогами кваліфікаційних характеристик до кожної військово-облікової спеціальності, що передбачає визначений рівень знань та вмінь, основні з яких є **знання**: тактичних понять, визначень і термінів; основного озброєння та бойової техніки; основ сучасного загальновійськового бою (тактичних дій); основ управління підрозділами в ході бою; способів вивчення та оцінки місцевості, порядку орієнтування, спостереження; способів і послідовність обладнання одиночних окопів, бліндажів, перекритих щилин, порядок встановлення та подолання мінних полів; основних положень з організації бойового забезпечення підрозділів; озброєння і тактику дій противника та визначених **вмінь**, зокрема: дій у складі малих тактичних груп; в обладнанні окопів й укриттів, здійсненні їх маскування; орієнтування на місцевості та руху за азимутами; у веденні розвідки противника та місцевості, діяти на блокпосту, КПВВ; вести службові переговори на засобах зв'язку; надавати першу медичну допомогу собі та ближньому, евакуювати поранених з поля бою; оформлювати робочу карту офіцера тощо.

По-друге, поетапним переходом на стандарти НАТО, використання нових стандартів підготовки у всіх елементах бойової підготовки, відмова від пострадянських підходів у всіх складових повсякденної діяльності військ.

По-третє, великий обсяг нової (військового характеру) інформації для цивільної молоді, яку достатньо складно опанувати в початковий період навчання під час проведення всіх видів занять з модулів військових дисциплін та недостатньою особистою зацікавленістю в опануванні навчального матеріалу.

Тому, одним з актуальних напрямків покращення рівня теоретичних знань майбутніх офіцерів є впровадження технологій подвійного призначення при дистанційному викладанні військових дисциплін; визначення конкретних навчальних питань на самостійне вивчення (опрацювання), розробка тестових та графічних завдань різноманітного характеру, максимально наближених до сьогоденної обстановки на сході України в тактичній ланці.

Технології подвійного призначення при дистанційній формі навчання фахівці з визначення проблем освітньої діяльності називають однією з пріоритетних освітніх систем XXI століття. Сьогодні на неї зроблена величезна ставка. Актуальність проблеми дистанційного навчання полягає в тому, що результати суспільного процесу, раніше зосереджені в сфері тільки технологій, сьогодні концентруються в інформаційній сфері за умови можливості її подвійного призначення. Виходячи з того, що професійні знання науково-педагогічних працівників старіють дуже швидко, необхідно їх постійно вдосконалювати.

Дистанційна форма навчання дає можливість створення систем масового безперервного самонавчання, загального обміну інформацією. Саме ця система може найбільш адекватно і гнучко реагувати на потреби суспільства щодо підготовки високопрофесійних військових фахівців [1-4]. Можна констатувати, що дистанційне навчання увійшло в XXI століття як найефективніша система підготовки і безперервної підтримки високого кваліфікаційного рівня фахівців всіх сфер та галузей, зокрема, офіцерів тактичного рівня з невеликим досвідом роботи.

Аналіз останніх досліджень і публікацій та постановка задачі. Останнім часом проблемі дистанційного навчання приділяється велика увага в науковій літературі. Дистанційна система навчання знаходиться у центрі уваги наукових кіл, і сучасні тенденції свідчать про подальшу активізацію досліджень у цій сфері. Так, теоретичними, методичними та методологічними проблемами дистанційного навчання займались такі науковці, як В. Кухаренко, С. Вітвицька, С. Лєнков, Ю. Гунченко, С. Шворов, І. Адамова, А. Петров, Ю. Стасєв, С. Сідченко, А. Веремчук, А. Гризо [1-13] та інші.

Зокрема, в роботах [1-3] розкриваються психолого-педагогічної компетентності визначеної категорії студентів (курсантів) при змішаному (очному та дистанційному) викладанні певних дисциплін та ефект, який досягнутий при симбіозі різних видів, форм, способів, методів проведення занять (вправ).

В роботах [8-13] розкриваються аспекти організаційно-методичних підходів до побудови структури центрів дистанційного навчання в системі загальної військової освіти; побудова та використання систем дистанційного навчання з елементами штучного інтелекту; проведений аналіз понятійно-термінологічного апарату з питань розвитку дистанційної освіти та технологій подвійного призначення при викладанні певних дисциплін; визначені структурно-організаційні підходи побудови системи дистанційного навчання в системі військової освіти, а також проблеми і перспективи дистанційного навчання у закладах вищої освіти України.

Крім того, один з авторів статті, в момент її написання, підписаний та проходять навчання з використанням дистанційних технологій, що розроблені при НТУ «ХПІ», керівник курсу – професор Володимир Кухаренко. Платформа – Moodle, назва курсу – «Змішане навчання 2019-2». В основу теоретичної підготовки покладена монографія «Теорія та практика змішаного навчання».

Метою статті є визначення деяких технологій подвійного призначення при дистанційному викладанні військових дисциплін в системі підготовки курсантів, офіцерів запасу та їх впровадження в освітній процес Військового інституту.

Виклад основного матеріалу. Дистанційне навчання – взаємодія педагога та студентів між собою на відстані, яка висвітлює всі притаманні навчальному процесу компонентів (мета, зміст, методи, організаційні форми, засоби навчання) специфічними засобами Інтернет-технологій. Воно передбачає інші засоби, методи, організаційні форми навчання, іншу форму взаємодії викладача і студента, студентів між собою. Дистанційне навчання – це дистанційний освітній процес з використанням дистанційного курсу [1,2,4,9].

Разом із тим, як і будь-яка форма навчання, система дистанційного навчання має такий компонентний склад: цілі, які обумовлені відповідними замовленням для всіх військово-облікових спеціальностей; зміст, передбачений діючими освітніми програмами для майбутніх офіцерів запасу; методи, організаційні форми та засоби навчання.

Дистанційна форма навчання при викладанні навчальних модулів дисципліни Військова підготовка обумовлена специфікою використовуваної технологічної основи (або тільки комп'ютерних телекомунікацій загального доступу на сайті МО України або комп'ютерних телекомунікацій у комплексі з методичними розробками, матеріалами лекцій, групових занять, презентаційним матеріалом, так званою кейс-технологією, яка в свою чергу дозволяє розіграти бойові епізоди, варіанти тактичних дій підрозділів тощо).

Не слід ототожнювати заочне та дистанційне навчання. Їх головна відмінність у тому, що при дистанційному навчанні забезпечується систематична і ефективна інтерактивність. Слід розглядати дистанційне навчання як нову форму навчання і, відповідно, дистанційну освіту (як результат, так і процес, систему) як нову форму освіти, хоча вона не може розглядатися як абсолютно автономна система [1,5,7,9].

Дистанційне навчання будується відповідно до тієї самої мети та змісту, що і очне навчання, але форми подачі матеріалу і форми взаємодії суб'єктів освітнього процесу (викладача та громадянина, що навчається за програмою підготовки офіцерів запасу) між собою суттєво відрізняються. Дидактичні принципи організації дистанційного навчання (принципи науковості, системності і систематичності, активності, принципи розвивального навчання, наочності, диференціації та індивідуалізації навчання) аналогічні очному навчанню, але специфічною є їх реалізація.

Насамперед це пов'язано зі специфікою та можливістю опрацювання того чи іншого матеріалу з модулю Тактична підготовка. Не можна винести на самостійне опанування такий матеріал, який потребує тренування, практичного виконання тих чи інших тактичних прийомів. Так, можна визначити для вивчення конкретні нормативи зі Збірника нормативів з бойової підготовки для Сухопутних військ, але їх виконання повинно здійснюватися тільки за наявності викладача, який визначить недоліки та допоможе досягти необхідних практичних навичок під час проведення тактико-стройових занять.

Характерними рисами дистанційного навчання є [5,6,9]:

- інтерактивність навчання: інтерактивні можливості використовуються в системі дистанційного навчання як системи доставки інформації, дозволяють налагодити і навіть стимулювати зворотний зв'язок, забезпечити діалог і постійну підтримку, які не можливі в більшості традиційних систем навчання;

- гнучкість навчання майбутніх офіцерів, що одержують дистанційну освіту, у виборі місця і часу навчання. Громадяни мають можливість не відвідувати навчальних занять, а навчаються у зручний для себе час та у зручному місці;

- в основу програми дистанційної освіти покладається модульний принцип, що дозволяє з набору незалежних курсів-модулів сформувати навчальну програму, яка відповідає вимогам Замовника та кваліфікаційним характеристикам випускника за відповідною військової спеціальністю;

- індивідуалізація навчання, яка дозволяє реалізувати для групи громадянин індивідуальну навчальну програму й індивідуальний навчальний план. Можна самостійно вибирати послідовність вивчення тем навчальних модулів дисципліни Військова підготовка на основі індивідуального графіку;

- економічність дистанційного навчання знаходить прояв у ефективному використанні навчальних площ та технічних засобів, концентрованому й уніфікованому представленні інформації, використанні і розвитку комп'ютерного моделювання, що може призвести до деякого зниження оплати за навчання за рахунок зменшення кількості науково-педагогічних працівників;

- відсутність проблеми придбання навчальних матеріалів та підручників; використання в освітньому процесі нових досягнень інформаційних технологій, які сприяють входженню громадянина до світового інформаційного простору, що забезпечує технологічність навчання;

- інформаційна забезпеченість дистанційного навчання модулю Тактична підготовка характеризується тим, що громадяни отримують доступ до комплекту необхідних навчальних матеріалів у сучасному електронному вигляді безпосередньо з серверу закладу вищої освіти, де вони навчаються, інших закладів вищої освіти та Інтернет-ресурсів. Сучасні комп'ютерні телекомунікації здатні забезпечити передачу знань і доступ до різноманітної навчальної інформації на рівні, а іноді й набагато ефективніше, ніж традиційні засоби навчання;

- якість дистанційної освіти має бути високого рівня, не поступатися якості очної форми навчання. Це досягається шляхом підготовки дидактичних засобів навчання, до розробки яких залучаються науково-педагогічні працівники кафедри тактики та загальновійськової підготовки та використовуються сучасніші навчально-методичні матеріали з врахуванням досвіду участі Сухопутних військ на сході України;

- паралельність дистанційного навчання – вона здійснюється одночасно з професійною діяльністю або з навчанням за іншим напрямом підготовки, тобто без відриву від навчання на основному факультеті ЗВО або іншого виду діяльності. Також з'являється можливість одночасного навчання в українському та зарубіжному ЗВО;

- відкритість і об'єктивність оцінки знань громадян, її незалежність від викладача за деякими темами, оскільки використовуються сучасні комп'ютерні технології і відповідні програми виставлення оцінок за шкалою ЄКТС;

- висока самоорганізація громадян, за якою підвищується творчий і інтелектуальний потенціал, прагнення до здобуття знань у військовій сфері, уміння взаємодіяти з комп'ютерною технікою і опанування новітніми інформаційними технологіями.

Основні проблеми організації дистанційної форми навчання з аналізом [1-3,6,7], на думку авторів, криються в наступному.

Ефективність дистанційних технологій подвійного призначення безпосередньо залежить від тих викладачів, хто веде роботу з громадянами в Інтернет-просторі. Це повинні бути викладачі з універсальною підготовкою, які володіють сучасними педагогічними та інформаційними технологіями, психологічно готові до роботи з майбутніми офіцерами у новому навчально-пізнавальному мережевому середовищі, спроможними самостійно

оволодіти та опанувати зміни за стандартами НАТО, особливо стосовно нових тактичних знаків, позначень та алгоритмом прийняття рішення.

Інша проблема – інфраструктура інформаційного забезпечення громадянина в мережах. Питання про те, якою має бути структура і композиція навчального матеріалу, вирішує конкретний військовий заклад вищої освіти та кафедра, яка здійснює наповнення дистанційного курсу.

Певною проблемою при створенні дистанційного курсу модулю Тактична підготовка є недосконаліть методик створення і використання дистанційних курсів в освітньому процесі на основі сучасних педагогічних, інформаційних й комунікаційних технологій на факультеті післядипломної освіти. Це завдання вирішується перспективно викладачами і розробниками визначених дистанційних курсів, які повинні професійно володіти всіма сучасними інноваційними технологіями створення електронного контенту. Нажаль, с цим є певні проблеми у зв'язку з тим, що базова підготовка викладачів факультету, за специфіки перебування 100% НПП на військовій службі, не передбачала масове використання електронно-обчислювальної техніки й інформаційних технологій.

Інша проблема, що може бути визначена, це психолого-педагогічна проблема. Вона пов'язана з тим, що кожен викладач кафедри тактики та загальновійськової підготовки за декілька років роботи відшліфовує свої методичні матеріали, які індивідуально розроблені на основі навчального плану, власного педагогічного та науково-методичного досвіду і є його інтелектуальною власністю. Дистанційний курс викладається на WEB-порталі, що перетворює його на загальнодоступний не тільки для громадян, але й інших користувачів. Виникає психологічний бар'єр щодо розробки навчально-методичних матеріалів, оскільки вони можуть бути використані кимось іншим, хто не брав участі в даній розробці. В зв'язку з цим повинна бути вирішена проблема захисту прав на інтелектуальну власність викладача – розробника (автора і тьютора) дистанційного курсу.

Деякі підходи вирішення проблем впровадження технологій подвійного призначення при дистанційному викладанні військових дисциплін у Військовому інституті [4,9,13]:

– розробка концепції дистанційної освіти за всіма розділами військової підготовки;

– подальший розвиток і адаптація корпоративної мережі Військового інституту, доведення пропускної здатності телекомунікаційного каналу (вихід в Internet) до мінімально необхідної, що відповідають вимогам забезпечення навчального процесу дистанційної освіти;

– розробка, розміщення електронних підручників і навчально-методичних матеріалів на сайті Військового інституту та створення бази даних дистанційної освіти;

– організація взаємодії між організаторами та розробниками й науково-педагогічними працівниками щодо наповнення дистанційного курсу навчально-методичними, наочними тощо матеріалами;

– пошук, придбання і впровадження існуючих розробок електронних підручників і навчально-методичних матеріалів в освітній процес;

– створення єдиної корпоративної системи дистанційної освіти і єдиних ресурсів;

– організація підготовки та підвищення кваліфікації викладачів і технічного персоналу в галузі інформаційних технологій дистанційної освіти з врахуванням поетапного переходу у викладанні на стандарти НАТО;

– створення електронної бібліотеки, включення її в корпоративну мережу бібліотек регіону, забезпечення доступу до відкритих бібліотек мережі Internet;

– створення «Системи контролю дистанційного курсу» на одному з факультетів Військового інституту, яка може займатися розробкою єдиних норм, стандартів, здійснювати методичне забезпечення, спрямоване на удосконалення освітнього процесу, а також проводити вибірковий контроль навчальних модулів.

Технічна проблема виникає в зв'язку з недостатністю технічних комунікаційних можливостей користувачів, частковою відсутністю Інтернет-доступу, відсутністю або дорожнечею офіційного програмного забезпечення, та частковою відсутністю персональних

комп'ютерів у громадян, які навчаються за програмою підготовки офіцерів запасу, особливо тих, що переїхали або проживають у сільській місцевості.

І ще одна проблема технічного характеру, це не достатня технічна база аудиторного фонду сучасною комп'ютерною технікою до визначених потреб.

Висновок. Що необхідно врахувати при впровадженні певних технологій подвійного призначення при дистанційному викладанні військових дисциплін? Це: необхідність створення сховищ (баз даних) з відповідних модулів навчання навчальної дисципліни на єдиній платформі; подальше впровадження та використання понятійного апарату дистанційних курсів; розуміння, що взаємодія між викладачами кафедр, курсантом та майбутнім офіцером запасу здійснюється в різний час та в різних місцях; пошук принципів побудови, структури та функціональності мережі ресурсного центру дистанційної навчання на базі Військового інституту; формування таких компетенцій як: комунікативні (безпосереднє спілкування і за допомогою інформаційних засобів), інформаційні (пошук інформації з різних джерел та можливість її опанування), самоосвіти.

У статті також визначені деякі переваги та проблеми впровадження деяких технологій подвійного призначення при дистанційному викладанні військових дисциплін.

Переваги та проблеми впровадження визначених технологій у Військовому інституті охоплюють далеко не повний їх перелік. Кожна з розглянутих проблем, і тим більше методи їх вирішення, вимагають глибокого і всебічного вивчення та можуть бути основою подальшого дослідження технологій подвійного призначення при дистанційному навчанні курсантів та майбутніх офіцерів запасу.

ЛІТЕРАТУРА:

1. І. Адамова, Т. Головачук. Дистанційне навчання: сучасні погляди на переваги та проблеми. Збірник наукових праць Полтавського національного педагогічного університету імені В. Г. Короленка. – 2012 – Вип. 10, С. 3-6. Режим доступу: http://dspace.pnpu.edu.ua/bitstream/123456789/389/1/Adamova.pdf

2. Кухаренко В.М. Теорія і практика змішаного навчання. Монографія. Харків: НТУ «ХПІ», 2016. – 281 с.

3. Толок І.В. Динаміка експериментального дослідження формування психолого-педагогічної компетентності військових фахівців оперативно-тактичного рівня підготовки / І.В. Толок // Вісник Національної академії державної прикордонної служби України. –2012. – Вип.63. – С. 137-142.

4. Толок І.В. Методика проведення експериментального дослідження розвитку психолого-педагогічної компетентності майбутніх магістрів військового управління в системі післядипломної освіти / І.В. Толок // Вісник Національного університету оборони України. –2012. – Вип.6 (31). – С. 175-178.

5. Пометун О.І. Енциклопедія інтерактивного навчання / О.І. Пометун. – К. : 2007. – 144 с.

6. Фіцула М.М. Педагогіка вищої школи: навч. посібн. / М.М. Фіцула. – К. : «Академвидав», 2006. – 352с.

7. Гризо А. А. Впровадження дистанційної форми навчання у навчально-виховний процес при викладанні професійно-орієнтованих дисциплін / А. А. Гризо, С. О. Сідченко, І. С. Добринін // Збірник наукових праць Харківського університету Повітряних Сил – Х. : ХУПС, 2006. Вип. 6 (12). С. 124-127.

8. Стасєв Ю.В. Організаційно-методичні підходи до побудови структури центру дистанційного навчання в системі військової освіти / Ю. В. Стасєв, К. І. Хударковський, С. О. Сідченко, В. В. Бєлімов, А. І. Комишан, А. А. Поселенко // Навчально-виховний процес: методика, досвід, проблеми. Науково-методичний збірник. – Х. : ХУПС, 2006. – № 4 (102). – С. 4-19.

9. Побудова та використання систем дистанційного навчання з елементами штучного інтелекту : монографія / С. В. Лєнков, С. В. Гахович, Ю. О. Гунченко, В. Є. Лукін, С. А. Шворов. – Одеса : Вид-во ВМВ, 2013. - 324 с.

10. Дистанційне навчання : умови застосування. Дистанційний курс : навчальний. І міжн. наук.-практич. конф. Проблеми впровадження дистанційного навчання в освітньому процесі вищих військових навчальних закладів та можливі шляхи їх вирішення посібник / В. М. Кухаренко, Т. О. Олейник, О. В. Рибалко, Н. Г. Сиротинко / за ред. В. М. Кухаренка. – Харків : ХНТУ "ХПІ", "Торсінг", 2001. – 320 с.

11. Іванюк І.В. Формування понятійно-термінологічного апарату з питань розвитку дистанційної освіти. Режим доступу: http://lib.iitta.gov.ua/750.pdf

12. Сідченко С. О. Структурно-організаційні підходи побудови системи дистанційного навчання в системі військової освіти / С. О. Сідченко, В. В. Бєлімов, А. І. Комишан, І. С. Добринін, О. М. Бовкун // Педагогіка і психологія формування творчої особистості: проблеми і пошуки: Збірник наукових праць. – Київ – Запоріжжя, 2006. – Вип. 37. – С. 453-460.

13. А. Веремчук. Проблеми і перспективи дистанційного навчання у ВНЗ. Проблеми підготовки сучасного вчителя № 7, 2013, с. 319-325. Режим доступу: http://nbuv.gov.ua/UJRN/ppsv_2013_7_50

REFERENCES:

1. I. Adamova, T. Golovachuk. Distance Learning: Some Views on Benefits and Challenges. Collection of scientific works of Poltava National Pedagogical University named after VG Korolenko. - 2012 - Issue. 10, pp. 3-6. Access mode: http://dspace.pnpu.edu.ua/bitstream/123456789/389/1/Adamova.pdf

2. Kukharenko V. Theory and practice of blended learning. Monograph. Kharkiv: NTU "KPI", 2016. - p.p. 281.

3. Tolok I. Dynamics of experimental study of the formation of psychological and pedagogical competence of military specialists operationally-tactical level of training / I. Tolok // Bulletin of the National Academy of State Border Guard Service of Ukraine. – 2012. - Issue 63. – p.p. 137-142.

4. Tolok I. Methods of conducting an experimental study of the development of psychological and pedagogical competence of future masters of military management in the system of postgraduate education / I. Tolok // Bulletin of the National University of Defense of Ukraine. –2012. - Issue 6 (31). – p.p. 175-178.

5. Pometun O. Encyclopedia of interactive learning / O. Sweeper. - K., 2007. - 144 p.

6. Fitsula M. Pedagogy of the Higher School: Pupilchnik / M. Fitzula. - K.: Akademvidav, 2006. – 352 p.

7. Gryzo A. The introduction of distance learning in the educational process in teaching vocationally oriented disciplines / A. Gryzo, S. Sidchenko, I. Dobrinin, O. Bovkun, V. Belimov // Proceedings of Kharkiv University of the Air Force - Kharkiv: KhUAF, 2006. - Issue. 6 (12). - p.p. 124-127.

8. Stasev Yu., Khudarkovsky K., Sidchenko S., Belimov V., Komyshan and Poselenko A. (2006). Organizational-methodical approaches to the structure of the center of distance learning in the military education system. *Educational process: methodology, experience, problems. Scientific and methodical collection*. Kharkiv: KhUAF, no. 4 (102), pp. 4-19.

8. Construction and use of distance learning systems with elements of artificial intelligence: monograph / S. Lenkov, S. Gakhovich, Yu. Gunchenko, V. Lukin, S. Shvorov - Odesa: WWII edition, 2013. - p. 324

10. Distance learning: conditions of application. Distance Course: Training. I intern. scientific-practical Conf. Problems of introduction of distance learning in the educational process of higher military educational establishments and possible ways of their solution. V. Kukharenko. - Kharkiv: KhNTU "KPI", "Torsing", 2001. - p. 320.

11. Ivanyuk I. Formation of conceptual and terminological apparatus for development of distance education. Access mode: http://lib.iitta.gov.ua/750.pdf

12. Sidchenko S. Structural and organizational approaches to building a distance learning system in the military education system / S. Sidchenko, V. Belimov, A. Komyshan, I. Dobrinin, O. Bovkun // Pedagogics and psychology of creative personality formation: problems and searches: Collection of scientific works. – K.: Zaporozhye, 2006. - Issue. 37. p.p. 453-460.

13. Veremchuk A. Problems and prospects of distance learning in universities. Problems of preparation of the modern teacher № 7, 2013, p.p. 319-325. Access mode: http://nbuv.gov.ua/UJRN/ppsv_2013_7_50.

к.пед.н., доц. Толок И.В., к.воен.н., доц. Зайцев Д.В., к.воен.н., доц. Швалючинский В.В.

ВНЕДРЕНИЕ НЕКОТОРЫХ ТЕХНОЛОГИЙ ДВОЙНОГО НАЗНАЧЕНИЯ ПРИ ДИСТАНЦИОННОГО ПРЕПОДАВАНИЯ ВОИНСКИХ ДИСЦИПЛИН: ПРЕИМУЩЕСТВА И ПРОБЛЕМЫ

В статье раскрываются некоторые технологии двойного назначения при дистанционном преподавании военных дисциплин. Определена роль внедрения некоторых технологий двойного назначения при дистанционном обучении в системе подготовки курсантов и офицеров запаса. Перечислены основные преимущества и проблемы по разработке та внедрению в образовательный процесс технологий двойного назначения дистанционных технологий при подготовке будущих офицеров запаса.

Дистанционное обучение строится в соответствии с той же целью и содержанием, что и очное обучение, но формы подачи материала и формы взаимодействия субъектов образовательного процесса между собой существенно отличаются. Дидактические принципы организации дистанционного обучения (принципы научности, системности и систематичности, активности, принципы развивающего обучения, наглядности, дифференциации и индивидуализации обучения) аналогичные очному обучению, но специфической является их реализация. Определены характерные черты дистанционного обучения при преподавании военных дисциплин, а именно: интерактивность обучения; гибкость обучения; модульный принцип по соответствующей военной специальности; индивидуализация обучения на основе индивидуального графика; экономичность дистанционного обучения; отсутствие проблемы приобретения учебных материалов и учебников; информационной обеспеченность; параллельность дистанционного обучения; открытость и объективность оценки знаний граждан; высокая самоорганизация граждан.

Определены некоторые подходы к решению проблем внедрения технологий двойного назначения при изложении военных дисциплин: разработка концепции дистанционного образования по всем разделам военной подготовки; дальнейшее развитие и адаптация корпоративной сети Военного института; разработка, размещение электронных учебников и учебно-методических материалов на сайте Военного института и создание базы данных дистанционного образования; организация взаимодействия между всеми участниками образовательного процесса; создание единой корпоративной системы дистанционного образования и единых ресурсов; организация подготовки и повышения квалификации преподавателей и технического персонала в области информационных технологий двойного назначения с учетом поэтапного перехода в преподавании на стандарты НАТО и т.д.

Ключевые слова: технологии двойного назначения, дистанционное обучение, дистанционный курс, черты дистанционного обучения, преимущества и недостатки технологий двойного назначения при изложении военных дисциплин.

Ph.D. Tolok I., Ph.D. Zaitsev D., Ph.D. Shvaliuchynskyi V.

IMPLEMENTATION OF SOME DUAL-TECHNOLOGY TECHNOLOGIES IN REMOTE TEACHING OF MILITARY DISCIPLINES: ADVANTAGES AND PROBLEMS

The article reveals some remote technologies in teaching military training. The role of the introduction of distance learning in the system of training of reserve officers is determined. The main advantages and problems of development and implementation of distance technologies in the education of future reserve officers are listed.

Distance learning is built according to the same purpose and content as face-to-face training, but the forms of material submission and the forms of interaction between the subjects of the educational process differ significantly. The didactic principles of distance learning (principles of scientific, systematic and systematic, activity, principles of developmental learning, clarity, differentiation and individualization of learning) are similar to face-to-face training, but their implementation is specific. The characteristic features of distance learning are defined, namely: interactivity of learning, flexibility of learning; modular principle in the relevant military specialty; individualization of training on the basis of an individual schedule; economics of distance learning; no problem with the acquisition of educational materials and textbooks; parallelism of distance learning; openness and objectivity of citizens' knowledge assessment; high self-organization of citizens.

Some approaches to solving problems of introduction of distance education are defined: development of the concept of distance education in all sections of military training; further development and adaptation of the Military Institute's corporate network; development, placement of electronic textbooks and teaching materials on the website of the Military Institute and creation of a database of distance education; organization of interaction between all participants of the educational process; creation of a single corporate system of distance education and unified resources; organization of training and advanced training of teachers and technical staff in the field of information technology in distance education, taking into account the gradual transition in teaching, including the Tactical Training module, to NATO standards, etc.

Keywords: distance learning, distance course, features of distance learning, advantages and disadvantages of distance learning.

УДК 621.396

к.т.н., доц. **Туровський О.Л.** (ДУТ)
к.т.н., доц. **Кирпач Л.А.** (ДУТ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-07

ВПЛИВ ФАЗОВОЇ НЕСТАБІЛЬНОСТІ ГЕНЕРАТОРІВ НА ПАРАМЕТРИ РОБОТИ СИСТЕМИ СИНХРОНІЗАЦІЇ НЕСУЧОЇ ЧАСТОТИ НА ФОНІ АДИТИВНОГО ГАУСІВСЬКОГО ШУМУ ТА ДОППЛЕРІВСЬКОГО ЗМІЩЕННЯ ЧАСТОТИ

Предметом вивчення в статті є системи фазової синхронізації радіотехнічних пристроїв техніки зв'язку. Метою статті є теоретичні дослідження в напрямку розробки, аналізу та удосконалення відомих і синтез нових схем фазової синхронізації, що характеризуються високою завадостійкістю, точністю і швидкодією при простоті конструкції. Задача, що вирішується – дослідити можливості замкнутої та комбінованої систем синхронізації, щодо роботи в умовах фазової нестабільності генераторів в каналі зв'язку на фоні зовнішнього адитивного гаусівського шуму та допплерівського зміщення частоти. Отримані наступні результати. Проведено аналіз систем синхронізації замкнутого типу при роботі в умовах фазової нестабільності генераторів та показана її невідповідність щодо мінімізації дисперсії фазової помилки та підвищення динаміки під час стеження за несучою частотою. Проведено уточнення процесу синтезу розімкнутого зв'язку в комбінованій системі синхронізації та запропоновані аналітичні залежності, що дозволяють уточнити методику синтезу розімкненого зв'язку для комбінованої системи синхронізації з врахуванням фазової нестабільності генераторів на фоні впливу адитивного гаусівського шуму та допплерівського зміщення частоти. Висновки. Збільшення шумової смуги пропускання пропорційно-інтегруючого фільтра вхідного сигналу системи фазової синхронізації закритого типу до параметрів ідеального фільтра в умовах фазової нестабільності генераторів погіршує динаміку вказаної системи. Для комбінованій системі синхронізації, в умовах фазової нестабільності генераторів, збільшення шумової смуги пропускання вхідного сигналу можна досягнути застосувавши в замкнутому контурі пропорційно-інтегруючий фільтр та здійснивши відповідний підбір параметрів передавальної функції ланки розімкненого каналу. В умовах фазової нестабільності генераторів в комбінованій системі синхронізації шляхом підбором параметрів пропорційно-інтегруючого фільтра можна забезпечити необхідну динаміку системи та досягти збереження оптимального значення дисперсії фазової помилки в ній. Врахування допплерівського шуму в умовах фазової нестабільності генераторів для системи синхронізації замкнутого типу та комбінованої системи синхронізації вимагає зменшення оптимального значення шумової смуги пропусканн .

Ключові слова. синхронізація несучої частоти, система синхронізації замкнутого типу, комбінована система синхронізації, фазова нестабільності генератора, що підлаштовується.

Вступ. Постановка задачі. У різні радіотехнічні пристрої техніки зв'язку, радіолокації і управління а також в пристрої точного магнітного запису широко впроваджені системи фазової синхронізації. Зокрема, в фазокогерентних системах телекомунікації і управління вони застосовуються для відновлення несучої і тактовою частот та для когерентної демодуляції аналогових і цифрових сигналів з кутовою модуляцією [1].

Робота систем синхронізації характеризується впливом ряду збурень та шумів на їх роботу. А саме адитивного флуктуаційного шуму, збурення корисної кутовий модуляції (в разі фільтрації несучої частоти), стрибків фази і частоти та інших. В лініях космічного зв'язку, наприклад, основними зовнішніми збуреннями є адитивний гауссовский шум і допплерівські зміщення частоти.

Поряд з зовнішнім впливом на якість роботи системи фазової синхронізації можуть чинити і внутрішні збурення, основними з яких в фазокогерентних системах є нестабільності генератора, що підлаштовується [2]. Системи синхронізації, що працюють в таких умовах, повинні характеризуватися малою дисперсією фазової помилки і високою швидкодією. Очевидно, що для ефективної роботи радіопристрою в цілому, в тому числі, необхідно

безпосередньо забезпечити високу точність роботи системи фазової синхронізації в сталому і перехідному режимах під впливом як зовнішніх так і внутрішніх збурень [1].

Питання визначення напрямків розробки, аналізу та удосконалення відомих систем синхронізації замкнутого типу (ЗСС) і синтез нових комбінованих схем синхронізації (КСС), що характеризуються високою завадостійкістю, точністю і швидкодією при роботі під впливом як зовнішніх так і внутрішніх збурень є актуальним та своєчасним науковим завданням

Аналіз останніх досліджень і публікацій. Питання аналізу відомих та розробки нових схем систем фазової синхронізації з врахуванням різних джерел збурень розглядались в ряді наукових робіт.

У роботі [3] поданий алгоритм оцінки фазового шуму на основі застосування розрахункових коефіцієнтів розрізненого дискретно - косинусного перетворення та запропоновано ряд реалізацій запропонованого алгоритму. Алгоритм враховує як зміщення несучої частити так і фазовий шум, але оцінку впливу внутрішніх чинників, а саме нестабільність роботи генератора, що підлаштовується на ефективність роботи системи синхронізації запропонований алгоритм не враховує.

У роботі [4] подані результати дослідження КСС з розімкнутим зв'язком при умові впливу зовнішніх збурень. Відмічено, що на відміну від простих КСС, перспективна комбінована система автоматичного регулювання в якій пропонується синтез розімкнутої зв'язку при умові підвищення порядку астатизму має свої особливості, зумовлені специфічними вхідними вузлами замкнутого і розімкнутому каналів управління. В даній роботі відсутня оцінка можливостей таких КСС по підвищенню ефективності роботи з врахуванням нестабільності роботи генераторів в каналі зв'язку.

У роботах [5 - 7] досліджено оптимізацію параметрів фільтра і системи в цілому для класу ЗСС. Отримані результати показали, що ЗСС через властивих їм протиріч не дозволяють в ряді випадків забезпечити необхідну якість роботи. Це особливо відчутно, коли потрібно поліпшити якість системи по двом і більше суперечливим показникам. Вплив нестабільності генераторів в даних роботах не оцінювався.

Великі можливості щодо поліпшення якості систем синхронізації є в класі КСС, які можуть поєднувати принципи регулювання по відхиленню і збуренню, що визначалось в якості перспективних напрямків удосконалення систем синхронізації в роботах [1,8]. В роботі [8] визначена важливість оцінки впливу нестабільності генераторів, ала безпосередньо в ній та в роботі [1] оцінка впливу нестабільності генераторів відсутня

У таких роботах по КСС, як [9, 10], в основному проводиться аналіз динаміки КСС при простому розімкнутому зв'язку, що складається з частотного дискримінатора (ЧД) і різних фільтрів (або без них), без урахування шуму як від зовнішніх так і від внутрішніх джерел.

В роботі [11] відмічено, що вплив нестабільності генераторів може бути суттєвим. Його врахування та мінімізація може бути одним з напрямків підвищення ефективності системи фазової синхронізації. Оцінка впливу вказаної нестабільності в даній роботі не викладена.

Мета і завдання даного дослідження. Завдання оцінки впливу нестабільністю роботи генераторів в каналі зв'язку на ефективності роботи ЗСС та КСС при умові впливу зовнішнього адддитивного гаусівського шуму та допплерівського зміщення частоти, на даний час не вирішувалися та є актуальною науковою задачею, розв'язанню якої присвячена дана стаття.

У загальному випадку фазова модуляція сигналу містить чотири складові [12]:

$$\varphi_{вх}(t) = d(t) + M(t) + \Delta\psi(t) + N(t), \qquad (1)$$

де $d(t)$ – допплерівський зсув на вході;

$M(t)$ – корисна кутова модуляція;

$\Delta\psi(t)$ – нестабільність генераторів.

При когерентному прийомі необхідне точне знання поточної фази несучого коливання. При використанні системи синхронізації як фільтру фази, вхідним сигналом є, у відповідності до виразу (1) сума $d(t)+\Delta\psi(t)$, де $\Delta\psi(t)=\psi_1(t)-\psi_2(t)$, $\psi_2(t)$ - нестабільності генератора, що підлаштовується. Процеси $M(t)$ і $N(t)$ представляють в даному випадку перешкоду.

Дисперсія фазової помилки складається, таким чином, з чотирьох компонентів [13]:

$$\sigma_\varphi^2=\sigma_d^2+\sigma_{\Delta\varphi}^2+\sigma_M^2+\sigma_N^2, \tag{2}$$

кожна з яких відповідно до спектральної теорії визначається наступним чином:

$$\sigma_1^2=\sigma_d^2+\sigma_{\Delta\varphi}^2=\frac{1}{2\pi}\int_{-\infty}^{\infty}\left|W_\varphi(j\omega)\right|^2 G_S(\omega)d\omega, \tag{3}$$

$$\sigma_2^2=\sigma_M^2+\sigma_N^2=\frac{1}{2\pi}\int_{-\infty}^{\infty}\left|W_\varphi(j\omega)\right|^2 G_n(\omega)d\omega, \tag{4}$$

де $W(S)=1-W_\varphi(S)$.

Для даного випадку $G_S(\omega)=G_d(\omega)+G_{\Delta к}(\omega)$, $G_n(\omega)=G_M(\omega)+G_N(\omega)$.

Передавальна функція по помилці ЗСС визначена виразом (5) [4, 14]:

$$W(S)=\frac{1}{1+W_1(S)W_2(S)W_3(S)}=\frac{T_2(S+1)S}{a_0S^2+a_1S+a_2}=\frac{D_{\varphi з0}(S)S^{\nu_з}}{F_з(S)}, \tag{5}$$

отже, передавальна функція $W_3(S)$ буде:

$$W_3(S)=[W_1(S)W_2(S)W_3(S)]/[1+W_1(S)W_2(S)(S)W_3(S)]. \tag{6}$$

З виразів (5), (6) видно, що мінімізувати величину σ_φ^2 можна лише шляхом відповідного підбору параметрів ланок $W_1(S)-W_3(S)$. Оскільки ці параметри входять в характеристичне рівняння ЗСС $F_3(S)=0$, то зміна їх з метою зменшити дисперсію фазової помилки погіршить якість перехідного процесу в системі ЗСС [3].

Визначимо можливості мінімізації дисперсії фазової помилки в КСС і методику синтезу розімкненого зв'язку з умови $\min\sigma_\varphi^2$.

Структурна схема лінійної моделі КСС з додатковою ланкою, прийнята для дослідження, показана на рис. 1.

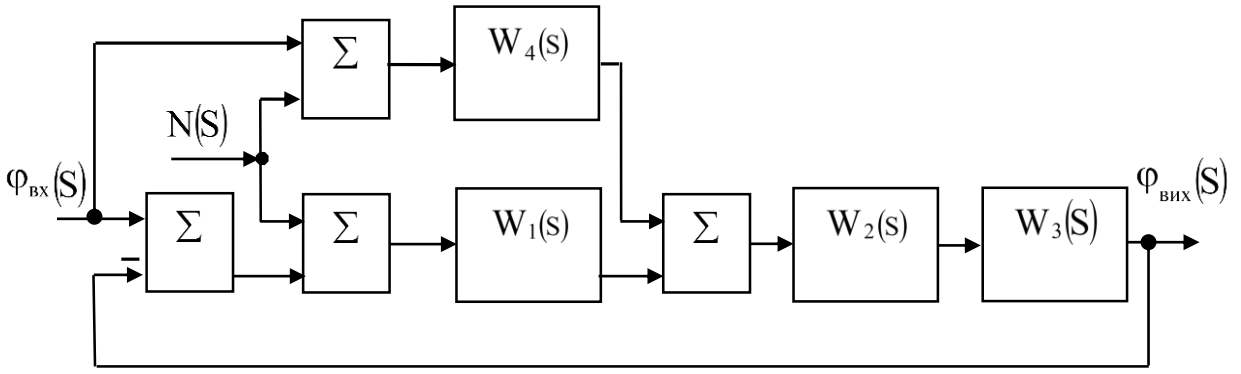

Рис. 1. Структурна схема лінійної моделі комбінованої системи синхронізації з додатковою ланкою

Відповідно до передавальної функції по помилці КСС з виразу (5) знайдемо [4, 14]:

$$W_K(S) = \frac{[D_1(S)D_2(S)F_4(S) + F_1(S)F_2(S)D_4(S)]D_3(S)}{[F_1(S)F_2(S)F_3(S) + D_1(S)D_2(S)D_3(S)]F_4(S)} = \frac{D_K(S)}{F_K(S)}, \quad (7)$$

де $F_K(S) = F_3(S) \times F_4(S)$.

Оскільки в чисельники передавальних функцій КСС, заданих виразами (5), (7) входять поліноми $F_4(S)$, $D_4(S)$ додаткової розімкненої ланки, то шляхом відповідного вибору їх параметрів можна додатково мінімізувати дисперсію фазової помилки. Приймемо до уваги, що поліном $F_4(S)$ входить в характеристичне рівняння КСС у вигляді співмножника, тому корені, що вносяться ним, можна вибрати так, щоб вони не впливали на перехідний процес початкової системи. Якщо вимагати, щоб виконувалася умова:

$$F_4(S) = F_1(S)F_2(S), \quad (8)$$

то передавальні функції КСС по помилці і по вихідному сигналу відповідно будуть:

$$W_{\varphi K}(S) = \frac{F_1(S)F_4(S) + D_3(S)D_4(S)}{F_1(S)F_2(S)F_3(S) + D_1(S)D_2(S)D_3(S)} = \frac{D_{\varphi K}(S)}{F_3(S)}, \quad (9)$$

$$W_K(S) = \frac{[D_1(S)D_2(S) + D_4(S)]D_3(S)}{F_1(S)F_2(S)F_3(S) + D_1(S)D_2(S)D_3(S)} = \frac{D_K(S)}{F_3(S)} \quad (10)$$

У цьому випадку характеристичні рівняння ЗСС і КСС однакові, тобто $F_K(S) = F_3(S)$ і розімкнений зв'язок $W_4(S)$ можна синтезувати тільки з умови $\min \sigma_\varphi^2$.

Розглянемо випадок стеження за несучою частотою на фоні шуму при $d(t) = M(t) = 0$, і порівняємо можливості мінімізації дисперсії фазової помилки в ЗСС і КСС.

Якщо потрібно врахувати компоненту $d(t)$, то необхідно розглядати спектри

$$G_S(\omega) = G_d(\omega) + G_{\Delta\phi}(\omega),\ \ G_n(\omega) = G_M(\omega) + G_N(\omega). \tag{11}$$

Як відомо [2, 15] енергетичний спектр нестабільностей генераторів може бути представлений у вигляді:

$$G_{\Delta\varphi}(\omega) = N_T + (2\pi N_f)/|j\omega|, \tag{12}$$

де N_T, N_f – постійні, що характеризують тепловий шум і шум типу $1/f$ відповідно.

У цьому випадку вираз для дисперсії фазової помилки в ЗСС буде [13]:

$$\sigma^2_{\varphi 3} = \sigma^2_{\Delta\psi} + \sigma^2_N = \frac{r+1}{4r}\frac{N_T}{W_{L3}} + G(r)\frac{N_f}{W^2_{L3}} + \frac{N_0 W_{L3}}{2A_0^2}, \tag{13}$$

де $r = (A_0 K T_1^2)/T_2$, $W_{L3ПФ} = (r+1)/[2T_1(1 + T_1/rT_2)]$ двостороння шумова смуга пропорційно-інтегруючого фільтра (ПІФ), $G(r) \approx 1{,}5$.

З цього виразу видно, що зміна шумової смуги по різному впливає на величину дисперсії фазової помилки, яка викликана нестабільністю генераторів і адитивним шумом.

Якщо взяти похідну по W_{L3} і прирівняти її до нуля, знайдемо $W_{L3ОПТ}$, аналіз якого показує, що мінімум дисперсії фазової помилки отримуємо при включенні в замкнутий контур ідеального фільтра (ІФ) замість пропорційно-інтегруючого фільтра (ПІФ), що, як було показано в [3], погіршує динаміку системи ЗСС.

При $Pc/P = 6\times10^4$, $N_T = 0$, $N_f = 0{,}08$ оптимальними з точки зору $\min\sigma^2_\varphi$ будуть наступні значення r = 7; W_{L3} = 26 Гц. При цьому отримуємо $G(r)$ = 1,6, $\sigma_\varphi = \sqrt{\sigma^2_\varphi} = 1{,}93^\circ$.

Включення в ЗСС ІФ замість ПІФ дещо розширює шумову смугу системи [3]. Дійсно, $W_{L3ІФ} \approx (r+1)/(2T_1)$ і $W_{L3ІФ}/W_{L3ПІФ} = 1 + T_1/(rT_2) \geq 1$.

Таке ж збільшення шумової смуги можна отримати при ПІФ в замкнутому контурі шляхом відповідного вибору параметрів розімкненого каналу.

Визначимо вид і параметри ланки $W_4(S)$ розімкненого зв'язку, що дозволяє отримати КСС з такою ж смугою як ЗСС з ІФ, але при ПІФ в замкнутому контурі, параметри якого можуть бути вибрані з умови забезпечення необхідної якості динаміки системи. Іншими словами будемо синтезувати розімкнений зв'язок з умови:

$$W_{LK} = W_{L3ІФ}, \tag{14}$$

що дозволить оптимізувати систему по мінімуму дисперсії фазової помилки без погіршення динаміки.

На рис. 1 позначені: $W_1(S)$– передавальна функція фазового дискримінатора (ФД), $W_2(S)$ – фільтру (Ф), $W_3(S)$ – генератора, що підлаштовується (ПГ), які мають наступний вигляд [4]:

$$W_1(S) = K_1 + \left(D_1(S)\middle/F_1(S)\right) \qquad W_3(S) = K_3\middle/S = D_3(S)/F_3(S), \tag{15}$$

де $K_1 = A_1 K_{ФД}$;

K_1 – коефіцієнт підсилення ПГ;

S – оператор Лапласа.

Надалі розглядатимемо системи синхронізації з ПІФ в замкнутому контурі з передавальною функцією виду [14]:

$$W_2(S) = (T_1 S + 1) / (T_2 S + 1). \tag{16}$$

Загальний вигляд передавальної функції $W_4(S)$ розімкнутого зв'язку, що задовольняє умові забезпечує ν_k = 1 визначається виразом [4, 14]:

$$W_4(S) = \left(\sum_{i=\nu_3}^{n} K_{4i} S^i\right) \Big/ \left(\sum_{j=0}^{m} T_{4j} S^j\right) = D_4(S)/F_4(S), \tag{17}$$

де ν_3 - порядок астатизму вихідної системи без зв'язку.

Якщо в формули (9), (10) підставити вирази для передавальних функцій ланок системи рис. 1 з (15), (16) і (17), при n=1, отримаємо:

$$W_{\varphi K}(S) = (b_0 S^2 + b_1 S)/(a_0 S^2 + a_1 S + a_2) = D_{\varphi K}(S)/F_3(S), \tag{18}$$

$$W_K(S) = (C_0 S + C_1)/(a_0 S + a_1 S + a_2) = D_K(S)/F_3(S), \tag{19}$$

де $b_0 = T_2$, $b_1 = 1 - K_3 K_4$, $G_1 = A_0 K_1 K_3$, $G_0 = A_0 K_1 T_1 + K_3 K_4$.

Двостороння шумова смуга КСС з ПІФ в замкнутому контурі буде [16].

$$W_{LK} = \frac{1}{2\pi} \int_{-\infty}^{\infty} |W_K(j\omega)|^2 d\omega = W_{L3ПІФ} + \Delta W_L, \tag{20}$$

$$W_L = \frac{\beta^2 r (K_3 K_4)^2 + 2\beta r (K_3 K_4)}{2T_1(1+\beta)}, \tag{21}$$

де $\beta = T_1/(rT_2)$.

З умови (14) знаходимо необхідне значення ΔW_L. З урахуванням виразів ΔW_L ІФ і ΔW_{L3} ПІФ маємо:

$$\Delta W_L = W_{L3ІФ} - W_{L3ПІФ} = \beta(r+1)/[2T_1(1+\beta)]. \tag{22}$$

Порівнюючи вирази (21) і (22), отримаємо наступне рівняння:

$$\alpha_0(K_3K_4)^2 + \alpha_1(K_3K_4)^2 + \alpha_2 = 0, \qquad (23)$$

де $\alpha_0 = \beta^2 r;\ \alpha_1 = 2\beta r;\ \alpha_{21} = -\beta(r+1).$

Якщо розв'язати рівняння (23), знайдемо значення параметра K_4, при якому забезпечується оптимальна передавальна функція КСС з умови $\min\sigma_\varphi^2$ при необхідній якості динаміки системи.

Для наведених вище числових значень маємо $K_4 = 57/K_3$.

Збільшити абсолютні значення коренів характеристичного рівняння можна, наприклад, збільшуючи значення параметра T_2 фільтру. При цьому шумова смуга системи, що дорівнює

$$W_{L\text{ЗПФ}} = \frac{r+1}{2T_1\left[1 + T_1/(rT_2)\right]} = \frac{A_0K(A_0K+1)}{2\left[A_0K + 1/T_2\right]},$$

буде зменшуватися, відхиляючись від оптимального значення. Тому розімкнений зв'язок необхідно вибирати так, щоб компенсувати це відхилення.

Розкривши вираз (21), отримаємо вираз для приросту величини ΔW_L, таким чином:

$$\Delta W_L = \frac{1}{2(mA_0KT_2+1)}(K_3K_4)^2 + \frac{A_0K}{(mA_0K+1/T_2)}(K_3K_4). \qquad (24)$$

З цього виразу видно, що при будь-якому скільки завгодно малому значенні параметра T_2, при збільшенні параметра K_4 розімкненого зв'язку, можна отримати будь-який необхідний приріст шумової смуги [13]. Отже, збільшення абсолютного значення коренів характеристичного рівняння при збереженні оптимального значення дисперсії фазової помилки, обмежене лише фізично досяжним значенням параметра T_2 фільтру.

Якщо необхідно враховувати також допплерівський ефект $(d(t) \neq 0)$, то методика розрахунку розімкненого зв'язку залишається без змін, тільки у формулу (3) в якості $G_S(\omega)$ необхідно підставити суму $G_S(\omega) = G_{\Delta\phi} + G_d(\omega)$.

Допплерівський зсув на вході системи визначається функцією поліноміального типу [12]:

$$d(t) = \varphi_0 + \sum_{r=0}^{N-1}\left(\Omega_r t^{r+1}\right)(r+1). \qquad (25)$$

Якщо прийняти, наприклад, у розрахунку допплерівського зсуву (25) r=0, отримаємо $G_d(\omega) = \varphi_0^2/\omega^2 + \Omega_0^2/\omega^4$. Таким чином, врахування складової $G_d(\omega)$ змінює лише оптимальне значення шумової смуги ЗСС КСС.

Висновки. В роботі розглянуте питання впливу фазової нестабільності генераторів в каналах зв'язку на мінімізацію дисперсії фазової помилки в ЗСС та КСС на фоні адитивного гаусівського шуму та допплерівського зміщення частоти.

Показано, що для ЗСС мінімізація дисперсії фазової помилки шляхом зменшення параметрів передавальних функцій складових ланок системи при фазової нестабільності генераторів погіршить якість перехідного процесу.

Збільшення шумової смуги пропускання пропорційно-інтегруючого фільтра вхідного сигналу ЗСС до параметрів ідеального фільтра погіршує динаміку вказаної системи.

Для КСС, в умовах фазової нестабільності генераторів, збільшення шумової смуги пропускання вхідного сигналу можна досягнути застосувавши в замкнутому контурі ПІФ та здійсненням відповідного підбору параметрів передавальної функції ланки розімкненого каналу.

В умовах фазової нестабільності генераторів КСС шляхом підбором параметрів ПІФ можна забезпечити необхідну динаміку системи та досягти збереження оптимального значення дисперсії фазової помилки в ній. Врахування допплерівського шуму в умовах фазової нестабільності генераторів для ЗСС та КСС вимагає зменшення оптимального значення шумової смуги пропускання.

Запропоновані в роботі аналітичні залежності дозволяють уточнить методику синтезу розімкненого зв'язку для КСС з врахуванням фазової нестабільності генераторів на фоні впливу адитивного гаусівського шуму та впливу допплерівського зміщення частоти.

ЛІТЕРАТУРА:

1. Анализ систем синхронизации при наличии помех / Б.И. Шахтарин. М. : Горячая линия – Телеком, 2016. 360 с.

2. Габриэльян Д.Д., Енгибарян И.А., Сафарьян О.А. Новый метод стабилизации частоты генераторов / *REDS: телекоммуникационные устройства и системы*. 2014. Том. 4. №1. С.30-34.

3. Bhatti J., Noels N. and Moeneclaey M. Low–complexity frequency offset and phase noise estimation for burst–mode digital transmission in Proc / *IEEE PIMRC,* 11-14 September 2011, Toronto. pp.1662–1669.

4. Grosu F., Bîrzu A., Lazar A. and Grosu I. Coupling Systems for a New Type of Phase Synchronization / *Mathematical Problems in Engineering,* Volume 2016, 10 pages.

5. Бойко Ю. М. Оцінювання якісних показників пристроїв синхронізації сигналів засобів телекомунікацій / *Вісник Хмельницького національного університету*. 2015. № 1. С. 204-213.

6. Understanding Digital Signal Processing / Lyons R.G. Boston : Prentice Hall, 2010. 992 p.

7. Scheers B. and Nir V. A Modified Direct-Sequence Spread Spectrum Modulation Scheme for Burst Transmissions / *Military Communications and Information Systems Conference (MCC'2010),* September 27–28, 2010. Wroclaw, Poland, P.366–3673.

8. Salim O., Nasir A., Mehrpouyan H., Xiang W., Durrani S. and Kennedy R. Channel, phase noise, and frequency offset in OFDM systems: Joint estimation, data detection, and hybrid cramer-rao lower bound / *IEEETrans. Commun*. 2014, №62(9), pp. 3311–3325.

9. Бойко Ю. М., Єрьоменко О. І. Аналіз моделей систем синхронізації у цифрових приймачах / *Матеріали XIV міжнародної науково-практичної конференції. Одесська національна академія зв'язку ім. Попова,* 5–10 червня, 2015 р. Одеса, С. 192-194.

10. Кучер Д.Б., Макогон В.П. Відновлення несучої при когерентній демодуляції сигналу з безперервною фазою засобів зв'язку / *Наука і техніка Повітряних Сил Збройних Сил України*. 2013. № 2(11). С. 148-149.

11. Сафарьян О. А. Метод оценки частоты генераторов в условиях непрогнозируемого изменения длительности интервала измерений / *Вестник ДГТУ*. 2014. Т. 14, № 4 (79). С.142-149.

12. Цифровая связь. Теоретические основы и практическое применение. 2-е издание.:Пер. с английского / Б.Скляр. М. :Издательский дом «Вильямс», 2003. 1099 с.

13 Помехоустойчивость приема спектрально-эффективных шумоподобных сигналов : монографія / В.Н. Бондаренко. Красноярск :Сибирский Федеральный Университет, 2015. 160 с.

14. The Art of Electronics : 3rd edition / P. Horowitz and W. Hill. Cambridge :Cambridge University Press, 2015, 1220 p.

15. Поликаровских А. И. Современные опорные генераторы для систем синтеза частот и сигналов / *Вестник Воронежского государственного технического университета*. 2014. Т. 10, № 4, С. 100-108.

16. Nasir A., Durrani S. and Kennedy R. Particle filters for joint timing and carrier estimation: Improved resampling guidelines and weighted bayesian cramer–rao bounds / *IEEE Trans. Commun*. 2012. №60(5). pp.1407–1419.

REFERENCES:

1. Shakhtarin B.I. (2016), "Analiz sistem sinkhronizatsii pri nalichii pomekh" [Analysis of synchronization systems in the presence of interference], Hotline – Telecom, Moscow. 360 p.

2. Gabrielyan D.D., Yengibaryan I.A. and Safaryan O.A. (2014), "Novyy metod stabilizatsii chastoty generatorov" [A New Method for Stabilizing Generator Frequency], REDS: Telecommunication Devices and Systems, Vol. 4, No. 1, pp.30-34.

3. Bhatti J., Noels N. and Moeneclaey M. (2011), "Low–complexity frequency offset and phase noise

estimation for burst–mode digital transmission in Proc", IEEE PIMRC, 11-14 September 2011, Toronto. pp.1662–1669.

4. Grosu F., Bîrzu A., Lazar A. and Grosu I. (2016), "Coupling Systems for a New Type of Phase Synchronization", Mathematical Problems in Engineering, Volume 1, 10 pages.

5. Boyko Y.M. (2015), "Otsinyuvannya yakisnykh pokaznykiv prystroyiv synkhronizatsiyi syhnaliv zasobiv telekomunikatsiy" [Estimation of quality indicators of telecommunication signal synchronization devices], News of the Khmelnitsky National University, No. 1, pp. 204-213.

6. Lyons R.G. (2010) "Understanding Digital Signal Processing", Prentice Hall, Boston. 992 p.

7. Scheers B. and Nir V. A. (2010), "Modified Direct-Sequence Spread Spectrum Modulation Scheme for Burst Transmissions", Military Communications and Information Systems Conference (MCC'2010), September 27–28, 2010, Wroclaw, Poland, pp.366-3673.

8. Salim O., Nasir A., Mehrpouyan H., Xiang W., Durrani S. and Kennedy R. (2014), "Channel, phase noise, and frequency offset in OFDM systems: Joint estimation, data detection, and hybrid cramer-rao lower bound", IEEE Trans. Commun, №62(9), pp. 3311-3325.

9. Boyko Y.M. and Eremenko O.I. (2015), "Analiz modeley system synkhronizatsiyi u tsyfrovykh pryymachakh" [Analysis of models of synchronization systems in digital receivers], Proceedings of the XIV International Scientific-Practical Conference National Academy of Communication, June 5-10 2015, Odessa, pp. 192-194.

10. Kucher D.B. and Makogon V.P. (2013), "Vidnovlennya nesuchoyi pry koherentniy demodulyatsiyi syhnalu z bezperervnoyu fazoyu zasobiv zv″yazku" [Recovery of a carrier with coherent demodulation of a continuous phase signal of communications], Science and Technology of the Air Force of the Armed Forces of Ukraine, No. 2 (11), pp. 148-149.

11. Safaryan O.A. (2014), "Metod otsenki chastoty generatorov v usloviyakh neprognoziruyemogo izmeneniya dlitel'nosti intervala izmereniy " [A method of estimating the frequency of generators in the conditions of unpredictable change in the duration of the measurement interval], DGTU Bulletin, Vol. 14, No. 4 (79). pp.142-149.

12. Sklyar B. (2003), "Tsifrovaya svyaz'. Teoreticheskiye osnovy i prakticheskoye primeneniye" [Digital communication. Theoretical foundations and practical application], Williams Publishing House,. Moscov, 1099 p.

13 Bondarenko V.N. (2015), "Pomekhoustoychivost' priyema spektral'no-effektivnykh shumopodobnykh signalov" [Immunity of reception of spectrally effective noise-like signals], monograph, Siberian Federal University, Krasnoyarsk, 160 p.

14. Horowitz P. and Hill W. (2015), "The Art of Electronics", Cambridge University Press, Cambridge, 1220 p.

15. Polikarovskikh A.I. (2014), " Sovremennyye opornyye generatory dlya sistem sinteza chastot i signalov" [Modern reference generators for frequency and signal synthesis systems], Bulletin of the Voronezh State Technical University, Vol. 10, No. 4. pp. 100-108.

16. Nasir A., Durrani S. and Kennedy R. (2012), "Particle filters for joint timing and carrier estimation: Improved resampling guidelines and weighted bayesian cramer–rao bounds", IEEE Trans. Commun, №60(5), pp.1407–1419.

к.т.н., доц. Туровский О.Л., к.т.н., доц. Кирпач Л.А.

ВЛИЯНИЕ ФАЗОВОЙ НЕСТАБИЛЬНОСТИ ГЕНЕРАТОРОВ НА ПАРАМЕТРЫ РАБОТЫ СИСТЕМЫ СИНХРОНИЗАЦИИ НЕСУЩИХ ЧАСТОТ НА ФОНЕ АДДИТИВНОЙ ГАУССОВСКОЙ ШУМА И ДОППЛЕРОВСКОГО СМЕЩЕНИЕ ЧАСТОТЫ

Предметом изучения в статье является системы фазовой синхронизации радиотехнических устройств техники связи. Целью статьи является теоретические исследования в направлении разработки, анализа и совершенствования известных и синтез новых схем фазовой синхронизации, характеризующихся высокой помехоустойчивостью, точностью и быстродействием при простоте конструкции. Задача, решаемая - исследовать возможности замкнутой и комбинированной систем синхронизации, о работе в условиях фазовой нестабильности генераторов в канале связи на фоне внешнего аддитивного гауссовского шума и доплеровского смещения частоты. Получены следующие результаты. Проведен анализ систем синхронизации замкнутого типа при работе в условиях фазовой нестабильности генераторов и показана ее несоответствие по минимизации дисперсии фазовой ошибки и повышение динамики

при слежении за несущей частотой. Проведено уточнение процесса синтеза разомкнутой связи в комбинированной системе синхронизации и предложены аналитические зависимости, позволяющие уточнить методику синтеза разомкнутой связи для комбинированной системы синхронизации с учетом фазовой нестабильности генераторов на фоне влияния аддитивного гаусовского шума и допплеровского смещения частоты. Выводы. Увеличение шумовой полосы пропускания пропорционально-интегрирующего фильтра входного сигнала системы фазовой синхронизации закрытого типа с параметрами идеального фильтра в условиях фазовой нестабильности генераторов ухудшает динамику указанной системы. Для комбинированной системе синхронизации, в условиях фазовой нестабильности генераторов, увеличение шумовой полосы пропускания входного сигнала можно достичь, применив в замкнутом контуре пропорционально-интегрирующий фильтр и осуществив соответствующий подбор параметров передаточной функции звена разомкнутого канала. В условиях фазовой нестабильности генераторов в комбинированной системе синхронизации путем подбора параметров пропорционально-интегрирующего фильтра можно обеспечить необходимую динамику системы и достичь сохранения оптимального значения дисперсии фазовой ошибки в ней. Учет доплеровского шума в условиях фазовой нестабильности генераторов для системы синхронизации замкнутого типа и комбинированной системы синхронизации требует уменьшения оптимального значения шумовой полосы пропускания.

Ключевые слова: синхронизация несущей частоты, система синхронизации замкнутого типа, комбинированная система синхронизации, фазовая нестабильности генератора, который подстраивается.

Ph.D. Turovsky O.L., Ph.D. Kirpach L.A.

EFFECT OF PHASE INSTABILITY OF GENERATORS ON THE OPERATING PARAMETERS OF A CARRIER FREQUENCY SYNCHRONIZATION SYSTEM AGAINST A BACKGROUND OF ADDITIVE GAUSSIAN NOISE AND A DOPPLER FREQUENCY SHIFT

The article deals with the systems of phase synchronization of radio engineering devices of communication technology. The purpose of the article is theoretical research in the direction of development, analysis and improvement of known and synthesis of new phase synchronization circuits, characterized by high noise immunity, accuracy and speed with simplicity of design. The problem is solved to investigate the possibilities of closed and combined synchronization systems for operation under conditions of phase instability of generators in a communication channel against the background of external additive Gaussian noise and Doppler frequency shift. The following results were obtained. The analysis of closed-type synchronization systems during operation under the conditions of phase instability of generators is carried out and its inconsistency is shown in order to minimize the phase error variance and increase the dynamics during carrier frequency monitoring. The process of synthesis of open communication in the combined synchronization system is refined and analytical dependences are offered, which allow to refine the technique of synthesis of open communication for the combined synchronization system with regard to the phase instability of the generators against the background of the influence of the adducts. Conclusions. Increasing the noise bandwidth of the proportional-integrating filter of the closed-loop phase-in-phase synchronization system to the parameters of the ideal filter impairs the dynamics of the specified system. For the combined synchronization system, in the conditions of phase instability of the generators, an increase in the noise bandwidth of the input signal can be achieved by applying a closed-loop proportional-integrating filter and by making appropriate selection of parameters of the transfer function of the link of the open channel. In the conditions of phase instability of the generators in the combined system of synchronization by selecting the parameters of the proportional-integrating filter, it is possible to provide the necessary dynamics of the system and to achieve the optimal value of the dispersion of the phase error in it. Taking into account Doppler noise under conditions of phase instability of generators for a closed-type synchronization system and a combined synchronization system requires a reduction of the optimal value of the noise bandwidth.

Keywords. carrier frequency synchronization, closed-type synchronization system, combined synchronization system, phase instability of the adjustable generator.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.891

к.т.н., доц. **Джулій В.М.** (ХмНУ)
к.т.н., доц. **Бойчук В.О.** (ХмНУ)
к.т.н., доц. **Тітова В.Ю.** (ХмНУ)
д.т.н., с.н.с. **Сєлюков О.В.** («Укрспецконсалтинг»)
к.т.н., с.н.с. **Мірошніченко О.В.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-08

МОДЕЛІ І МЕТОДИ ЗАХИСТУ ВІД ЗАГРОЗЛИВИХ ПРОГРАМ ІНФОРМАЦІЙНИХ СИСТЕМ

У статті запропоновано підхід до розвитку методів захисту від загрозливих програм в сучасних інформаційних системах, що складається в розробці методів захисту, заснованих на реалізації контролю доступу до файлів по їх типам, які можуть бути ідентифіковані розширеннями файлів, що істотно перевершують відомі методи антивірусного захисту, як по ефективності захисту, так і в міру впливу на завантаження обчислювальних ресурсів інформаційної системи.

Показано, що найбільш актуальними для захисту є виконувані бінарні і скриптові файли і про те, що дані класи шкідливих програм передбачають обов'язкове збереження загрозливого файлу на жорсткому диску перед його виконанням (читанням). Це дозволило зробити висновок щодо того, що захист від загрозливих програм може будуватися реалізацією контролю (розмежування прав) доступу до файлів.

Запропоновано загальний підхід до реалізації захисту від загрозливих програм, заснований на реалізації контролю доступу до файлів по їх типам, які можуть бути ідентифіковані розширеннями файлів. Можливість використання подібного підходу обґрунтовано проведеним дослідженням засобів захисту.

Методи захисту від загрозливих програм дозволяють захистити інформаційну систему, як від завантаження, так і від виконання бінарних і скриптових загрозливих файлів, що відрізняються можливістю врахування розташування виконуваних файлів, можливістю адміністрування при працюючій системі захисту, можливістю контролю модифікації об'єктів доступу, перейменування об'єктів доступу, можливістю захисту від скриптових загрозливих програм, в тому числі з урахуванням можливості наділення загрозливими властивостями інтерпретаторів (віртуальних машин).

Розроблено моделі контролю доступу, що дозволили на побудованих матрицях доступу сформулювати вимоги до побудови безпечної системи, виконання яких запобігає витоку заданих прав доступу суб'єктів до об'єктів.

Ключові слова: загрозливі програми, комп'ютерна безпека, інформаційна система, контроль доступу, об'єкт доступу, суб'єкт доступу.

Вступ. Однією з ключових сучасних проблем забезпечення комп'ютерної безпеки є необхідність ефективної протидії загрозливим програмам. При цьому необхідно враховувати, що це можуть бути, як самостійні програми, покликані здійснювати відповідні несанкціоновані дії, так і цілком легальні, санкціоновано використовувані додатки, що наділяються в процесі роботи загрозливими властивостями. На сьогоднішній день для вирішення розглянутих задач використовуються різноманітні способи сигнатурного і поведінкового аналізів, покликаних запобігти можливості несанкціонованого впровадження та запуску загрозливих програм на ресурси, що захищаються. Однак існуюча статистика зростання загрозливих програм дозволяє припустити про низьку ефективність методів вирішення найбільш актуальних сучасних завдань захисту інформації. Більшість сучасних

методів захисту від загрозливих програм зводиться до виявлення таких, або до спроби запобігання атаки з боку присутньої на комп'ютері загрозливої програми.

Технологія виявлення загрозливих програм була заснована на використанні сигнатур - ділянок коду, однозначно ідентифікують ту чи іншу загрозливу програму. У міру того, як еволюціонували загрозливі програми, ускладнювалися і розвивалися технології їх детектування. Умовно роботу антивірусних програм можна розділити на збір даних для виявлення загрозливих програм і якийсь механізм, що визначає на основі зібраної інформації загрозлива ця програма чи ні. Узагальнюючи, можна виділити наступні способи: робота з файлом як з масивом байтів; емуляція коду програми; запуск програми в «пісочниці» (sandbox2) (а також використання близьких за змістом технологій віртуалізації); моніторинг системних подій; пошук системних аномалій.

Сучасні антивірусні засоби захисту, як правило, одночасно реалізують і технічний, і аналітичний компоненти, засновані на сукупності методів захисту. При цьому, незважаючи на те, що сигнатурний метод застарів, він на сьогодні залишається в захисних продуктах і рекламується, як частина стійкої бізнес моделі. При цьому не варто забувати, що створення сигнатур - ручний процес, тому розробка нових сигнатур і випуск оновлень для користувача може займати від декількох годин до доби. Таким чином, сигнатурні механізми не рятують від нових, що не потрапили в базу, погроз. У зв'язку з ручним складанням сигнатур вони дають помилкові спрацьовування. База сигнатур зростає, і, в зв'язку з цим, робота з сигнатурами накладає все більші витрати на ресурси комп'ютера.

Як показує практика, евристичний метод справляється лише в невеликій кількості випадків, тому цей підхід також не вирішує завдання захисту від запуску загрозливих програм. При сучасних методах приховування і шифрування виконуваних файлів виявити нові загрози такими методами практично неможливо.

Постановка задачі. На підставі проведених досліджень можемо зробити наступний важливий висновок - всі дослідження ефективності антивірусних засобів захисту зводяться до оцінювання ефективності детектування загрозливих програм, причому на деяких відомих кінцевих наборах, що вже ставить під сумнів коректність подібних оцінок. Разом з тим, систему створення і виявлення загрозливих програм можна розглядати, як стохастичну систему, яка характеризується відповідними інтенсивностями і можливостями. Саме застосування такого підходу дозволить виявити і кількісно коректно оцінити основні характеристики системи антивірусного захисту - системи захисту від загрозливих програм. Виходячи з вище викладеного, в рамках проведеного дослідження ставиться задача моделювання системи антивірусного захисту з використанням математичного апарату теорії масового обслуговування, визначення і розрахунку основних характеристик з подальшою оцінкою реальної ефективності відомих методів захисту від загрозливих програм. Інший висновок, зроблений в результаті проведених досліджень, полягає в тому, що завдання захисту від загрозливих програм апріорі розглядається експертами з безпеки в якості актуальної. В рамках проведеного дослідження ставиться задача розробки математичної моделі, що дозволяє кількісно оцінювати актуальність загрози в інформаційній системі, що може служити обґрунтуванням рішення задачі захисту від тієї чи іншої загрози.

Проведене дослідження існуючих підходів до оцінки ефективності методів і засобів захисту від загрозливих програм, в результаті якого зроблені висновки про неможливість з використанням відомих підходів ні кількісно оцінити актуальність окремої загрози для інформаційної системи в цілому (з урахуванням безлічі інших потенційних загроз), в тому числі загрози занесення і запуску загрозливих програм, ні кількісно оцінити основні стохастичні характеристики безпеки системи від загрозливих програм. В результаті чого сформульована задача розробки відповідних математичних моделей і наступного проведення на них досліджень, що дозволять отримати необхідні кількісні оцінки.

Основна частина. Розглянемо ефективність антивірусного програмного забезпечення (ПЗ), що використовує бази сигнатур, евристик або поведінки загрозливих програм.

Представимо виявлення нової загрозливої програми як систему масового обслуговування, де прилад - аналітик, заявка - нова загрозлива програма. В результаті отримуємо багатоканальну СМО з необмеженою чергою M/M/C. Математична модель для розрахунку ефективності, яка може будуватися в залежності від розв'язуваних завдань:

$$p_0 = f(\lambda, \mu) , \tag{1}$$

де μ - інтенсивність випуску нових сигнатур і евристик; λ - інтенсивність виявлення нових загрозливих програм. Дані величини задаються виходячи з існуючих статистик. Розглянемо стаціонарну роботу системи:

$$\frac{\rho}{C} < 1 , \tag{2}$$

де ρ - інтенсивність навантаження, що дорівнює відношенню інтенсивності надходження заявок до інтенсивності обслуговування:

$$\rho = \frac{\lambda}{\mu}, \tag{3}$$

C - кількість обслуговуючих приладів. Із формул (2) і (3), отримуємо нерівність:

$$\frac{\lambda}{\mu \cdot C} < 1 . \tag{4}$$

Інтенсивність обслуговування і кількість приладів ми задаємо виходячи із загальних відомостей про роботу антивірусних компаній. Знаючи ці параметри, з формули (4) отримуємо інтервал, яким обмежується інтенсивність надходження заявок в умовах стаціонарної роботи системи:

$$\lambda < \mu \cdot C . \tag{5}$$

Для початку розрахуємо ймовірність (p_0) того, що всі аналітики виявляться вільними і в системі не виявиться жодної заявки. Імовірність p_0 - характеристика актуальності загрози, чим ймовірність менше, тим загроза актуальніша.

Імовірність p_0 того, що система готова до експлуатації в будь-який момент часу і відсутні не виявлені сигнатури, розраховується за формулою:

$$p_0 = \left(\sum_{n=0}^{C} \frac{\left(\lambda/\mu\right)^n}{n!} + \frac{\left(\lambda/\mu\right)^{C+1}}{C!\left(C - \frac{\lambda}{\mu}\right)} \right)^{-1} . \tag{6}$$

Розрахуємо, яка буде довжина черги виходячи з статистичної інтенсивності надходження заявок. Розглянемо випадок стаціонарної роботи системи:

$$\frac{\rho}{C} < 1 . \tag{7}$$

З формули (7) і (3), отримуємо:

$$\mu > \frac{\lambda}{C} . \tag{8}$$

Виходячи, що $\mu = 1/ T_{обс}$, отримуємо з формули (8) обмеження на середній час обслуговування заявки:

$$T_{обс} < \frac{C}{\lambda} . \tag{9}$$

Виходячи з формули (5), будемо задавати $T_{обс}$ і розрахуємо середню довжину черги:

$$L_{дч} < \frac{\rho^{C+1} p_0}{C \cdot C!\left(1 - \rho/C\right)^2} . \tag{10}$$

Середній час обслуговування заявки розраховується за формулою:

$$T_{обс} = \frac{L_{дч}}{\lambda} . \quad (11)$$

Припускаючи, що система працює в стаціонарному режимі, задаючи інтенсивність надходження заявок і кількість аналітиків, отримали систему близьку до нестаціонарної, так як в крайніх точках черга різко зростає. Це свідчить про низьку ефективність існуючих антивірусних програм і про відсутність необхідного рівня захисту.

На підставі введеної класифікації загрозливих програм, зроблено висновок про потенційну можливість реалізації захисту від загрозливих програм на основі контролю (розмежування) доступу до ресурсів, зокрема, до файлових об'єктів. Пропонується будувати захист від загрозливих програм на основі дискреційної моделі розмежування доступу до об'єктів файлової системи. Дискреційний принцип управління доступом будемо розглядати як примусове управління потоком інформації, виключаючи власника об'єкта доступу. Вихідною вимогою для заданої моделі є те, що ніякий користувач не зможе вивести систему з безпечного стану. В рамках цієї моделі система обробки інформації представляється у вигляді сукупності активних сутностей - суб'єктів (множини *S*), які здійснюють доступ до інформації, пасивних сутностей - об'єктів (множина *O*), що містять інформацію яка захищається, і кінцевої множини прав доступу $R-\{r_1, ..., r_n\}$, що означають повноваження на виконання відповідних дій (наприклад, читання, запис, виконання). Рядки матриці відповідають суб'єктам, а стовпці - об'єктам. Будь-яка комірка матриці $M[S,O]$ містить набір прав суб'єкта *S* до об'єкта *O*, що належать множині прав доступу *R*. Множина режимів доступу залежить від типу аналізуємих об'єктів. До режимів доступу відносяться: читання, запис, виконання.

Формальний опис моделі складається з наступних елементів: кінцевий набір вихідних суб'єктів $S=\{S_1, ..., S_n\}$; кінцевий набір вихідних об'єктів $O=\{O_1, ..., O_n\}$; кінцевий набір прав доступу $R-\{r_1, ..., r_n\}$ вихідна матриця доступу *M*, що містить права доступу суб'єктів до об'єктів.

Для аналізу безпеки системи захисту, що реалізує дискреціонну політику безпеки, будемо використовувати модель Харрісона - Руззо - Ульмана. Для заданої моделі початковий стан $Q_0=(S_0,O_0,M_0)$ є безпечним щодо права *r*, якщо не існує застосовної до Q_0 послідовності команд, в результаті якої право *r* буде занесено в комірку матриці *M*, в якій воно було відсутнє в стані Q_0. Іншими словами це означає, що суб'єкт ніколи не отримає право доступу *r* до об'єкта, якщо він не мав його на початку. Якщо ж право *r* виявилося в комірці матриці *M*, в якій воно на початку було відсутнє, то стався витік критичного права *r* по об'єкту доступу.

Для запобігання несанкціонованого завантаження і створення загрозливої програми необхідно заборонити модифікацію, видалення і створення подібних існуючих файлів, які підпадають під зазначені розширення. Для скорочення списку контрольованих об'єктів доступу слід дозволяти виконувати (бінарні файли) і читати (скриптові) тільки обмежений набір існуючих об'єктів, які теж задаються виходячи з їх розширень. В результаті основна суть пропонованого підходу захисту від загрозливого ПЗ полягає в тому, що: об'єкти доступу визначаються по їх розширенням (виконувані, системні або інформаційні); виключається будь-яка можливість несанкціонованої модифікації заданих об'єктів; виключається будь-яка можливість несанкціонованого видалення заданих об'єктів; виключається будь-яка можливість створення заданих об'єктів; тільки задані об'єкти доступу дозволяється виконувати.

Згідно класифікації загрозливих програм (ЗП), вони поділяються на бінарні і скриптові виконані файли і макро-програми. Перший і другий типи ЗП є файлами з певними розширеннями, відповідно можуть виступати в якості об'єктів доступу в пропонованому

підході захисту. Розглянемо варіант роботи в інформаційній системі, коли у всіх користувачів однакові права доступу, включаючи системних користувачів і адміністратора. В якості суб'єктів доступу виступатимуть користувачі системи $S_i : S = \{S_1, \ldots, S_k\}$. В якості суб'єкта доступу може бути будь-який користувач, у тому числі з правами системи - користувач System. Об'єкти доступу діляться на виконувані, системні та інформаційні: $O = \{ O_{вик1}, \ldots, O_{викq}, O_{сист1}, \ldots, O_{систm}, O_{інф1}, \ldots, O_{інфn} \}$. Це дозволяє захищати як від вже відомих загрозливих програм, так і від нових. Кінцевий набір прав доступу включає читання, виконання і запис: *R* = {*Чт, В, Зп*}.

Права доступу призначаються суб'єктам доступу, а не як атрибути об'єктів доступу. Використовується дозвільна політика доступу, тобто все що явно не дозволено, то заборонено. Згідно з основною ідеєю пропонованого підходу захисту від загрозливого ПЗ, пропонований метод полягає в наступному: для виконуваних об'єктів доступу (ОД) дозволяється читання і виконання; для системних ОД дозволяється тільки читання; для інформаційних ОД дозволяється читання і запис; все інше забороняється.

Виходячи із заданих параметрів, отримуємо наступну матрицю доступу (МД):

$$M = \begin{array}{c} \\ S_1 \\ \ldots \\ \ldots \\ S_k \end{array} \begin{array}{c} \begin{array}{ccc} O_{вик1}, \ldots, O_{викq} & O_{сист1}, \ldots, O_{систm} & O_{інф1}, \ldots, O_{інфn} \end{array} \\ \begin{bmatrix} Чт, В & Чт & Чт, Зп \\ & \ldots & \\ & \ldots & \\ Чт, В & Чт & Чт, Зп \end{bmatrix} \end{array}.$$

У даній МД критичний витік права доступу «Запис» і «Виконання». Оскільки послідовність дій, в результаті яких відбудеться витік права, генерує суб'єкт доступу (користувач), то його дії не зможуть привести до витоку права доступу. В тому числі при даній політиці виключена сутність «Власник», відповідно користувач, який створив новий об'єкт, не зможе наділити правом доступу «Запис» інших користувачів. При створенні нового СД також неможливий витік права доступу, так як розмежування застосовні до будь-якого користувачева і не важливі ні його ім'я, ні його SID.

Перевагою даного методу є те, що неможливо зберегти або запустити загрозливе ПЗ.

Недоліком даних розмежувань є той факт, що дозволено виконувати всі виконувані файли, незалежно від їх розташування. У даній ситуації не можемо розмежовувати доступ до тих ресурсів, зміну яких ми не можемо проконтролювати. Другим недоліком є те, що Адміністратор системи не зможе встановлювати нове програмне забезпечення або оновлювати існуюче.

Для виключення недоліку, пов'язаного з неможливістю розмежовувати доступ до тих ресурсів, зміну яких ми не можемо проконтролювати, введемо додаткову вимогу для розташування виконуваних файлів. Можливі два способи обмеження: системні каталоги «%ProgramFiles%» і «%windir%»; системний диск, наприклад, «C:\». В якості суб'єктів доступу виступатимуть користувачі системи $S_i : S = \{S_1, \ldots, S_k\}$. ОД залишаються незмінними: $O = \{ O_{вик1}, \ldots, O_{викq}, O_{сист1}, \ldots, O_{систm}, O_{інф1}, \ldots, O_{інфn} \}$. Кінцевий набір прав доступу включає в себе читання, виконання і запис: *R* = {*Чт, В, Зп*}. Введемо зміни для завдання об'єкта доступу: дозволити читання і виконання тільки тих виконуваних ОД, які вже знаходяться на системному диску; дозволити тільки читання для системних ОД; дозволити читання і запис для інформаційних ОД; все інше забороняється.

Виходячи із заданих параметрів, отримуємо наступну матрицю доступу:

$$M=\begin{array}{c} \\ S_1 \\ \dots \\ \dots \\ S_k \end{array}\begin{array}{c} \begin{array}{ccc} O_{вик1}, \dots, O_{викq} & O_{сист1}, \dots, O_{систm} & O_{інф1}, \dots, O_{інфn} \end{array} \\ \begin{bmatrix} Чт, В & Чт & Чт, Зп \\ \dots & \dots & \\ \dots & \dots & \\ Чт, В & Чт & Чт, Зп \end{bmatrix} \end{array}.$$

Перевагою даного методу є контроль всіх виконуваних файлів, в тому числі на зовнішніх пристроях і в мережевих каталогах. Недоліком залишається той факт, що Адміністратор системи не зможе встановлювати нове програмне забезпечення або оновлювати існуюче.

Для усунення недоліку, пов'язаного з відсутністю можливості установки нового програмного забезпечення або відновлення існуючого розглянемо варіант, коли Адміністратору інформаційної системи дозволено додатково встановлювати програмне забезпечення. Вводимо додатковий суб'єкт доступу Адміністратор і отримуємо $S_i : S = \{S_1, \dots, S_k, A\}$. Об'єкти доступу залишаються незмінними: $O = \{ O_{вик1}, \dots, O_{викq}, O_{сист1}, \dots, O_{систm}, O_{інф1}, \dots, O_{інфn} \}$. Кінцевий набір прав доступу включає в себе читання, виконання і запис: $R = \{Чт, В, Зп\}$.

Даний метод захисту полягає в наступному:

- для суб'єкта доступу Адміністратор: дозволити читання, запис (установка) і виконання виконуваних ОД; дозволити читання, запис (установка) системних ОД; дозволити читання і запис інформаційних ОД; все інше забороняти.

- для всіх інших суб'єктів доступу: дозволити читання і виконання тільки тих виконуваних ОД, які вже знаходяться на системному диску; дозволити читання системних ОД; дозволити читання і запис інформаційних ОД; все інше забороняти.

У даній МД критична витік права доступу «Запис». Оскільки послідовність дій, в результаті яких право «Запис» буде занесено в комірку матриці, що відноситься до виконуваних ОД, генерує суб'єкт доступу (користувач), то його дії не зможуть привести до витоку права доступу.

Виходячи із заданих параметрів, отримуємо наступну матрицю доступу:

$$M=\begin{array}{c} \\ S_1 \\ \dots \\ \cdots \\ S_k \\ A \end{array}\begin{array}{c} \begin{array}{ccc} O_{вик1}, \dots, O_{викq} & O_{сист1}, \dots, O_{систm} & O_{інф1}, \dots, O_{інфn} \end{array} \\ \begin{bmatrix} Чт, В & Чт & Чт, Зп \\ \dots & \dots & \\ \cdots & \cdots & \\ Чт, В & Чт & Чт, Зп \\ Чт, Зп, В & Чт, Зп & Чт, Зп \end{bmatrix} \end{array}.$$

У даній ситуації при аналізі змін стану системи не розглядаємо дії адміністратора так як він просто може відключити засіб захисту. В тому числі при даній політиці виключена сутність «Власник», відповідно користувач, який створив новий об'єкт, не зможе наділити правом доступу «Запис» інших користувачів. При створенні нового ОД також неможливий витік права доступу «Запис», так як розмежування застосовні до будь-якого користувача і не важливі ні його ім'я, ні його SID. У разі підвищення привілею звичайного користувача до Адміністратора можливий витік права щодо суб'єкта доступу.

Перевагою даного методу є можливість адміністратора встановлювати нове ПЗ або оновлювати існуюче. Недоліком даного методу є можливість отримання адміністративних прав і внаслідок чого необхідність додаткового захисту від підвищення привілею до адміністративних прав. Дана технологія реалізована для надання можливості окремому потоку

виконуватися від імені іншого користувача, тобто в цьому випадку буде наданий інший маркер доступу.

Для усунення недоліку даного методу і можливості підвищення привілею і для контролю зміни прав доступу необхідно СД задавати виходячи з двох сутностей: ефективного та первинного користувача, і забороняти уособлення будь-якого користувача з Адміністратором.

Одним з варіантів проникнення загрозливого ПЗ є його впровадження під виглядом санкціонованого типу файлів (інформаційного), видалення санкціонованого виконуваного файлу і після цього його перейменування. Для вирішення цієї проблеми пропонується розділяти способи модифікації об'єктів. Даний метод робить акцент на способах модифікації ОД. Відмінними моментами від попереднього методу є: заборона будь-якої модифікації об'єктів (санкціонованих програм), дозволених до запуску шляхом перейменування; заборона будь-якої модифікації об'єктів (санкціонованих програм), дозволених до запуску шляхом видалення виконуваного файлу.

Суб'єкти доступу - $S_i : S = \{S_1, \dots, S_k, A\}$. Об'єкти доступу залишаються незмінними: $O = \{ O_{вик1}, \dots, O_{викq}, O_{сист1}, \dots, O_{системm}, O_{інф1}, \dots, O_{інфn} \}$. Кінцевий набір прав доступу включає в себе читання, виконання і запис: $R = \{Чт, В, Зп\}$. Крім звичайного набору прав доступу, введемо додаткові методи доступу. Заборона запису - «~~*Зп*~~». Заборона перейменування - «~~*П*~~». Перейменування виділяємо, щоб уникнути підміну санкціонованого виконуваного файлу. У набір прав доступу додамо заборону видалення - «~~*Д*~~». В результаті отримаємо наступний набір прав: $R = \{Чт, В, Зп, ~~Зп~~, ~~П~~, ~~Д~~\}$.

Даний метод захисту полягає в наступному:

- для суб'єкта доступу Адміністратор: дозволити читання, запис (установка) і виконання виконуваних ОД; дозволити читання, запис (установка) системних ОД; дозволити читання і запис інформаційних ОД; все інше заборонити.

- для всіх інших суб'єктів доступу: дозволити читання і виконання тільки тих виконуваних ОД, які вже знаходяться на системному диску; заборонити запис, перейменування і видалення існуючих виконуваних ОД на системному диску; дозволити читання для системних ОД; заборонити для системних ОД запис, перейменування і видалення; дозволити для інформаційних ОД читання і запис; заборонити для інформаційних ОД перейменування і видалення; все інше заборонити.

Виходячи із заданих параметрів, отримуємо наступну матрицю доступу:

$$M = \begin{array}{c} \\ S_1 \\ \dots \\ \cdots \\ S_k \\ A \end{array} \begin{array}{c} \begin{array}{ccc} O_{вик1}, \dots, O_{викq} & O_{сист1}, \dots, O_{системm} & O_{інф1}, \dots, O_{інфn} \end{array} \\ \begin{bmatrix} Чт, В, ~~Зп~~, ~~П~~, ~~Д~~ & Чт, ~~Зп~~, ~~П~~, ~~Д~~ & Чт, Зп, ~~П~~, ~~Д~~ \\ \dots & \dots & \\ \cdots & \cdots & \\ Чт, В, ~~Зп~~, ~~П~~, ~~Д~~ & Чт, ~~Зп~~, ~~П~~, ~~Д~~ & Чт, Зп, ~~П~~, ~~Д~~ \\ Чт, Зп, В & Чт, Зп & Чт, Зп \end{bmatrix}. \end{array}$$

У даній МД критичний витік права доступу «Запис». Оскільки послідовність дій, в результаті яких право «Запис» буде занесено в комірку матриці, що відноситься до виконуваних ОД, генерує суб'єкт доступу (користувач), то його дії не зможуть привести до витоку права доступу. У даній ситуації при аналізі змін стану системи не розглядаємо дії адміністратора так як він просто може відключити засіб захисту. В тому числі при даній політиці виключена сутність «Власник», відповідно користувач, який створив новий об'єкт, не зможе наділити правом доступу «Запис» інших користувачів. При створенні нового СД також неможливий витік права доступу «Запис», так як розмежування застосовні до будь-якого користувачева і не важливі ні його ім'я, ні його SID.

Перевагою даного методу є захист від впровадження шкідливої програми під виглядом санкціонованої. Недоліком даного методу є можливість отримання адміністративних прав і внаслідок чого необхідність додаткового захисту від підвищення привілею до адміністративних прав. Відповідно для усунення можливості підвищення привілею і для контролю зміни прав доступу необхідно суб'єкт доступу задавати виходячи з двох сутностей: ефективного та первинного користувача, і забороняти уособлення будь-якого користувача з Адміністратором. Іншим недоліком даного методу є той факт, що не враховується різниця між перейменуванням існуючого виконуваного файлу від перейменування, наприклад, інформаційного файлу, запис якого дозволена, в виконуваний файл.

Для усунення даного недоліку в даному методі додатково додається заборона перейменування існуючого виконуваного файлу (позначається «~~Пв~~»), заборона перейменування в виконуваний файл (позначається «~~ПвВ~~»). Суб'єкти доступу - $S_i : S = \{S_1, \ldots, S_k, A\}$. Об'єкти доступу залишаються незмінними: $O = \{ O_{вик1}, \ldots, O_{викq}, O_{сист1}, \ldots, O_{системm}, O_{інф1}, \ldots, O_{інфn} \}$. Кінцевий набір прав доступу включає в себе читання, виконання і запис, заборона запису, заборона перейменування існуючого виконуваного файлу, заборона перейменування в виконуваний файл, заборона видалення. В результаті отримаємо наступний набір прав: *R* = {*Чт, В, Зп, ~~Зп~~, ~~Пв~~, ~~ПвВ~~, ~~Д~~*}.

Даний метод захисту полягає в наступному:

- для суб'єкта доступу Адміністратор: дозволити читання, запис (установка) і виконання виконуваних ОД; дозволити читання, запис (установка) системних ОД; дозволити читання і запис інформаційних ОД; все інше заборонити.

- для всіх інших суб'єктів доступу: дозволити читання і виконання тільки тих ОД, які вже знаходяться на системному диску; заборонити запис, перейменування існуючого виконуваного ОД, видалення існуючих виконуваних ОД на системному диску; дозволити читання для системних ОД; заборонити для системних ОД запис, перейменування існуючого ОД, видалення; дозволити для інформаційних ОД читання і запис; заборонити для інформаційних ОД перейменування існуючого ОД, видалення; все інше заборонити.

Виходячи із заданих параметрів, отримуємо наступну матрицю доступу:

$$M = \begin{array}{c} \\ S_1 \\ \ldots \\ \ldots \\ S_k \\ A \end{array} \begin{array}{c} \begin{array}{ccc} O_{вик1}, \ldots, O_{викq} & O_{сист1}, \ldots, O_{системm} & O_{інф1}, \ldots, O_{інфn} \end{array} \\ \begin{bmatrix} Чт,В,\sout{Зп},\sout{Пв},\sout{ПвВ},\sout{Д} & Чт,\sout{Зп},\sout{Пв},\sout{ПвВ},\sout{Д} & Чт,Зп,\sout{Пв},\sout{ПвВ},\sout{Д} \\ & \ldots & \\ & \ldots & \\ Чт,В,\sout{Зп},\sout{Пв},\sout{ПвВ},\sout{Д} & Чт,\sout{Зп},\sout{Пв},\sout{ПвВ},\sout{Д} & Чт,Зп,\sout{Пв},\sout{ПвВ},\sout{Д} \\ Чт,Зп,В & Чт,Зп & Чт,Зп \end{bmatrix} \end{array}.$$

У даній МД критичний витік права доступу «Запис». Оскільки послідовність дій, в результаті яких право «Запис» буде занесено в комірку матриці, що відноситься до виконуваних ОД, генерує суб'єкт доступу (користувач), то його дії не зможуть привести до витоку права доступу. В тому числі при даній політиці виключена сутність «Власник», відповідно користувач, який створив новий об'єкт, не зможе наділити правом доступу «Запис» інших користувачів. При створенні нового СД також неможливий витік права доступу «Запис», так як розмежування застосовні до будь-якого користувачева і не важливі ні його ім'я, ні його SID.

Перевагою даного методу є додатковий контроль перейменування об'єктів доступу.

Недоліком даного методу є можливість отримання адміністративних прав і внаслідок чого необхідність додаткового захисту від підвищення привілею до адміністративних прав. Для усунення можливості підвищення привілею і для контролю зміни прав доступу необхідно

суб'єкт доступу задавати виходячи з двох сутностей: ефективного та первинного користувача, і забороняти уособлення будь-якого користувача з Адміністратором. Іншим недоліком даного методу є той факт, що не враховується особливість впровадження загрозливого скриптового виконуваного файлу.

Додамо захист від скриптових виконуваних файлів. Їх головна відмінність в тому, що для їх виконання необхідно встановити інший інтерпретатор (середовище виконання). В даному випадку не користувач запускає виконуваний файл, а інтерпретатор. Таким чином, слід розглядати процес в якості самостійного суб'єкта доступу. До нього також слід застосовувати розмежувальні політики для управління доступом до ресурсів. Метод захисту враховує особливості скриптових виконуваних загрозливих файлів. У разі скриптових виконуваних файлів головне не дати записати, а потім не дати інтерпретатору запустити скрипт. Але проблема в тому, що інтерпретатор при доступі до даного файлу використовує метод доступу читання, а воно дозволено для всіх користувачів. В даному випадку можна розглянути всі інтерпретатори (процеси), які запускаються окремо і для кожного призначити свої права доступу. Будемо захищати безпосередньо від запису скриптового виконуваного файлу, а не від подальшого його читання. Отримаємо, що суб'єкт доступу слід задавати трьома сутностями: первинний користувач, ефективний користувач і процес. Основою моделі захисту від скриптових виконуваних файлів є захист від витоку права модифікації функцій санкціонованої програми. Особливістю методу є розбиття методу доступу «Запис» на створення нового об'єкту доступу і зміна існуючого об'єкта доступу шляхом перейменування. Заборона створення нового будемо позначати «~~*ЗпН*~~», а зміна існуючого - «~~*ЗпІ*~~». Суб'єкти доступу - $S_i : S = \{S_1, \ldots, S_k, A\}$. Об'єкти доступу залишаються незмінними: $O = \{ O_{вик1}, \ldots, O_{викq}, O_{сист1}, \ldots, O_{систm}, O_{інф1}, \ldots, O_{інфn} \}$. Кінцевий набір прав доступу включає в себе читання, виконання і запис, заборона створення нового ОД, заборона зміни існуючого ОД, заборона перейменування існуючого виконуваного файлу, заборона перейменування в виконуваний файл, заборона видалення. В результаті отримаємо наступний набір прав: *R* = {*Чт, В, Зп,* ~~*ЗпН*~~*,* ~~*ЗпІ*~~*,* ~~*Пв*~~*,* ~~*ПвВ*~~*,* ~~*Д*~~}.

Метод полягає в наступному:

- для суб'єкта доступу Адміністратор: дозволити читання, запис (установка) і виконання виконуваних ОД; дозволити читання, запис (установка) системних ОД; дозволити читання і запис інформаційних ОД; все інше заборонити.

- для всіх інших суб'єктів доступу: дозволити читання і виконання тільки тих виконуваних ОД, які вже знаходяться на системному диску; заборонити створення нового ОД, зміни існуючого ОД, перейменування існуючого виконуваного ОД, видалення існуючих виконуваних ОД на системному диску; дозволити читання для системних ОД; заборонити для системних ОД створення нового ОД, зміна існуючого ОД, перейменування існуючого ОД; дозволити для інформаційних ОД читання і запис; заборонити для інформаційних ОД перейменування існуючого ОД видалення; все інше заборонити.

Виходячи із заданих параметрів, отримуємо наступну матрицю доступу:

$$M = \begin{array}{c} \\ S_1 \\ \cdots \\ \cdots \\ S_k \\ \\ A \end{array} \begin{array}{c} \begin{array}{ccc} O_{вик1}, \ldots, O_{викq} & O_{сист1}, \ldots, O_{систm} & O_{інф1}, \ldots, O_{інфn} \end{array} \\ \left[\begin{array}{ccc} \text{Чт, В, } \sout{\text{ЗпН, ЗпІ,}} & \text{Чт, ЗпН, ЗпІ,} & \text{Чт, ЗпН, ЗпІ,} \\ \sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} \\ & \cdots & \\ \text{Чт, В, } \sout{\text{ЗпН, ЗпІ,}} & \text{Чт, ЗпН, ЗпІ,} & \text{Чт, ЗпН, ЗпІ,} \\ \sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} \\ \text{Чт,Зп, В} & \text{Чт,Зп} & \text{Чт, Зп} \end{array} \right]. \end{array}$$

У даній МД критичний витік права модифікації функцій в процесі виконання невиконуваних файлів. Іншими словами санкціонована програма наділяється загрозливими можливостями. Також критичний витік права доступу «*~~ЗпН~~*» і «*~~ЗпІ~~*». Оскільки послідовність дій, в результаті яких право «*~~ЗпН~~*» або «*~~ЗпІ~~*» буде занесено в комірку матриці, що відноситься до виконуваних ОД, генерує суб'єкт доступу (користувач), то його дії не зможуть привести до витоку права доступу. В тому числі при даній політиці виключена сутність «Власник», відповідно користувач, який створив новий об'єкт, не зможе наділити правом доступу «Запис» інших користувачів. При створенні нового СД також неможливий витік права доступу «Запис», так як розмежування застосовні до будь-якого користувача і не важливі ні його ім'я, ні його SID.

Перевагою даного методу є контроль запису скриптових виконуваних програм, тобто протидія їх впровадження. Недоліком даного методу є можливість отримання адміністративних прав і внаслідок чого необхідність додаткового захисту від підвищення привілею до адміністративних прав. Відповідно для усунення можливості підвищення привілею і для контролю зміни прав доступу необхідно суб'єкт доступу задавати виходячи з двох сутностей: ефективного і первинного користувача, і забороняти уособлення будь-якого користувача з Адміністратором. Іншим недоліком даного методу є відсутність контролю роботи браузера з інтерпретаторами.

Модель і метод захисту з додатковим захистом від наділення загрозливими властивостями інтерпретаторів (віртуальних машин). Тепер усунемо недолік попереднього методу: відсутність контролю, коли браузер, використовуючи інтерпретатор, відкриває файл для читання. Виходячи з матриці доступу попереднього методу, процес може читати виконуваний файл, і тим самим зможе його запустити. В такому випадку виділимо окремий суб'єкт доступу, який є інтерпретатором (віртуальна машина), наприклад, java.exe (JVM). Таким чином, в якості суб'єктів доступу виступатимуть користувачі системи і віртуальні машини $S_i : S = \{S_1, \ldots, S_k, A, VM_1, \ldots, VM_j\}$. ОД залишаються незмінними: $O = \{O_{вик1}, \ldots, O_{викq}, O_{сист1}, \ldots, O_{систm}, O_{інф1}, \ldots, O_{інфn}\}$. Кінцевий набір прав доступу включає в себе читання, виконання і запис, заборона створення нового ОД, заборона зміни існуючого ОД, заборона перейменування існуючого виконуваного файлу, заборона перейменування в виконуваний файл, заборона видалення. Введемо додатково право доступу - заборона читання (позначимо заборона читання як «*~~Чт~~*»). В результаті отримаємо наступний набір прав: *R* = {*Чт, ~~Чт~~ , В, Зп, ~~ЗпН~~, ~~ЗпІ~~, ~~Пв~~, ~~ПвВ~~, ~~Д~~*}.

Метод передбачає захист від наділення загрозливими властивостями інтерпретаторів і полягає в наступному:

- для суб'єкта доступу Адміністратор: дозволити читання, запис (установка) і виконання виконуваних ОД; дозволити читання, запис (установка) системних ОД; дозволяти читання і запис інформаційних ОД; все інше забороняти.

- для суб'єктів доступу віртуальна машина (інтерпретатор): дозволити виконання тільки тих виконуваних ОД, які вже знаходяться на системному диску; заборонити читання, запис, перейменування існуючого виконуваного ОД, видалення існуючих виконуваних ОД на системному диску; дозволити читання для системних ОД; заборонити для системних ОД запис, перейменування існуючого ОД, видалення; дозволити для інформаційних ОД читання і запис; заборонити для інформаційних ОД перейменування існуючого ОД, видалення; все інше заборонити.

- для всіх інших суб'єктів доступу: дозволити читання і виконання тільки тих виконуваних ОД, які вже знаходяться на системному диску; заборонити запис, перейменування існуючого виконуваного ОД, видалення існуючих виконуваних ОД на системному диску; дозволити читання для системних ОД; заборонити для системних ОД запис, перейменування існуючого ОД, видалення; дозволити для інформаційних ОД читання і

запис; заборонити для інформаційних ОД перейменування існуючого ОД, видалення; все інше заборонити. Виходячи із заданих параметрів, отримуємо наступну матрицю доступу:

Перевагою методу є те, що після установки даних прав доступу ні бінарні, ні скриптові виконувані загрозливі програми не будуть загрожувати безпеці системи.

Недоліком даного методу є можливість отримання адміністративних прав і внаслідок чого необхідність додаткового захисту від підвищення привілею до адміністративних прав. Відповідно для усунення можливості підвищення привілею і для контролю зміни прав доступу необхідно суб'єкт доступу задавати виходячи з двох сутностей: ефективного та первинного користувача, і забороняти уособлення будь-якого користувача з Адміністратором.

$$
M = \begin{array}{c}
 \\
S_1 \\
\cdots \\
\cdots \\
S_k \\
 \\
VM_1 \\
\cdots \\
\cdots \\
VM_j \\
 \\
A
\end{array}
\begin{array}{|c|c|c|}
\multicolumn{3}{c}{O_{вик1}, \ldots, O_{викq} \quad O_{сист1}, \ldots, O_{систm} \quad O_{інф1}, \ldots, O_{інфn}} \\
\hline
\text{Чт, В, } \sout{\text{ЗпН, ЗпІ,}} & \text{Чт, } \sout{\text{ЗпН, ЗпІ,}} & \text{Чт, Зп,} \\
\sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} \\
\cdots & \cdots & \\
\text{Чт, В, } \sout{\text{ЗпН, ЗпІ,}} & \text{Чт, } \sout{\text{ЗпН, ЗпІ,}} & \text{Чт, Зп,} \\
\sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} \\
 & & \\
\sout{\text{Чт, В, ЗпН, ЗпІ,}} & \text{Чт, } \sout{\text{ЗпН, ЗпІ,}} & \text{Чт, Зп,} \\
\sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} \\
\cdots & \cdots & \\
\sout{\text{Чт, В, ЗпН, ЗпІ,}} & \text{Чт, } \sout{\text{ЗпН, ЗпІ,}} & \text{Чт, Зп,} \\
\sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} & \sout{\text{Пв, ПвВ, Д}} \\
\text{Чт,Зп, В} & \text{Чт,Зп} & \text{Чт, Зп}
\end{array}.
$$

Висновки. Проведено дослідження основних типів загрозливих програм, на підставі якого запропоновано класифікацію загрозливих програм за способом їх виконання. На підставі існуючої статистики зроблено висновок, що найбільш актуальними для захисту є виконувані бінарні і скриптові файли.

Проведено дослідження способів впровадження загрозливих програм, в результаті якого зроблено висновок - класи загрозливих програм, що розглядаються передбачають обов'язкове збереження файлу на жорсткому диску перед виконанням (читанням). Для захисту від найбільш актуальних загрозливих програм потенційно може бути реалізований контроль доступу (розмежувальна політика доступу) до файлових об'єктів.

Результатом дослідження існуючих підходів до оцінки ефективності методів і засобів захисту від загрозливих програм, зроблені висновки про неможливість з використанням відомих підходів ні кількісно оцінити актуальність окремої загрози для інформаційної системи в цілому (з урахуванням безлічі інших потенційних загроз), в тому числі загрози занесення і запуску загрозливих програм, ні кількісно оцінити основні стохастичні характеристики безпеки системи від загрозливих програм. В результаті чого сформульована задача розробки відповідних математичних моделей і наступного проведення на них досліджень, що дозволяють отримати необхідні кількісні оцінки.

Запропоновано загальний підхід до захисту від загрозливих програм, заснований на контролі доступу до ресурсів по розширенням і типам файлів. Розроблені методи, що дозволяють захищати від бінарних і скриптових загрозливих файлів.

Розроблені моделі безпечної системи, що дозволяють сформулювати вимоги до побудови безпечної системи в частині запобігання витоку прав доступу. Сформульовані вимоги до механізмів захисту, реалізація яких дозволить побудувати безпечну систему, що обґрунтовано на побудованих моделях.

ЛІТЕРАТУРА:

1. Основы программно-аппаратной защиты информации. / М. А. Борисов, И. В. Заводцев, И. В. Чижов. – М.: УРСС: Либроком, 2013. – 370 с.

2. Михайлов А.В. Компьютерные вирусы и борьба с ними. / А.В. Михайлов. – М.: Диалог-МИФИ, 2012. – 148 с.

3. Касперский Е. В. «Компьютерное зловредство» / Е. В. Касперский. – Санкт-Петербург: Питер, 2009. – 208 с.

4. Партыка Т. Л. Информационная безопасность учебное пособие / Т. Л. Партыка, И. И. Попов. – М.: ФОРУМ, 2011. – 432 с.

5. Сердюк В. А. Организация и технологии защиты информации / В. А. Сердюк. – М.: Издательский дом Государственного университета – Высшей школы экономики, 2011. – 571 с.

6. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 576 с.

7. Гольдштейн, Б.С. Сети связи пост-NGN/Б.С. Гольдштейн, А.Е. Кучерявый. – СПб.:БХВ-Петербург,2014. – 160с.: ил.

8. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы /В. Г. Олифер, Н. А.Олифер - СПб.: Питер, 2017. – 992 с.

9. Рыжиков, Ю.И. Имитационное моделирование. Теория и технология / Ю.И. Рыжиков - СПб: КОРОНА принт, 2015. – 384 с.

10. Советов, Б. Я. Моделирование систем : учебник для бакалавров / Б. Я. Советов, С. А. Яковлев. – 7-е изд. – М. : Издательство Юрайт, 2015. – 343 с.

11. Тюрликов, А. М. Методы случайного множественного доступа [Текст] : монография / А. М. Тюрликов – Санкт-Петербург : ГУАП, 2014. - 299 с. : ил.

REFERENCES:

1. Borisov, M.A., Zavodcev, I.V. and CHizhov, I.V. (2013). ”Osnovy programmno-apparatnoj zashchity informacii”, M.: URSS: Librokom, 370 p.

2. Mihajlov, A.V. (2012), ”Komp'yuternye virusy i bor'ba s nimi.”, M.: Dialog-MIFI, 148 p.

3. Kasperskij, E.V. (2009), ”Komp'yuternoe zlovredstvo”, Sankt-peterburg: Piter,. 208 p.

4. Partyka, T.L. and Popov, I.I. (2011). ”Informacionnaya bezopasnost' uchebnoe posobie” , M.: FORUM, 432 p.

5. Serdyuk, V. A. (2011). ”Organizaciya i tekhnologii zashchity informacii ”, M.: Izdatel'skij dom Gosudarstvennogo universiteta – Vysshej shkoly ekonomiki,. 571 p.

6. SHan'gin V. F. (2012). ”Zashchita informacii v komp'yuternyh sistemah i setyah ”. / V. F. SHan'gin. - M.: DMK Press, 576 p.

7. Goldshteyn, B.S. and Kucheryavy, A.E. (2014). ”Seti svyazi post-NGN”[Post-NGN communication networks], SPb.:BHV-Peterburg, 160p.: il.

8. Olifer, V. G. and Olifer, N. A. (2017). ”Kompyuternyie seti. Printsipyi, tehnologii, protokolyi ” [Computer networks. Principles, technologies, protocols], SPb.: Piter, 992p.

9. Ryizhikov, Yu.I. (2015). ”Imitatsionnoe modelirovanie. Teoriya i tehnologiya.” [Imitation modeling. Theory and technology], SPb: KORONA print, 384p.

10. Sovetov, B. Ya. and Yakovlev, S.A. (2015). ”Modelirovanie sistem : uchebnik dlya bakalavrov” [System modeling: a textbook for bachelors] ,7-e izd. M. : Izdatelstvo Yurayt, 343p.

11. Tyurlikov, A. M. (2014). ”Metodyi sluchaynogo mnozhestvennogo dostupa”[Random Multiple Access Methods], [Tekst] : monografiya , Sankt-Peterburg : GUAP, 299p.

к.т.н., доц. Джулий В.Н., к.т.н., доц. Бойчук В.А., к.т.н.Титова В.Ю.
д.т.н., с.н.с. Селюков А.В., к.т.н., с.н.с. Мирошниченко О.В.

МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ ИНФОРМАЦИОННЫХ СИСТЕМ

В статье предложен подход к развитию методов защиты от вредоносных программ в современных информационных системах, состоит в разработке методов защиты, основанных на реализации контроля доступа к файлам по их типам, которые могут быть идентифицированы расширениями файлов, существенно превосходят известные методы антивирусной защиты, как

по эффективности защиты, так и по мере влияния на загрузку вычислительных ресурсов информационной системы.

Показано, что наиболее актуальными для защиты являются выполняемые бинарные и скриптовые файлы и о том, что данные классы вредоносных программ предусматривают обязательное сохранение вредоносного файла на жестком диске перед его выполнением (чтением). Это позволило сделать вывод о том, что защита от вредоносных программ может строиться реализацией контроля (разграничение прав) доступа к файлам.

Предложен общий подход к реализации защиты от вредоносных программ, основанный на реализации контроля доступа к файлам по их типам, которые могут быть идентифицированы расширениями файлов. Возможность использования подобного подхода обоснованно проведенным исследованиям средств защиты.

Методы защиты от вредоносных программ позволяют защитить информационную систему, как от загрузки, так и от выполнения бинарных и скриптовых вредоносных файлов, отличающиеся возможностью учета расположения исполняемых файлов, возможностью администрирования при работающей системе защиты, возможностью контроля модификации объектов доступа, переименование объектов доступа, возможностью защиты от скриптовых вредоносных программ, в том числе с учетом возможности наделения вредоносными свойствами интерпретаторов (виртуальных машин).

Разработаны модели контроля доступа, позволили на построенных матрицах доступа сформулировать требования к построению безопасной системы, выполнение которых предотвращает утечку заданных прав доступа субъектов к объектам.

Ключевые слова: вредоносные программы, компьютерная безопасность, информационная система, контроль доступа, объект доступа, субъект доступа.

Ph.D. Dzhulij V.M., Ph.D. Boychuk V.A., Ph.D. Titova V.Y.,
Doctor of Technical Sciences Selyukov A.V., Ph.D. Miroshnichenko O.V.

PROTECTION MODELS AND METHODS AGAINST THREATED PROGRAMS INFORMATION SYSTEMS

The article proposes an approach to the development of protection methods against threatening programs in modern information systems, which consists in the development of security methods based on the implementation of access control to files by their types, which can be identified by file extensions that significantly exceed the known methods of antivirus protection, such as on the effectiveness of protection, as well as the impact on the load of computing resources of the information system.

It is shown that the most important for protection are executable binary and script files, and that these classes of malware require mandatory storage of the threatening file on the hard disk before its execution (read). This led to the conclusion that protection against threatening programs can be built by implementing control (delineation) of access to files.

A general approach to the implementation of protection against threatening programs is proposed, based on the implementation of control of access to files by their types, which can be identified by file extensions. The possibility of using such an approach is substantiated by a study of remedies.

Methods of protection against threatening programs allow to protect the information system, both from loading, and from execution of binary and scripted threat files, differing in the possibility of taking into account the location of executable files, the possibility of administration with a working security system, the ability to control the modification of access objects, renaming access features, the ability to protect against scripted threat programs, including the ability to give threatening properties to interpreters (virtual x machines).

Models of access control have been developed, which allowed the built-in access matrices to formulate requirements for building a secure system, the implementation of which prevents the leakage of given access rights of subjects to objects.

Keywords: threatening programs, computer security, information system, access control, object of access, subject of access.

УДК 37.091.33:004.031.42(045)

к.т.н., доц. **Кльоц Ю.П.** (ХмНУ)
к.т.н., доц. **Муляр І.В.** (ХмНУ)
к.т.н., доц. **Чешун В.М.** (ХмНУ)
Бурдюг О.В. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-09

ВИКОРИСТАННЯ РОЗПОДІЛЕНИХ ХЕШ-ТАБЛИЦЬ НАДАННЯ ДОСТУПУ ДО ХМАРНИХ СЕРВІСІВ

У статті розкрито актуальність проблеми надання доступу до сервісів розподіленої хмарної системи, зокрема, охарактеризовано однорангову розподілену хмарну систему. Подано процес взаємодії основних компонентів для отримання доступу до веб-ресурсу з доменним ім'ям. Досліджено, що розподіл ресурсів між вузлами однорангової розподіленої хмарної системи з подальшим наданням сервісів за запитом реалізується за допомогою протоколу Kademlia в локальній мережі або мережі Інтернет і містить процеси публікації ресурсу на початковій стадії його власником, реплікації і безпосередньо надання доступу до ресурсів.

Застосування сучасних технологій адаптивних систем захисту інформації не дозволяє здійснювати повний контроль за інформаційними потоками середовища хмарних обчислень, оскільки вони функціонують на верхніх рівнях ієрархії. Тому для створення ефективних механізмів захисту ПЗ в середовищі хмарних обчислень потрібна розробка нових моделей загроз і створення методів відображення комп'ютерних атак, які дозволяють оперативно ідентифікувати приховані і потенційно небезпечні процеси інформаційної взаємодії.

Правила розмежування доступу, складають основу політики безпеки, включають і обмеження на механізми ініціалізації процесів доступу. В рамках розробленої моделі операцій формалізований опис прихованих загроз зводиться до появи контекстно-залежних переходів в мультиграфі транзакцій

Обґрунтовано метод надання доступу до сервісів розподіленої хмарної системи. Визначено, що для пошуку вузла реплікації, який має репліку запитуваного ресурсу або його частину, застосовується інфраструктура розподілених хеш- таблиць (Distributed Hash Table, DHT). У дослідженні визначено етапи валідації ідентифікатора вузла. Описано процеси додавання нового вузла, валідації автентичності, публікації ресурсу й отримання доступу до ресурсу подано у вигляді поетапної послідовності дій у межах методу надання доступу до сервісів розподіленої хмарної системи за допомогою графічного опису інформаційних потоків, взаємодії процесів оброблення інформації та об'єктів.

Ключові слова: метод, хмарна система, хеш-таблиці.

Вступ. Розповсюдження мереж з високою потужністю, низька вартість комп'ютерів і пристроїв зберігання даних, а також широке впровадження віртуалізації, сервіс-орієнтованої архітектури привели до величезного зростання хмарних обчислень. Хмарні обчислення – це модель забезпечення зручного доступу на вимогу через мережу до обчислювальних ресурсів, які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера.

Середовище хмарних обчислень - це сукупність обчислювальних ресурсів у вигляді віртуальних машин, що надаються користувачеві за допомогою загальних сервісів доступу. Фізичний рівень хмарної системи складається з апаратних ресурсів, які необхідні для забезпечення сервісів, що надаються, і, як правило, включає сервери, системи зберігання і мережеві компоненти. Застосування технологій хмарних обчислень визначає необхідність розгляду можливих способів дестабілізуючих дій, що приводять до порушення функціонування компонентів інформаційного середовища.

Характерною особливістю сучасного середовища хмарних обчислень є активний характер суб'єктів і об'єктів інформаційної взаємодії. Це дозволяє розглядати цільову функцію системи безпеки як збереження конфіденційності, цілісності і доступності програмних і інфраструктурних сервісів, що надаються в режимі видаленого доступу в умовах динамічної

зміни стану обчислювальних ресурсів. Побудова перспективних механізмів забезпечення безпеки в середовищі хмарних обчислень зв'язується не із захистом від виявлених вразливостей, а полягає в можливості запобігання новим невідомим методам проведення атак, в розробці нових моделей загроз і методів запобігання або віддзеркалення комп'ютерних атак на інформаційні ресурси, які використовують можливості предикативної ідентифікації прихованих каналів і потенційно небезпечних процесів інформаційної взаємодії [1]

Важливим напрямом вдосконалення технологій захисту і систем інформаційної безпеки є протидія білатеральним загрозам, в яких суб'єкт і об'єкт процесів інформаційної взаємодії є потенційним носієм небезпечних дій. У таких випадках необхідно використовувати моделі загроз, які ідентифікують потенційні вразливості як на рівні процесів контролю доступу до ресурсів гостьових операційних систем (ОС) або додатків, так і на рівні системних викликів гіпервізора [2], який сам може стати джерелом руйнуючих дій що реалізовуються шляхом порушення функціонування планувальника завдань або диспетчера устаткування. Загрози, що виникають при цьому, необхідно не тільки оперативно виявляти, але і блокувати використовувані неавторизовані канали інформаційних дій, які в середовищі хмарних обчислень зазвичай реалізуються в прихованому для гостьових ОС режимах. Тому важливим чинником підвищення ефективності систем захисту від прихованих загроз є облік напряму передачі, синтаксису і контексту потоків даних, які передаються [2, 3].

Аналіз останніх досліджень і публікацій.

Поява хмарних технологій сприяла відмові від застосування децентралізованої архітектури як єдиної, а тому викликала значну кількість проблем: «велика вартість розгортання, високе енергоспоживання, значні простої й неефективне використання обладнання, зменшення продуктивності ресурсів зі збільшенням кількості користувачів, негативний вплив на навколишнє середовище».

Потужні трансформаторні підстанції, дизельні генератори, системи охолодження й резервні джерела живлення, які використовуються для підтримки працездатності хмарного центру обробки даних [4, 5] та мають істотний негативний вплив на навколишнє середовище. Крім того, підвищення популярності, затребуваності й кількості інформаційних інтернет-сервісів, а також збільшення кількості пристроїв і користувачів, для яких потрібно забезпечити доступність і гарантований час відгуку таких сервісів [3], призводить до того, що провайдери хмарних послуг змушені збільшувати потужності й кількість дата-центрів.

Варто зазначити, що для хмарних інфраструктур необхідно виконувати достовірне оцінювання, а також забезпечувати необхідний рівень доступності сервісів, одночасно з підвищенням енергоефективності [6], зменшенням споживання енергії й негативного впливу на навколишнє середовище [7].

Існуючі методи оцінювання й забезпечення готовності та доступності хмарних архітектур [8 - 10] дозволяють зробити висновок, що вони не надають можливості визначити фактичну доступність і продуктивність хмарних сервісів з використанням об’єктивних кількісних показників.

Ефективною, на нашу думку, буде модернізація інфраструктури хмарної системи шляхом усунення або розвантаження хмарних сервісі, які є причиною споживання великої кількості енергії та виділення тепла і, як наслідок, негативного впливу на навколишнє середовище. Прикладом такої модернізації є перетворення хмарної архітектури на розподілений децентралізований тип, тобто коли кожен вузол надає виділену частину власних апаратних ресурсів у загальне користування.

Використання технології між мережного екранування з урахуванням специфіки захищеності середовища. Для цього необхідна формалізація вимог розмежування доступу до інформаційних сервісів [9]. Така формалізація може бути представлена з використанням динамічно формованого набору правил фільтрації, що забезпечує виконання вимог політики доступу. При цьому зростаюча складність алгоритмів фільтрації пред'являє високі вимоги до продуктивності між мережевих екранів, що робить необхідним використання методів

паралельної обробки віртуальних з'єднань за допомогою віотуальних машин. У сучасній літературі підхід до створення складних технічних систем, зв'язаність яких забезпечується за рахунок організації процесів обміну інформацією з мережі, отримав назву мережево-центричний. Цей підхід стосовно задачі розмежування доступу вимагає забезпечення ситуаційної обізнаності та локальності дій кожного з між мережевих екранів, що входять до складу віртуальних машин.

Тому існує низка взаємозв'язаних завдань: для хмарних інфраструктур необхідно виконувати достовірне оцінювання, а також забезпечувати необхідний рівень доступності сервісів, одночасно з підвищенням енергоефективності [8], зменшенням споживання енергії й негативного впливу на навколишнє середовище [4]. Аналіз існуючих моделей і методів оцінювання й забезпечення готовності та доступності хмарних архітектур [8, 10] дає змогу зробити висновок, що вони не надають можливості визначити фактичну доступність і продуктивність хмарних сервісів з використанням об'єктивних кількісних показників.

Постановка задачі. Використання традиційних підходів не дозволяє вирішити проблему підвищення рівня захищеності середовища хмарних обчислень з урахуванням гнучкості, масштабованості (підтримка апаратних платформ різного класу) пропонованих програмно-технічних рішень і мінімізації витрат. Запропоновані методи зниження продуктивності ресурсів зі збільшенням кількості користувачів [6] не враховують повною мірою особливостей впровадження хмарних архітектур. Таким чином, актуальним науково-прикладним завданням є розробка методу надання доступу до ресурсів розподіленої хмарної системи з необхідним рівнем якості обслуговування.

Дослідження методу надання доступу до сервісів розподіленої хмарної системи

Для того, щоб проаналізувати доступності сервісів хмарної системи з клієнт-серверною архітектурою було досліджено функціональні й надійнісні характеристики інфраструктури хмарного ЦОД і його окремих компонентів, на базі яких функціонують сервіси. Доцільним буде розкрити сутність методу надання доступу до ресурсів розподіленої хмарної системи з необхідним рівнем якості обслуговування.

Standards and Technology - NIST) у документі «Cloud Computing Reference Architecture» [12] подав огляд еталонної архітектури хмарних обчислень, який ідентифікує основних суб'єктів, їх діяльність і функції у хмарних обчисленнях (рис1)

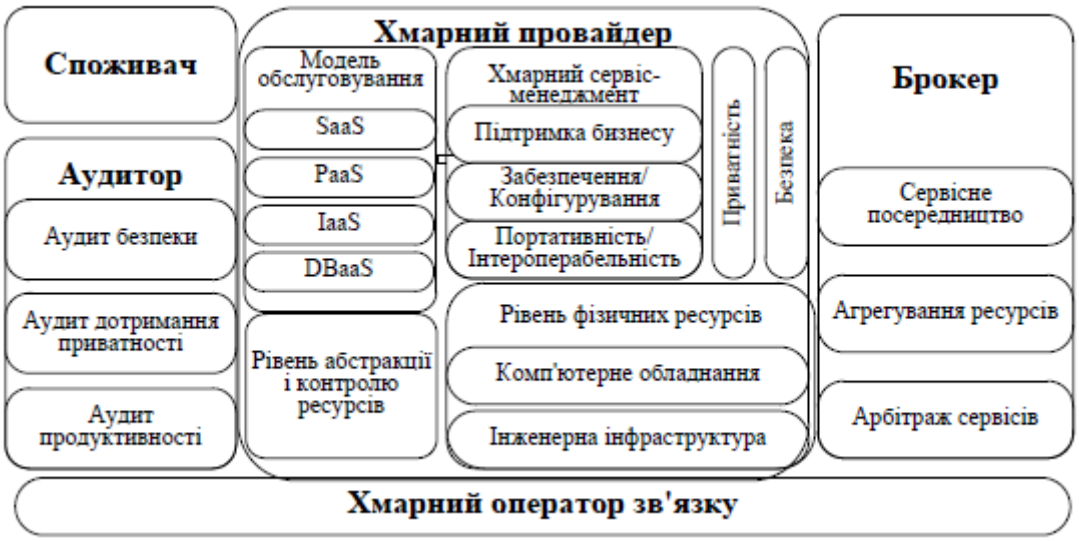

Рисунок 1 – Еталонна архітектура хмарних обчислень NIST

Ідея однорангової розподіленої хмарної системи (рис. 2) полягає в об'єднанні двох базових технологій: Grid-системи та Cloud (централізована клієнт-серверна система з підтримкою технології віртуалізації) за допомогою піринговых мереж [13].

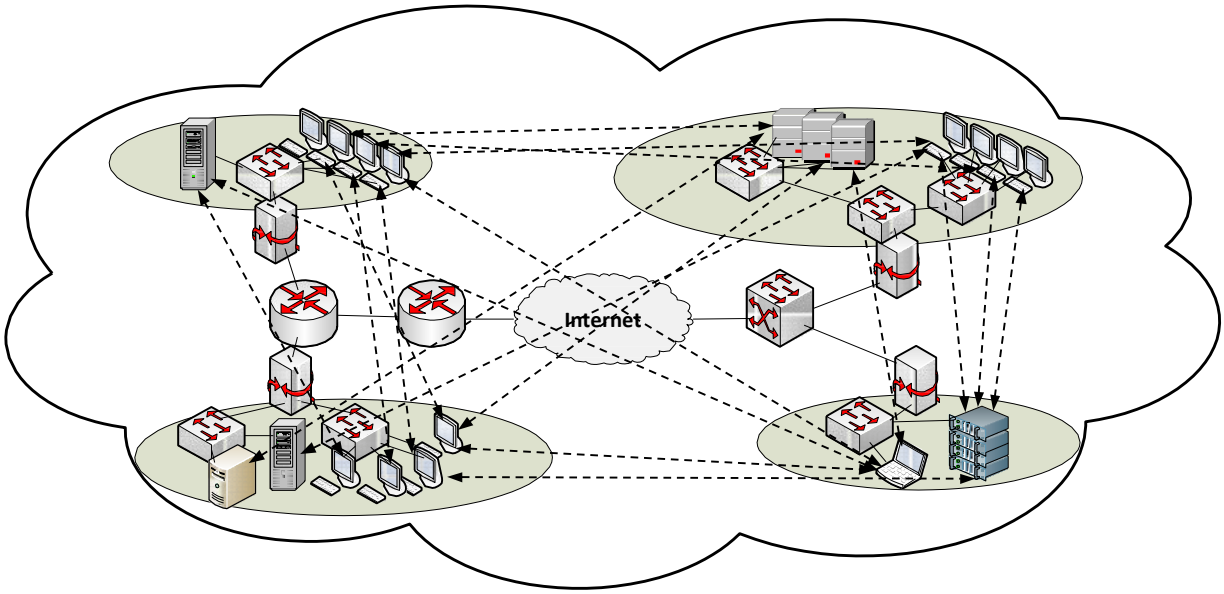

Рисунок 2 - Взаємодія користувачів однорангової розподіленої хмарної системи через глобальну мережу

Дана архітектура базується на принципі рівноправної взаємодії вузлів системи, які зв’язані між собою за допомогою мережі Інтернет або локальної мережі. Вузлами реплікації є робочі станції користувачів-учасників «хмари», які надають частину своїх ресурсів у загальне користування. Відповідь на запит користувача кешується на дисковому просторі його робочої станції, який потім на вимогу можна надати іншим учасникам однорангової розподіленої хмарної системи. Таким чином, з ростом популярності ресурсу буде збільшуватися продуктивність системи в цілому.

Принцип рівноправності покладено в основу взаємодії учасників однорангової розподіленої хмарної системи. Кожен вузол може виступати в ролі клієнта (якщо він запитує ресурс) і в ролі сервера (якщо він надає ресурс або його частину). Аналіз наукової літератури дозволяє виділити ще одну роль – власник ресурсу, який має повні права на нього.

Доменне ім'я використовується як глобальний ідентифікатор ресурсу для інтеграції з існуючими Інтернет сервісами, яке пов'язує з собою ряд ресурсних записів. Ресурсний запис (A) використовується для зберігання адрес власника ресурсу і вузлів, які мають повну репліку ресурсу. Додаткові ресурсні записи застосовується для зберігання унікального ідентифікатора ресурсу в одноранговій мережі. Унікальним ідентифікатором ресурсу в одноранговій мережі є хеш-сума його вмісту. На рис. 2 зображено процес отримання запитуваного ресурсу за доменним ім’ям http://domain-name.com/resource-name, що складається з N частин (складових).

Вузол, який знаходиться за NAT, застосовує механізми для з'єднання з приватною мережею [12]. Для пошуку вузла реплікації, який має репліку запитуваного ресурсу або його частину, застосовується інфраструктура розподілених хеш- таблиць (Distributed Hash Table, DHT). Велика кількість пірінгових сервісів була реалізована на базі інфраструктури DHT [13], серед яких можна виділити I2P, BitTorrent та ін. Багато з них побудовано на базі протоколу Kademlia [14], який забезпечує координацію взаємодіючих один з одним вузлів розподіленої однорангової архітектури без участі додаткових трекер-серверів.

З метою підвищення оперативності відповіді на запит за основу взято принцип розподілу ресурсів між вузлами хмарної системи з децентралізованою структурою. Розподіл ресурсів між вузлами однорангової розподіленої хмарної системи з подальшим наданням сервісів за запитом реалізується за допомогою протоколу Kademlia [14] в локальній мережі або мережі Інтернет і містить процеси публікації ресурсу на початковій стадії його власником, реплікації і безпосередньо надання доступу до ресурсів.

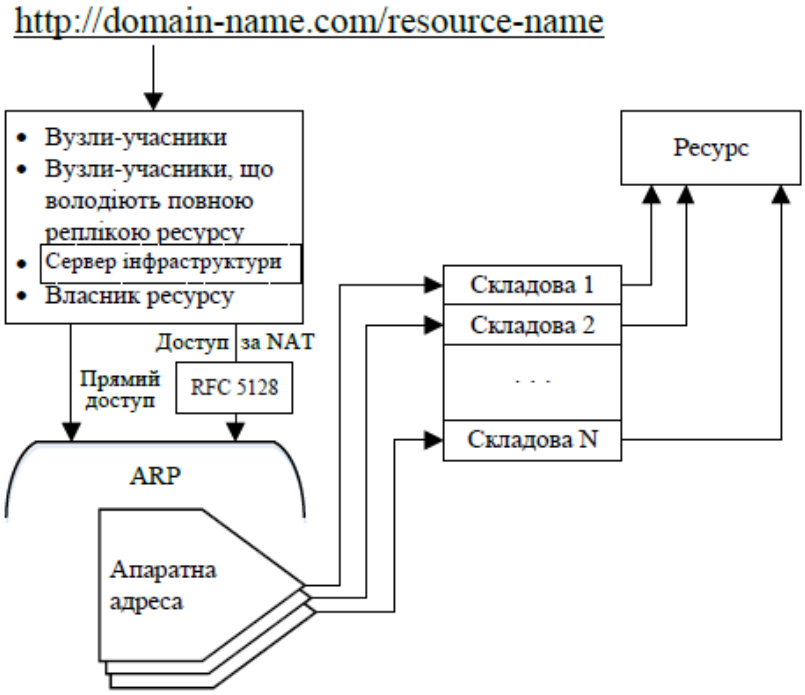

Рисунок 3 – Схема процесу отримання ресурсу за доменним ім’ям

Інформація у вигляді відповіді на запит вузла-учасника однорангової розподіленої хмарної системи зберігається на дисковому просторі його робочої станції, а потім надається в спільне користування іншим вузлам-учасникам. Процес розподілу ресурсів координується за допомогою DNS-сервера шляхом модифікації ресурсних записів.

Організація взаємодії вузлів здійснюється за допомогою спеціалізованого програмного забезпечення, встановленого на робочих станціях всіх вузлів-учасників однорангової розподіленої хмарної системи. Доступ до ресурсів для вузлів, які не є учасниками однорангової розподіленої хмарної системи, виконується завдяки стандартній взаємодії з сервером власника ресурсу або вузлами, що володіють повною реплікою ресурсу, за допомогою їх мережних адрес з урахуванням завантаженості каналів зв'язку і робочої станції власника ресурсу або вузлів, які мають повну репліку ресурсу.

На рис. 3 подано процес взаємодії основних компонентів для отримання доступу до веб-ресурсу http://domain-name.com/resource-name.

Взаємодія відбувається таким чином. На першому етапі вузол-учасник виконує стандартний запит до ресурсу http://domain-name.com/resource-name через веб-браузер на своїй робочій станції. На другому етапі вузол-учасник за допомогою прикладного програмного забезпечення виконує запит до додаткового ресурсного запису DNS- сервера ідентифікатора ресурсу ID_res з доменним ім'ям http://domain- name.com/resource-name, а також ідентифікаторів базових вузлів реплікації. Ця інформація необхідна для запуску на третьому етапі стандартного процесу пошуку DHT-lookup «FIND_NODE» найближчого за XOR-метрикою вузла реплікації ресурсу з ідентифікатором ID_res. На наступному етапі виконується запит типу «FIND_VALUE» на надання доступу до ресурсу до вузла з відповідним ідентифікатором. На завершальному етапі відбувається завантаження контенту для запитувача вузла через веб-браузер і збереження відповіді на запит на дисковому просторі цього вузла.

Процес публікації ресурсу полягає у відкритті доступу до інформації, що публікується (наприклад, веб-ресурсу), додаванні DNS-запису відповідності адреси власника ресурсу і доменного імені. Коли інший вузол-учасник на надання ресурсу, він звертається до DNS-сервера і отримує адресу власника ресурсу. Після отримання доступу безпосередньо до

ресурсу або його частини інформація у вигляді відповіді на запит зберігається на дисковому просторі вузла-учасника, і такий вузол може надати цей ресурс (або його складову) за запитом іншим вузлам мережі за допомогою протоколу Kademlia, тобто виступити в ролі сервера. Для цього його ідентифікатор додається в глобальну розподілену хеш-таблицю (DHT) ідентифікаторів ресурсів [14]. У разі, якщо інший вузол-учасник однорангової розподіленої хмарної системи запитує той самий ресурс, він отримує доступ до нього за ідентифікатором найближчого за XOR-метрикою [14] вузла реплікації, що володіє ресурсом частково або повністю, або за однією з адрес, що містяться в ресурсних записах DNS для даного ресурсу. Якщо вузол-учасник запитує всі частини ресурсу, на дисковому просторі його робочої станції буде закешовано весь ресурс повністю. У такому випадку цей вузол буде мати повну репліку ресурсу, а його адреса буде додана до основного ресурсного запису (A-запису) DNS-сервера. Таким чином, зі збільшенням популярності ресурсу більша кількість вузлів-учасників однорангової розподіленої хмарної системи може ним поділитися. Для виконання серверних функцій кожен вузол-учасник має надати в спільне користування частину власних апаратних ресурсів – дискового простору й потужності центрального процесора. Якщо вузли не є учасниками однорангової розподіленої хмарної системи, вони можуть отримати доступ до ресурсу завдяки стандартному способу взаємодії з сервером (робочою станцією) власника ресурсу або вузлами, що володіють повною реплікою ресурсу, за їхніми адресами з урахуванням завантаженості каналів зв'язку і станції власника ресурсу або вузлів, які володіють повною реплікою ресурсу шляхом відправлення стандартного запиту до основного ресурсного запису DNS-сервера й отримання адреси власника ресурсу та (або) вузлів, які мають повну репліку ресурсу.

Перевірка цілісності ресурсу та ідентичність реплік проводиться шляхом обчислення хеш-функції отриманого ресурсу і зіставлення зі значенням ідентифікатора цього ресурсу. Крім того, на проміжному етапі перед завантаженням контенту виробляється процес валідації вузла, що надає ресурс.

Рисунок 4 - Схема процесу надання доступу до ресурсів

Вузол, що надає ресурс, для підтвердження свого ідентифікатора відправляє повідомлення такого формату

ID_node	
Kpub1	SigKpriv2(Kpub1)
Kpub2	SigKpriv2(Kpub2)

На першому етапі валідації ідентифікатора вузла виконується перевірка автентичності переданих відкритих ключів Kpub1 і Kpub2 за рахунок механізму цифрового підпису. Якщо перевірка пройшла успішно, перевіряється істинність співвідношення

$$ID_{node} = Hash\left(K_{pub}1 + Sig_{K_{priv}2}(K_{pub}1)\right),$$

де ID_{node} – ідентифікатор вузла, переданий в повідомленні;

$K_{pub}1$ – відкритий ключ 1;

$Hash(Data)$ – оператор обчислення хеш-функції даних *Data*;

$Sig_{K_{priv}2}(K_{pub}1)$ – цифровий підпис даних $K_{pub}1$, отриманий за допомогою ключа $K_{priv}2$.

Якщо рівність виконується, то валідація пройшла успішно і вузол- відправник вважається успішно ідентифікованим і підтвердженим. Незалежно від ролі будь-який вузол-учасник однорангової розподіленої хмарної системи отримує високошвидкісний доступ до всіх ресурсів системи завдяки можливості отримати ресурс від найближчого вузла-учасника, який має копію цього ресурсу.

Описані процеси додавання нового вузла, валідації автентичності, публікації ресурсу й отримання доступу до ресурсу подано у вигляді поетапної послідовності дій у межах методу надання доступу до сервісів розподіленої хмарної системи за допомогою графічного опису інформаційних потоків, взаємодії процесів оброблення інформації та об'єктів, які є частиною цих процесів, IDEF3 на рис. 5.

Рисунок 5 – Метод надання доступу до сервісів розподіленої хмарної системи

Висновки. У будь-якій обчислювальній системі існують інтерфейсні рівні взаємодії між різними модулями(компонентами), що дозволяють використовувати недокументовані можливості, з одного боку, для проведення атак зловмисником, з іншої – для реалізації механізмів моніторингу з боку систем контролю і захисту ПЗ середовища хмарних обчислень.

Для досягнення цілей інформаційного забезпечення запропоновано шляхи підвищення ефективності набуття знань, зокрема, за допомогою аналізу і синтезу структури інформаційного забезпечення та визначення послідовності інформаційних об'єктів предметної області. Також запропонований підхід визначення такої траєкторії освоєння матеріалу, яка безпосередньо сприяє досягненню мети інформаційного забезпечення на основі вже наявних знань.

Запропоновано спосіб формування інформаційного забезпечення, призначений для ієрархічного мережевого представлення предметної області, що дозволяє структурувати контент інформаційно-довідкових та інших систем, що відрізняється від відомих використанням взаємопов'язаних етапів відбору, кластеризації та впорядкування контенту.

Отже, запропонований метод надання доступу до сервісів реалізує новий підхід, у межах якого виконується розподіл ресурсів у хмарній мережі з децентралізованою структурою, об'єднуючи переваги технологій GRID, хмарних обчислень і пірингових мереж. Особливістю запропонованого методу є самоорганізація процесу реплікації ресурсів засобами робочих станцій вузлів-учасників системи: цей процес не вимагає втручання адміністратора або сторонніх механізмів.

Отримані результати можуть бути використані для підтримки прийняття рішень при придбанні та застосуванні знань, а саме: при створенні інформаційного забезпечення виробничих процесів, в частині розробки елементів методичного забезпечення інформаційних систем, в корпоративних системах навчання персоналу; при розробці програм окремих курсів підвищення кваліфікації, а так само комплексів програм з подальшим їх коригуванням; інформаційного забезпечення систем електронного навчання; при формуванні програм дистанційної освіти; при розробці та наступним коригуванням навчальних планів; формуванні навчальних, довідкових матеріалів, курсів лекцій для окремих дисциплін.

ЛІТЕРАТУРА:

1. Технологии Web, Grid, Cloud для гарантоспособных ИТ- инфраструктур [Текст] : монография/ В. С. Харченко и др; Харьков. нац. аэрокосм. ун-т им. Н. Е. Жуковского. – «ХАИ», 2013. – 868 с.

2. Муляр І.В. Аналіз проблем забезпечення функціональної безпеки інформаційних систем обробки даних / І.В. Муляр, А.В. Джулій, М.В. Костюк // Вимірювальна та обчислювальна техніка в технологічних процесах: Міжнародний науково-технічний журнал.-Хмельницький, 2013. – №1 -С. 133-138.

3. Рыжкова, О.В. Сравнительный анализ эффективности использования алгоритмов изменения размера окна перегрузок в сетях Cloud Computing [Текст] / О. В. Рыжкова // Радіоелектронні і комп’ютерні системи. – 2012. – № 7(59). – С. 73 – 78.

4. Муляр І.В. Метод предикативної ідентифікації процесів для захисту від прихованих загроз в середовищі хмарних обчислень / С.В. Лєнков , В.М. Джулій , О.В. Селюков, І.В. Муляр // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 55. – С. 145-154.

5. Яновская, О.В. Модели надежности компонентов облачного дата-центра [Текст] / О. В. Яновская, В. С. Харченко // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка "Проблеми енергозабезпечення та енергозбереження в АПК України". – 2014. – Вып. 154. – С. 86 – 88.

6. Яновская, О.В. Модели доступности сервисов распределенных облачных систем [Текст] / О. В. Яновская // Наука і техніка Повітряних Сил Збройних Сил України.– 2016. – № 1(22). – С. 124 – 130.

7. Ленков С.В. Динамічні показники оцінки рівня функціональної безпеки інформаційної системи / С.В. Лєнков, В.М. Джулій, І.В. Муляр // Сучасна спеціальна техніка. Науково практичний журнал. - ДНДІ МВС України, 2016. - Вип. №2(45). - С.59-67.

8. Муляр І.В. Метод надання доступу до сервісів однорангової розподіленої хмарної системи / І.В. Муляр, А. С. Сівак // Вимірювальна та обчислювальна техніка в технологічних процесах.-2019.- № 1 (63).-С. 68-73

9. Dong, S.K. Availability Modeling and Analysis of a Virtualized System [Text] / S. K. Dong, F. Machida, K. S. Trivedi // 15th IEEE Pacific Rim International Symposium on Dependable Computing PRDC '09, 2009. – P. 365 – 371.

10. Муляр І.В. Розробка математичної моделі та методу її вирішення для підвищення ефективності використання обчислювальних ресурсів на основі технології віртуалізації / І.В. Муляр , Г.В. Гусляков , Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 54. – С. 134-143.

11. Peer-to-peer network [Electronic resource]. – Access mode: http://www.infosec.gov.hk/english/technical/files/peer.pdf. – 10.04.2016.

12. Srisuresh, P. RFC 5128. State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs) [Text] / P. Srisuresh, B. Ford, D. Kegel // The Internet Engineering Task Force (IETF), 2008. – 32 p.

13. Муляр, І.В. Модель оцінки ймовірнісно-часових характеристик інформаційної взаємодії в мережі інтернет речей / І.В. Муляр, О.В. Сєлюков, В.М. Джулій, Б.М. Кізюн // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. № 63. – С.96-107.

14. Zhou, Y. Kad-D: An Improved Model Based on Kademlia [Text] / Y. Zhou, S. Liu, and G. Huang. // Multimedia Information Networking and Security (MINES). – 2011. – P. 123 – 127.

REFERENCES:

1. Tekhnolohyy Web, Grid, Cloud dlia harantosposobnыkh YT-ynfrastruktur [Tekst] : monohrafyia / V. S. Kharchenko y dr; Kharkov. nats. aэrokosm. un-t ym. N. E. Zhukovskoho. – «KhAY», 2013. – 868 s.

2. Muliar I.V. Analiz problem zabezpechennia funktsionalnoi bezpeky informatsiinykh system obrobky danykh / I.V. Muliar, A.V. Dzhulii, M.V. Kostiuk // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh: Mizhnarodnyi naukovo-tekhnichnyi zhurnal. -Khmelnytskyi, 2013.-№1 -S. 133-138.

3. Rizhkova, O. V. Sravnytelnыi analyz эffektyvnosty yspolzovanyia alhorytmov yzmenenyia razmera okna perehruzok v setiakh Cloud Computing [Tekst] / O. V. Rizhkova // Radioelektronni i kompiuterni systemy. – 2012. – № 7(59). – S. 73 – 78.

4. Muliar I.V. Metod predykatyvnoi identyfikatsii protsesiv dlia zakhystu vid prykhovanykh zahroz v seredovyshchi khmarnykh obchyslen / S.V. Lienkov, V.M. Dzhulii, O.V. Seliukov, I.V. Muliar // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2017. – Vyp. № 55. – C. 145-154.

5. Yanovskaia, O. V. Modely nadezhnosty komponentov oblachnoho data-tsentra [Tekst] / O. V. Yanovskaia, V. S. Kharchenko // Visnyk Kharkivskoho natsionalnoho tekhnichnoho universytetu silskoho hospodarstva imeni Petra Vasylenka "Problemy enerhozabezpechennia ta enerhozberezhennia v APK Ukrainy". – 2014. – Vыp. 154. – S. 86 – 88.

6. Yanovskaia, O. V. Modely dostupnosty servysov raspredelennыkh oblachnыkh system [Tekst] / O. V. Yanovskaia // Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy.– 2016. – № 1(22). – S. 124 – 130.

7. Lenkov S.V. Dynamichni pokaznyky otsinky rivnia funktsionalnoi bezpeky informatsiinoi systemy / S.V. Lienkov , V.M. Dzhulii , I.V. Muliar // Suchasna spetsialna tekhnika. Naukovo praktychnyi zhurnal. - DNDI MVS Ukrainy, 2016. - Vyp. №2(45). - C.59-67.

8. Muliar I.V. Metod nadannia dostupu do servisiv odnoranhovoi rozpodilenoi khmarnoi systemy / I.V. Muliar, A. S. Sivak // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh.-2019.- № 1 (63).-S. 68-73

9. Dong, S. K. Availability Modeling and Analysis of a Virtualized System [Text] / S. K. Dong, F. Machida, K. S. Trivedi // 15th IEEE Pacific Rim International Symposium on Dependable Computing PRDC 09, 2009. – P. 365 – 371.

10. Muliar I.V. Rozrobka matematychnoi modeli ta metodu yii vyrishennia dlia pidvyshchennia efektyvnosti vykorystannia obchysliuvalnykh resursiv na osnovi tekhnolohii virtualiz / I.V. Muliar , H.V. Husliakov , L.V. Solodieieva // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2016. – Vyp. № 54. – C. 134-143.

11. Peer-to-peer network [Electronic resource]. – Access mode: http://www.infosec.gov.hk/english/technical/files/peer.pdf. – 10.04.2016.

12. Srisuresh, P. RFC 5128. State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs) [Text] / P. Srisuresh, B. Ford, D. Kegel // The Internet Engineering Task Force (IETF), 2008. – 32 p.

13. Mulyar I.V., Selyukov O.V., Dzhuliy V.M. and Kizyun B.M.(2019) “Model′ otsinky ymovirnisno-chasovykh kharakterystyk informatsiynoyi vzayemodiyi v merezhi internet rechey” [Model of estimation of probabilistic-temporal characteristics of information interaction in the Internet of things network], Zbirnyk naukovyh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka, №63, pp.96-107.

14. Zhou, Y. Kad-D: An Improved Model Based on Kademlia [Text] / Y. Zhou, S. Liu, and G. Huang. // Multimedia Information Networking and Security (MINES). – 2011. – P. 123 – 127.

Ph.D. Klots Yu.P., Ph.D. Muliar I.V., Ph.D. Cheshun V.M., Burdyug O.V.

USE OF DISTRIBUTED HASH TABLES TO PROVIDE ACCESS TO CLOUD SERVICES

In the article the urgency of the problem of granting access to services of distributed cloud system is disclosed, in particular, the peer distributed cloud system is characterized. The process of interaction of the main components is provided to access the domain name web resource. It is researched that the distribution of resources between nodes of a peer distributed cloud system with the subsequent provision of services on request is implemented using the Kademlia protocol on a local network or Internet and contains processes for publishing the resource at the initial stage of its owner, replication and directly providing access to resources.

Application of modern technologies of adaptive information security systems does not allow full control over the information flows of the cloud computing environment, since they function at the upper levels of the hierarchy. Therefore, to create effective mechanisms for protecting software in a cloud computing environment, it is necessary to develop new threat models and to create methods for displaying computer attacks that allow operatively to identify hidden and potentially dangerous processes of information interaction.

Rules of access form the basis of security policy and include restrictions on the mechanisms of initialization processes access. Under the developed operations model, the formalized description of hidden threats is reduced to the emergence of context-dependent transitions in the multigraph transactions.

The method of granting access to the services of the distributed cloud system is substantiated. It is determined that the Distributed Hash Table (DHT) infrastructure is used to find a replication node that has a replica of the requested resource or part of it. The study identified the stages of identification of the node's validation. The process of adding a new node, validating authenticity, publishing a resource, and accessing a resource is described in the form of a step-by-step sequence of actions within the framework of the method of granting access to services of a distributed cloud system by graphical description of information flows, interaction of processes of information and objects processing.

Keywords: method, cloud system, hash tables.

к.т.н., доц. Кльоц Ю.П., к.т.н., доц. Муляр И.В., Чешун В.Н., Бурдюг О.В.

ИСПОЛЬЗОВАНИЕ РАСПРЕДЕЛЁННЫХ ХЕШ-ТАБЛИЦ ДЛЯ ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ОБЛАЧНЫХ СЕРВИСОВ

В статье раскрыты актуальность проблемы предоставления доступа к сервисам распределенной облачной системы, в частности, охарактеризованы одноранговую распределенную облачную систему. Подано процесс взаимодействия основных компонентов для доступа к веб-ресурса с доменным именем. Доказано, что распределение ресурсов между узлами одноранговой распределенной облачной системы с последующим предоставлением сервисов по запросу реализуется с помощью протокола Kademlia в локальной сети или сети Интернет и содержит процессы публикации ресурса на начальной стадии его владельцем, репликации и непосредственно предоставления доступа к ресурсам.

Применение современных технологий адаптивных систем защиты информации не позволяет осуществлять полный контроль за информационными потоками среды облачных вычислений, поскольку они функционируют на верхних уровнях иерархии. Поэтому для создания эффективных механизмов защиты ПО в среде облачных вычислений требуется разработка новых моделей угроз и создания методов отображения компьютерных атак, которые позволяют оперативно идентифицировать скрытые и потенциально опасные процессы информационного взаимодействия.

Правила разграничения доступа, составляют основу политики безопасности, включают и ограничения на механизмы инициализации процессов доступа. В рамках разработанной модели операций формализованное описание скрытых угроз сводится к появлению контекстно-зависимых переходов в мультиграфом транзакций.

Обоснован метод предоставления доступа к сервисам распределенной облачной системы. Определено, что для поиска узла репликации, который имеет реплику запрашиваемого ресурса или его часть, применяется инфраструктура распределенных хеш таблиц. В исследовании определены этапы валидации идентификатора узла. Описаны процессы добавления нового узла, валидации подлинности, публикации ресурса и получения доступа к ресурсу представлен в виде поэтапной последовательности действий в рамках метода предоставления доступа к сервисам распределенной облачной системы с помощью графического описания информационных потоков, взаимодействия процессов обработки информации и объектов.

Ключевые слова: метод, облачная система, хеш-таблицы.

УДК 621.396.967

к.військ.н. **Нікіфоров М.М.** (ВІКНУ)
Нікіфоров М.М.

DOI: https://doi.org/10.17721/2519-481X/2020/67-10

АНАЛІЗ ЧИННИКІВ КОМУНІКАЦІЇ, ЩО ЗАСТОСОВУЄТЬСЯ ПІД ЧАС РОЗРОБЛЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ НА БАЗІ СІМЕЙСТВ ArcGIS

В роботі проведено аналіз особливостей використання чинників комунікацій що застосовується на робочому місці під час розроблення інформаційної системи на базі сімейства ArcGIS. У цій статті викладено кілька основних чинників комунікації та проведено дослідження, як покращити спілкування між різними категоріями людей враховуючи їх підхід, послідуючий вплив та наслідки. Досліджено ймовірні підходи до врахування окремих чинників комунікації, з метою ефективного впливу на людей та команди під час розроблення автоматизованої системи моніторингу інформаційного простору.

Досліджені можливості застосування взаємозв'язків між чинниками, підходами, впливами та наслідками комунікації що можуть допомогти вдосконалити наші навички спілкування та листування у слуханні, письмі та розмові. Визначено, що оскільки кожен з нас відрізняється особистими характеристиками, віком та національною культурою, ми повинні бути проникливими спостерігачами за тими, з ким ми плануємо взаємодіяти, і уважно слухати та налаштовувати методи комунікації для нашого кінцевого одержувача. Різноманітність культур може з різною мірою впливати на безперебійність кожного підходу до спілкування та розуміння намірів, проблем та перспектив один одного. Це, у свою чергу, впливає на стосунки між колегами, між начальниками та підлеглими.

Надано висновок що чинники комунікації переплітаються між собою і впливають на наш вибір методів комунікації та середовища, що згодом спричиняє вплив на взаєморозуміння та ефективність передачі інформації. У свою чергу, наслідки накопичуються, що призводить до значних труднощів для робочих відносин та продуктивності праці.

Ключові слова: чинники комунікації, підходи, впливи, наслідки.

Вступ. В сучасних умовах розвитку суспільства інформаційно-комунікаційні технології охоплюють усі сфери життя людей. Вони дуже швидко перетворилися на життєве важливий

елемент розвитку не тільки економіки, соціальної сфери, а й всіх інших видів діяльності. Зараз практично неможливо знайти таку сферу людської діяльності, в якій би не використовувались інформаційно-комунікаційні технології. Будь-які взаємовідносини між працівниками на різних рівнях управління базуються на комунікаціях, які також формують відповідний соціально-психологічний клімат в колективі. Комунікаційна система підприємства формується і розвивається внаслідок впливу людського чинника. Якість, швидкість, точність та ефективність управлінських рішень працівників такої системи значною мірою зумовлює досягнення цілей її функціонування.

У наукових напрацюваннях щодо системи комунікацій є чимало категорій, у трактуванні яких і застосуванні у наукових дослідженнях немає одностайності. З огляду на зазначене важливим є уточнення категорійного апарату, який застосовується при дослідженні комунікаційної системи. Першочергово увагу доцільно зосередити на розгляді семантики категорії «комунікація». Як зауважує Є. Романенко, це поняття походить від латинського «communication», що перекладається як передача, повідомлення, бесіда [1].

Зростаючі можливості використання сучасних інформаційних технологій змушують переглянути традиційні підходи до використання засобів та методів для аналізу наявних факторів комунікації щодо підвищення ефективності виконання інформаційних заходів. За цих обставин, виникає необхідність застосування нових технологій управління силами та засобами Збройних Сил для аналізу та прийняття рішень, відображення ситуацій, що склалися. Вони дають можливість прогнозувати можливі варіанти розвитку подій та пропонувати командирам будь якого рівня різні шляхи досягнення оптимального результату.

Для вирішення таких завдань необхідно використовувати технології, які ефективно поєднують простір та час зі значними за обсягом супутніми даними у вигляді атрибутивної інформації щодо об’єктів оперативної обстановки, довідкової інформації про театр (район) ведення бойових дій, кліматичні умови, дані розвідки та ін. Саме для вирішення подібних завдань в арміях багатьох держав світу використовуються геоінформаційні технології [2].

Геоінформаційні забезпечення системи управління повинне використовувати функціональні компоненти, які вбудовуються у відкриту, розширювану програмно-апаратну платформу для досягнення інтероперабільності використання просторово розподіленої інформації, використовуючи стандартні правила в рамках базових послуг, які підтримують обмін повідомленнями, перетворення даних за для подальшого їх поширення (розповсюдження) шляхом публікації та підписки на стандартні та спеціально створені шаблони проектування [3].

Україні необхідні сучасні, інформаційні технології (ІТ) на базі сімейства ArcGIS, інфраструктурне побудовані на ІТ-стандартах обробки та роботи по їх розробки з врахуванням організації комунікації робочого міста.

Аналіз останніх досліджень і публікацій, постановка задачі. Вагомий внесок у розроблення теоретико-прикладних положень у сфері інформаційно-комунікаційного менеджменту зробило чимало вітчизняних та зарубіжних науковців, серед яких варто виокремити праці Kourdi, J., Kim, J., & de Dear, R, Eccles, M., Smith, J., Tanner, M., Van Belle, J, Молочник, Ю. [7 - 10]. Основними науковими доробками О.Є. Кузьмін та О.Г. Мельник у цій сфері є розвиток сутності поняття «комунікації», класифікування видів комунікацій, ідентифікування складових елементів комунікаційної системи, особливості використання чинників комунікацій тощо [4]. Вагомий науковий доробок Н. Шпака розкриває проблему формування національного інформаційного простору [5].

Водночас, вагомий науковий доробок цих авторів лише фрагментарно розкриває проблему активізування діяльності працівників комунікаційної системи. Зокрема, потребує дослідження особливостей використання чинників комунікацій в інформаційної технології та їх вплив на взаєморозуміння та ефективність передачі інформації. У цій статті викладено кілька основних чинників комунікації та досліджено, як покращити спілкування, розуміючи їх відповідний підхід та послідуючий вплив та наслідки на людей та команди.

Мета роботи – дослідити значення чинників комунікацій в інформаційної технології та їх вплив на взаєморозуміння та ефективність передачі інформації.

Виклад основного матеріалу. Як відомо з теорії менеджменту, на підприємствах виокремлюють три рівні управління: технічний, управлінський та інституційний, яким, відповідають три групи працівників: працівники низової ланки, працівники середньої ланки та працівники вищої ланки [4]. Таким чином, працівники комунікаційної системи в компаніях можуть також належати до будь-якого з цих рівнів управління (наприклад, IT-директор – це представник інституційного рівня управління організації).

Організаційна комунікація на робочому місці має вирішальне значення як для індивідуального, так і для організаційного робочого процесу. Організації значно взаємодіють з різними функціональними та проектними зацікавленими сторонами різних структур та культур у світовій економіці. Таким чином, наша безперебійність передачі повідомлень впливає на плинність передач повідомлень, а отже, на ефективність їхніх намірів.

До чинників, що висвітлюються у цій статті, належать: ефективність та результативність, мета та важливість, характер чутливості, структура та культура та розуміння аудиторії. Загальні підходи до досліджуваного спілкування включають: push-метод, pull-метод, mass-метод, міжособистісність та інтерактивність [6]. З безліччю варіантів засобів середовища, доступних для організаційного спілкування, неминуче те, як ми підходимо до комунікації, що впливає на наші знання спілкування та на плинність потоків передачі. Це, в свою чергу, впливає на розуміння намірів та перспектив відправника та одержувача.

Слідом за цим виникають суттєві ефекти на стосунки колег, відносини начальників та підлеглих, а також міжфункціональна співпраця та внески, які можуть впливати на продуктивність проектних команд під час розроблення інформаційної системи на базі сімейства ArcGIS під час розроблення інформаційної системи на базі сімейства ArcGIS (таблиця 1).

Таблиця 1

Чинники, підходи, вплив та наслідки комунікації

Чинники	**Підходи**	**Вплив**	**Ефекти**
Ефективність та результативність; важливість та ціль комунікації; чутливість характеру; організаційна структура та культура; розуміння аудиторії.	Push-метод; pull-метод; mass-метод; міжособистісний; інтерактивний.	Плинність потоків передачі; розуміння намірів та перспектив відправника та одержувача.	Відносини колег; відносини начальників та підлеглих; міжфункціональна співпраця та внески; індивідуальна та командна продуктивність.

Ефективність та результативність. Ефективна передача передає повідомлення негайно, при цьому відправник переходить до інших завдань після відправлення повідомлення. Текстові повідомлення, електронні листи та голосові повідомлення можуть бути життєздатними методами, оскільки вони дозволяють відправнику здійснювати зручне та швидке спілкування.

Однак важливо зауважити, що використання ефективних методів зв’язку з точки зору швидкості передачі не обов'язково забезпечує ефективність через відсутність циклів зворотного зв’язку та підтвердження особистості. Коли призначені одержувачі не отримали повідомлення вчасно та задуманим чином, ефективність недостатня.

Коли завдання є критичним, гарантія успіху - залучати більше одного середовища. Повідомлення електронної пошти разом з телефонним дзвінком може зайняти час, але це дає

більше гарантії та ефективності, ніж просто відіслати email. Коли одержувач та відправник розвивають взаєморозуміння та бачення, поточні та текучі комунікаційні потоки вмикаються, що, в свою чергу, дає можливість взаєморозуміння.

Згодом наслідки цього тягнуть за собою позитивні наслідки виховання міцних і здорових робочих відносин між обома сторонами. Отже, обидві сторони здатні забезпечити згоду та співпрацю, готові ділитися відповідною інформацією та уважно стежити, тим самим підвищуючи продуктивність. Це вимагає часу та зусиль, але є ефективним у довгостроковій перспективі.

Ми повинні врахувати деякі можливі непередбачені технічні проблеми, такі як повідомлення електронної пошти, які потрапляють в корзину або спам, спільну платформу, де відео не підключається, або проблеми зі зберіганням даних для комунікації проектів. Це може не лише знизити ефективність, але й привести до безрезультативності, а отже, впливає на робочі стосунки та спричиняє зниження продуктивності праці. Такі альтернативи, як електронні листи та роздруківки, стануть у нагоді у випадку несправності платформи, особливо у віддалених проектних командах.

Мета та значення спілкування. Ступінь ефективності та результативності передачі залежить від відправника для визначення мети взаємодії з одержувачем. Теми, які є рутинними або невідкладними, які потрібно розповсюджувати безпосередньо певним одержувачам, можуть принести найбільше користі від push-методу, який стосується цільової масової аудиторії [6]. Push-комунікація не означає підштовхування або примушування одержувачів до інформації. Швидше, відправники ініціюють доставку повідомлень одержувачам, коли метою є поширення інформації, яка не потребує негайної відповіді або характер повідомлення не є терміновим.

Однак усне підтвердження електронної пошти та подальші дії від одержувачів після перегляду повідомлень будуть потрібні. Електронні листи, нагадування та повідомлення в бюлетенях - приклади push-методу, який використовується для ефективної передачі інформації для таких цілей, як поширення етапів проекту та оновлення та видача нагадувань про політику компанії щодо використання збалансованих щорічних відпусток працівникам. Немає особливої необхідності розширити комунікацію на інтерактивний підхід, коли наміром є розповсюдження звичайної інформації.

Pull-метод є оптимальним, коли метою одержувачів є доступ до контенту на власний розсуд, наприклад, самостійне навчання, доступ до бази знань про проект та отримання проектних завдань [6]. “Pull-комунікація” не означає примушувати або вимагати, щоб отримувачі читали повідомлення. Швидше за все, pull-підхід забезпечує рівний або загальний доступ для одержувачів від великої аудиторії для отримання необхідної інформації для використання у бажаний час та локації.

Таким чином, це дозволяє їм оптимально вивчати та розуміти повідомлення. Якщо одержувач не читає повідомлення спочатку, це не впливає на проект. Характер повідомлення є інформаційним, і користувачі можуть отримувати повідомлення, коли виникає потреба. Приклади pull-методу включають електронне навчання, знання репозиторіїв та програмного забезпечення для планування.

Найважливіші внутрішні чи зовнішні організаційні зміни потребують підтримку зацікавлених сторін, і тому активна участь та оцінка є важливими видами діяльності, які потребують ретельного обговорення з оцінкою як вербальної, так і невербальної комунікації. Обговорення та впровадження організаційних змін виходить за рамки розповсюдження інформації; це вимагає управління та контролю процесу змін.

Для цього необхідне регулярне спілкування з циклами зворотного зв’язку та подальшими завданнями, оскільки це забезпечує ефективну можливість для інших обговорювати вплив змін на їх трудову діяльність, навіть якщо це може бути неефективним за тривалий час [7].

Інструменти комунікації на робочому місці є більш різноманітними та досконалими, ніж будь-коли. Інтерактивні інструменти, такі як дискусійні форуми, програми зв’язку та програмне забезпечення соціальної інтрамережі, мають всебічні та інтерактивні функції [6]. Розвиток комп'ютерних і телефонних технологій розширює спектр варіантів для полегшення надсилання та отримання повідомлень. Інструменти для передачі оновлень та звітів колегам, начальству, клієнтам та постачальникам у режимі реального часу, віртуального та поточного часу є життєве важливими для успішної доставки та отримання призначених повідомлень.

Природа чутливості. Якщо мета повідомлення стосується конфіденційного питання, доцільно шукати більш приватну форму спілкування, яка дозволяє сторонам шукати та надавати зворотній зв'язок лише між собою. Конфіденційні повідомлення слід обробляти делікатно прямим способом - особисто чи телефоном у приватній розмові. Деякі приклади включають оцінку ефективності працівників, сповіщення тих, хто пропустив рекламні акції, та розслідування працівників щодо порушень політики. Колеги похилого віку можуть сприймати отримання інформації через технологічні пристрої як неповагу, особливо коли вона має важливий та конфіденційний характер [8].

Однак, конфіденційні повідомлення є суб'єктивними для окремих людей, оскільки можна мати різний погляд на характер чутливості. Отже, врахуйте точку зору одержувача. Хоча важко передати погані новини, нам потрібно дотримуватися ділового та соціального протоколу приватної розмови з активним слуханням. Це передбачає чітке розуміння, уточнення та підтвердження та визнання один одного для усунення бар'єрів [6]. Це дозволяє двом сторонам взаємодіяти в режимі реального часу та багатше з використанням жестів тіла та невербальної мови, які несуть емоційні підказки [9].

Невикористання відповідних каналів комунікації та вирішення конфіденційних тем дипломатичним шляхом призведе до недовіри та згодом може завдати шкоди робочим відносинам.

Організаційна структура та культура. Коли ієрархічний рівень організаційної структури високий, комунікація, ймовірно, проходить через кілька рівнів відповідно до ієрархічного ланцюга. Інформація може застарівати або спотворюватися, коли вона тече вгору і вниз по ієрархії, і, таким чином, впливає на видимість [9]. Отже, необхідно перевірити та переконатися, що інформація, яку ми маємо під рукою, є актуальною та найточнішою, перш ніж надсилати її наступним одержувачам. Коли організація має декілька функцій, кожна з яких має свою ієрархію, функції розвивають різні орієнтації субодиниць і, таким чином, віддаляються одна від одної і викликають проблеми спілкування.

Пріоритетом інженерної функції є підвищення технічної вдосконаленості продукту за допомогою оптимізованих конфігурацій та матеріалів. Пріоритетом функції продажу є необхідність пристосовуватися до коливаючих потреб клієнтів і швидко їх задовольняти, щоб досягти цілей продажів та збільшити дохід. Пріоритетом логістики є забезпечення оптимальної якості та кількості сировини на заводі для виготовлення готової продукції та доставки клієнтам вчасно [11].

Отже, нам потрібно поставити себе перед перспективами одержувачів і продумати спільну організаційну мету чи бачення, перш ніж формувати наше повідомлення. Організації можуть розвиватися або змінюватися до більш органічної та децентралізованої структури, щоб заохотити людей бути більш ініціативними та докладати більше зусиль у спілкуванні [10].

Організаційна культура - це сукупність спільних цінностей та поведінки працівників, які спрямовують взаємодію членів організації з внутрішніми функціями та зовнішніми сторонами [12]. Структура, політика та люди організації формують та контролюють її культуру. Висока бюрократична структура, складна політика та мережа, а також люди з різних країн чи різних часових поясів впливають на робочу культуру різноманітними мотиваційними факторами та питаннями координації.

Отже, розвиток згуртованого середовища із здоровими каналами комунікації призведе до сприяння взаємній синергії, яка заохочує працювати над спільним баченням. Виховання

такої позитивної культури дозволяє взаєморозуміти і, таким чином, створює певну гнучкість у підходах до передачі. Тим не менш, ми повинні бути максимально послідовними у використанні підходів для підтримки міжфункціональної співпраці та внеску.

Особисті характеристики

Звично спілкуватися з людьми через засоби комунікації, в яких обом або всім сторонам найбільш комфортно. Якщо ми віддаємо перевагу міжособистісному спілкуванню під час взаємодії з іншими, ми будемо схильні до особистих розмов особистого дотику [6]. І навпаки, якщо відправник та отримувач віддають перевагу зручності користування смартфоном, відправник, швидше за все, підбере пристрій, щоб звернутися до отримувача.

Перш ніж це зробити, важливо врахувати адресата повідомлення. Зазвичай візит планується чи відбувається експромтом? Вони зазвичай надсилають вам повідомлення електронною поштою, телефонують або безпосередньо звертаються до вас? Оскільки такі форми поведінки пропонують комунікативні підходи та часові уподобання, що іншим зручніше, слідування їм та досягнення консенсусу допомагає полегшити більш плавний комунікаційний потік. Легше буде передати та зрозуміти конкретні відповіді, які мають складний характер та підтримувати взаємну довіру при передачі повідомлень зручним для одержувача методом.

Вікове різноманіття

Різноманітність вікової робочої сили сьогодні дає можливість працівникам вивчити цифрову компетентність та розширити свій репертуар для спілкування. Міленіали, або покоління Y, - це працівники від двадцяти до тридцяти років, які, як правило, більше звикли до цифрового мислення, ніж інші вікові групи.

Отже, з більшою ймовірністю вони охоплюють новітні технології комунікацій, такі як програмне забезпечення соціальної мережі з інтерактивним створенням мультимедіа та можливістю обміну файлами або чат-боти зі штучним інтелектом (AI) з можливостями машинного навчання. Незважаючи на те, що деякі міленіали можуть бути менш кваліфікованими, вони все-таки шукають коучинг та наставництво щодо бажаних тем та навичок.

Покоління X, співробітники від сорока до п’ятдесяти років, яким зручно використовувати стандартні організаційні методи як рутинну форму спілкування з акцентом на результати. Вони мають досвід роботи з молодшими та старшими колегами та пройшли декілька технологічних розробок. Поєднання традиційної та сучасної комунікації для цього покоління може мати позитивний вплив на продуктивність індивідуумів, команди та організації.

Бебі-бумери, це співробітники від п’ятдесяти до семидесяти років, володіють розумною працелюбністю та сплатою мита. Співробітники цієї вікової групи цінують професійну ввічливість розмов віч-на-віч та отримання новин таким чином, що дозволяє двосторонній трафік при невербальному спілкуванні з використанням жестів тіла. Варто зазначити одне: ми повинні розглядати різні вікові групи як орієнтир, а не стереотипувати їх, оскільки характеристики та значення окремих людей різняться [13].

Культурне різноманіття

Розглянемо також культурне різноманіття членів команди проекту. Стилі спілкування мають різні трактування, залежно від національних культур [14]. Наприклад, використання зорового контакту, повага та уважність в американській культурі, що в азіатській культурі розглядається як неповага, особливо при спілкуванні з кимось із вищого статусу.

Американцям, швидше за все, буде комфортне пряме спілкування, яке відрізняється від інших культур, які вважають за краще використовувати мову тіла та невербальні підказки, а не прямі заяви. Отже, культурне розмаїття впливатиме на комунікативні підходи та часові уподобання.

Різноманітність культур може з різною мірою впливати на безперебійність кожного підходу до спілкування та розуміння намірів, проблем та перспектив один одного. Це, у свою

чергу, впливає на стосунки між колегами та між начальниками та підлеглими. Примітка. Ми повинні розглядати різні риси культури як орієнтир, а не стереотипувати їх, оскільки характеристики та значення окремих людей різняться [14].

Оскільки структури та культури організацій різняться, нам потрібно сформувати наше повідомлення для досягнення загальних організаційних цілей та виробити позитивне робоче середовище із взаємною синергією, яка призводить комунікацію до взаємодії. Повідомлення, які мають важливий, конфіденційний або складний характер, потребують більш насиченої форми взаємодії, яка охоплює обмін інформацією та обробку емоційних сигналів, а також двосторонній чи багатосторонній зворотній зв'язок. Це забезпечить ефективний обмін комунікаціями, навіть якщо він не є ефективним у короткий термін [15]. Перевірка з одержувачем до або після надсилання повідомлення може бути непростим та неефективним, але це може забезпечити чітке повідомлення та зобов'язання обох сторін. Підготовка альтернативних комунікацій стане у нагоді у випадку несправності платформи.

Оскільки кожен з нас відрізняється особистими характеристиками, віком та національною культурою, ми повинні бути проникливими спостерігачами за тими, з ким ми плануємо взаємодіяти, і уважно слухати та налаштовувати методи комунікації для нашого кінцевого одержувача.

Інші чинники, такі як емоційний стан відправника та одержувача, навички письма, вміння говорити та знання теми повідомлення тощо – не охоплені цією статтею.

Висновки

1. Чинники комунікації переплітаються між собою і впливають на наш вибір методів комунікації та середовища, що згодом спричиняє вплив на взаєморозуміння та ефективність передачі. У свою чергу, наслідки накопичуються, що призводить до значних наслідків для робочих відносин та продуктивності праці.

2. Тому вивчення взаємозв'язків між чинниками, підходами, впливами та наслідками комунікації може допомогти вдосконалити навички спілкування та листування у слуханні, письмі та розмові.

ЛІТЕРАТУРА:

1. Романенко Є.О. Теоретико-методологічна ідентифікація поняття комунікації у контексті сучасних дослідницьких підходів. Ефективність державного управління. – 2012. – Вип.38. – С.108-115.

2. Сосса Р.І. Сучасні виклики до топогеодизичного та картографічного забезпечення сектору безпеки та оборони держави / Р.І. Сосса, Ю.І. Голубінка. / Вісник Київського національного університету імені Тараса Шевченка військово-спеціальні науки – К., 2017. – Вип. 1(36). – С. 20-23.

3. Хірх–Ялан В. І. Метод аналізу ієрархій для оцінки пріоритетності показників стану місцевості в районі відповідальності для прийняття рішення на розміщення підрозділу / В. І.Хірх–Ялан // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К. : ВІКНУ, 2012. – Вип. № 39. – С. 353–359.

4. Кузьмін О.Є., Мельник О.Г. Основи менеджменту: Підручник. – Київ. "Академвидав", 2003. – 416 с.

5. Шпак Н.О. Комунікаційний менеджмент: сутність та розвиток / Н. О. Шпак // Економіка та держава. – 2010. – № 2. – С. 30-33. http://nbuv.gov.ua/UJRN/ecde_2010_2_9.

6. Project Management Institute (PMI). (2017). A guide to the project management body of knowledge (PMBOK® guide) – Sixth edition. Newtown Square, PA: Author.

7. Kim, J., R. Dear (2013, December). Workspace satisfaction: The privacy-communication trade-off in open-plan offices. Journal of Environmental Psychology, 36, December 2013, pp.18-26.

8. Eccles, M., Smith, J., Tanner, M., Van Belle, J. P., & van der Watt, S. (2010). The impact of collocation on the effectiveness of agile is development teams. IBIMA Publishing.

9. Kourdi, J. (2015): Business strategy: A guide to effective decision-making (The economist series), (3rd ed.). New York, NY: Public Affairs Publishing.

10.Молочник, Ю.Б., Використання системи збалансованих показників для оцінювання вмінь працівників комунікаційної системи підприємств. Вісник Національного технічного університету «Харківський політехнічний інститут»: збірник наукових праць. Серія: «Стратегічне управління, управління портфелями, програмами та проектами». – Х., 2015. – №2. – С.166-172.

11.Pejtersen J. H., Feveile, H., Christensen, K. B., & Burr, H. (2011, September). Sickness absence associated with shared and open-plan offices – A national cross-sectional questionnaire survey. Scand J Work Environ Health. 37(5), 376-382.

12.Robbins, S. P., & Judge, T. A. (2014). Organizational behavior. (12th ed.). Essex,UK: Pearson Education Limited.

13.James, G. (2016). 9 reasons that open-space offices are insanely stupid. Inc. Magazine.

14.Steers, R. M., Nardon, L., & Sanchez-Runde, C. J. (2013). Management across cultures: Developing global competencies. (2nd ed.). New York, NY: Cambridge University Press.

15.Melo, C. O., Cruzes, D. S., Kon, F., & Conradi, R. (2013, February). Interpretative case studies on agile team productivity and management. Information and Software Technology, 55(2), 412-427.

REFERENCES:

1. Ye.O., Romanenko (2012). Teoretyko-metodolohichna identyfikatsiia poniattia komunikatsii u konteksti suchasnykh doslidnyts'kykh pidkhodiv. [Theoretical and methodological identification of the concept of communication in the context of modern research approaches.] Efektyvnist' derzhavnoho upravlinnia, 32, p.p.108-115. [in Ukrainian].

2. R.I., Sossa, Yu.I., Holubinka (2017). Suchasni vyklyky do topoheodyzychnoho ta kartohrafichnoho zabezpechennia sektoru bezpeky ta oborony derzhavy. [Modern calls to topographical geodesy and cartographic providing to the sector of safety and defensive of the state] Visnyk Kyivs'koho natsional'noho universytetu imeni Tarasa Shevchenka vijs'kovo-spetsial'ni nauky. Kyiv, No. 1(36), pp. 20-23. [in Ukrainian].

3. V. I., Khirkh–Yalan. (2012). Metod analizu iierarkhij dlia otsinky priorytetnosti pokaznykiv stanu mistsevosti v rajoni vidpovidal'nosti dlia pryjniattia rishennia na rozmischennia pidrozdilu [Method of analysis of hierarchies for the estimation of priority of indexes of the state of locality in the district of responsibility for a decision-making on placing of subdivision]. Zbirnyk naukovykh prats' Vijs'kovoho instytutu Kyivs'koho natsional'noho universytetu imeni Tarasa Shevchenka. Kyiv, No. 39, p.p. 353–359. [in Ukrainian].

4. O.Ye., Kuz'min, O.H., Mel'nyk (2003). Osnovy menedzhmentu [Fundamentals of Management] Pidruchnyk. Kyiv. Akademvydav, 416 p. [in Ukrainian].

5. N. O., Shpak (2010) Komunikatsijnyj menedzhment: sutnist' ta rozvytok [Communication management: essence and development] Ekonomika ta derzhava, No.2., p.p. 30-33. http://nbuv.gov.ua/UJRN/ecde_2010_2_9.

6. Project Management Institute (PMI). (2017). A guide to the project management body of knowledge (PMBOK® guide) – Sixth edition. Newtown Square, PA: Author.

7. J., Kim, R., Dear, (2013) Workspace satisfaction: The privacy-communication trade-off in open-plan offices. Journal of Environmental Psychology, No 36, p.p.18–26.

8. M., Eccles, J., Smith, M., Tanner, J. P., Van Belle, S., Watt,. (2010). The impact of collocation on the effectiveness of agile is development teams. IBIMA Publishing.

9. J., Kourdi, (2015): Business strategy: A guide to effective decision-making (The economist series), (3rd ed.). New York, NY: Public Affairs Publishing.

10. Yu.B., Molochnyk, (2015) Vykorystannia systemy zbalansovanykh pokaznykiv dlia otsiniuvannia vmin' pratsivnykiv komunikatsijnoi systemy pidpryiemstv. [Using a balanced scorecard to assess the skills of employees of the enterprise communication system].Visnyk Natsional'noho tekhnichnoho universytetu Kharkivs'kyj politekhnichnyj instytut, zbirnyk naukovykh prats', No.2, p.p.166-172.

11. J. H., Pejtersen, H., Feveile, K. B., Christensen, H., Burr (2011, September). Sickness absence associated with shared and open-plan offices – A national cross-sectional questionnaire survey. Scand J Work Environ Health. , No 37(5), p.p 376–382.

12. S. P., Robbins, T. A., Judge, (2014). Organizational behavior. (12th ed.). Essex,UK Pearson Education Limited.

13. G., James (2016). 9 reasons that open-space offices are insanely stupid. Inc. Magazine.

14. R. M., Steers, L., Nardon, C. J., Sanchez-Runde (2013). Management across cultures: Developing global competencies. (2nd ed.). New York, NY: Cambridge University Press.

15. C. O., Melo, D. S., Cruzes, F., Kon, R., Conradi (2013, February). Interpretative case studies on agile team productivity and management. Information and Software Technology, No. 55(2), p.p. 412–427.

к.воен.н. Никифоров Н.Н., Никифоров Н.Н.

АНАЛИЗ ФАКТОРОВ КОММУНИКАЦИИ ПРИМЕНЯЕМЫХ ПРИ РАЗРАБОТКИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОГО ПРОСТРАНСТВА НА БАЗЕ СЕМЕЙСТВА ArcGIS

В работе проведен анализ особенностей использования факторов коммуникаций применяемых на рабочем месте при разработке информационной системы на базе семейства ArcGIS В этой статье изложены несколько основных факторов коммуникации и проведено исследование, как улучшить общение между различными категориями людей учитывая их подход, последующее влияние и последствия. Исследовано вероятные подходы к учету отдельных факторов коммуникации, с целью эффективного воздействия на людей и команды при разработке автоматизированной системы мониторинга информационного пространства.

Исследованы возможности применения взаимосвязей между факторами, подходами, воздействиями и последствиями коммуникации которые могут помочь усовершенствовать наши навыки общения и переписки в слушании, письме и разговоре. Определено, что поскольку каждый из нас отличается личными характеристиками, возрастом и национальной культурой, мы должны быть проницательными наблюдателями за теми, с кем мы планируем взаимодействовать, и внимательно слушать и настраивать методы коммуникации для нашего конечного получателя. Разнообразие культур может с разной степенью влиять на бесперебойность каждого подхода к общению и пониманию намерений, проблем и перспектив друг друга. Это, в свою очередь, влияет на отношения между коллегами, между начальниками и подчиненными.

Дано заключение что факторы коммуникации переплетаются между собой и влияют на наш выбор методов коммуникации и среды, впоследствии вызывает влияние на взаимопонимание и эффективность передачи информации. В свою очередь, последствия накапливаются, что приводит к значительным трудностям для рабочих отношений и производительности труда.

Ключевые слова: факторы коммуникации, подходы, влияния, последствия.

Ph.D. Nikiforov M.M., Snr PM Nikiforov M.M.

ANALYSIS OF COMMUNICATION FACTORS APPLIED DURING THE DEVELOPMENT OF AN ARCISIS-BASED AUTOMATED INFORMATION SPACE MONITORING SYSTEM

This paper analyzes the peculiarities of the use of communication factors used in the workplace when developing an information system based on the ArcGIS family. This article outlines some of the main communication drivers and studies on how to improve communication between different categories of people, taking into account their approach, subsequent impact, and effect. Possible approaches to the consideration of individual communication factors have been investigated to effectively influence people and teams when developing an automated information space monitoring system.

Possibilities of applying interrelationships between factors, approaches, influences, and consequences of communication have been explored that can help improve our communication and communication skills in listening, writing, and speaking. It is determined that since each of us differs in personal characteristics, age, and national culture, we must be astute observers of those with whom we plan to interact, and listen carefully and adjust the methods of communication for our final recipient. The diversity of cultures can, to varying degrees, affect the continuity of each approach to communication and understanding of each other's intentions, problems, and perspectives. This, in turn, affects relationships between colleagues, between superiors and subordinates.

It is concluded that the factors of communication intertwine with each other and influence our choice of methods of communication and environment, which subsequently causes an influence on mutual understanding and efficiency of information transmission. In turn, the consequences are cumulative, which leads to considerable difficulties for working relationships and productivity.

Keywords: communication factors, approaches, influences, consequences.

УДК 621.396.2

д.т.н., проф. **Оксіюк О.Г.** (КНУ)
д.т.н, доц. **Одарченко Р.С.** (НАУ)
к.т.н**. Даков С.Ю.** (КНУ)
Бурмак Ю.А. (Київський коледж зв'язку)
Федюра Т.В. (Киевстар)

DOI: https://doi.org/10.17721/2519-481X/2020/67-11

СТАНДАРТИ ТА ТЕХНОЛОГІЙ МЕРЕЖІ 5G І МОЖЛИВІСТЬ ЇЇ РЕАЛІЗАЦІЇ

У роботі було досліджено архітектуру мережі 5G та запропоновано варіант системи моніторингу параметрів на базі SCOM. Дану систему можна використовувати для збору та аналізу інформації про продуктивність мережі, виявлення відхилень, сповіщення про них для своєчасного усунення. Були представленні технології для використання мобільної мережі стандарту 3 GPP п'ятого покоління. Були проаналізовані та пропоновані к впровадженню. Також були досліджені сучасні можливості мережі 5го покоління та технології для їх впровадження. В роботі проаналізовані та надані рекомендації до впровадження наступних серверів. 5G мережі дають змогу значно підвищити швидкість передачі даних через різні технології радіодоступу (RAT), і за допомогою використання нових спектрів радіочастот 5G NR (New Radio). Для вирішення «Розумний будинок» (Smart Home) і «Розумна будівля» (Smart Building) доступний цілий спектр різних сервісів інтернету речей (IoT): відеоспостереження, управління та автоматизація побутової техніки, управління системами безпеки тощо. Сервіс віртуальної реальності VR (Virtual Reality) створює ілюзію переміщення людини в інший світ, впливаючи на органи чуття, перш за все на зір (VR-окуляри). Сервіс доповненої реальності AR (Augmented Reality) комбінує реальне оточення з віртуальними предметами. Ці сервіси призначені не лише для розваг, а й для науки. Мережа 5G, разом з технологією інтернету речей IoT, за допомогою промислових датчиків IIoT (Industrial Internet of things), а також за допомогою штучного інтелекту II (AI, Artificial Intelligence) здатні істотно підвищити ступінь автоматизації виробництва. При цьому з'являється можливість в режимі реального часу аналізувати великі обсяги різноманітних даних (Big Data) як на основі отриманих висновків (insights), так і з використанням машинного та глибокого навчання (Machine learning, Deep learning). До цих програм можуть відноситися, наприклад, електронна медицина (e-Health), зв'язок при надзвичайних ситуаціях (Mission Critical Communication), тактильний інтернет (Tactile Internet) та інші. Безпілотний транспорт може використовуватись як частина послуги «Розумне місто», однак, може існувати і окремо. Також на платформі 5G можлива реалізація систем допомоги водієві ADAS (Advanced Driver-Assistance Systems). Ключові слова: мобільна мережа, програмне забезпечення, середовище програмування, макро та мікро рівень, стандарти мобільних мереж, мережева архітектура, гіпервізор, моніторинг, автоматизація процесів.

Вступ. Сучасний світ вже неможливо уявити без інтернету, смартфону та інших гаджетів, які щільно увійшли в наше життя. Ці технології не лише роблять життя цікавішим але й використання інтернет-доступу дає можливість цілими підприємствами на видаленому доступі від об'єкту, моніторити стан нашого здоров'я та повідомляти лікаря заздалегідь як-що е загроза нашому життю, інтернет доступ робить можливим керування маніпуляторами, безпілотними об'єктами, дронами. Але технічні можливості мереж не мали не дозволяли нам цього, і лише мережі 5G централізованого типу згідно стандарту матимуть таку можливість, але для цього треба впровадити ряд технічних рішень.

Для коректної роботи мережі необхідно забезпечити постійний контроль за параметрами. На сьогоднішній день існує багато програмного забезпечення для моніторингу мереж, але якщо брати до уваги те, що 5G реалізується на віртуальних елементах, є доцільним використання компоненту SCOM для контролю параметрів та працездатності мережі та своєчасного усунення відхилень.

Мета і завдання виконання роботи. Дослідити архітектуру та функції мереж п'ятого покоління, розробити систему моніторингу параметрів мережі 5G.

Об’єкт дослідження – забезпечення контролю параметрів мережі 5G.

Предмет дослідження – центр моніторингу інцидентів з метою контролю параметрів та забезпечення безперервної роботи даної мережі.

Аналіз джерел. В статі [1] автор акцентує увагу на складну систему керування мобільною інфраструктурою яка складеться з багатьох інструментів та можливостей програмно-керованої мережі, але зовсім не зосереджена увага на низьку надійність мережі SDN

Багато проблем можливо вирішити за допомогою програмного забезпечення яке можливо встановити на прикладний рівень програмно-керованої мережі або 5G [2, 3].

За допомогою якого ми матимемо можливість керувати процесами та автоматизувати багато процесів мережі, в тому числи об’єднати існуючі моделі та функції.

За минулі 5 років на ринку відбулося величезна кількість злиттів / поглинань і багатообіцяючих інвестицій. Та сама обіцяна вендоро незалежність давала надію на появу стартапів в одній з найскладніших сфер в IT - мережеві технології. Ще 15-20 років тому диктат IT-гігантів Cisco, Brocade, Juniper і тд здавався непорушним. SDN обіцяли значний перерозподіл ринку. Наші колеги з NFware підрахували, що тільки в 2015 році сфера SDN та NFV привернула понад $ 600 млн інвестицій. [4]

А саме в комплексі ці моделі зможуть зменшити вартість та підняти показники мережі вилучив саме ті недоліки які не згадані в роботах на теми централізованих ПКМ.

На сьогодні багато великих корпорацій використовують технологію програмного забезпечення для керування проектами, такі як HP, Cisco, XeroX [5 - 7].

Але нажаль про системи керування комп’ютерною мережею поки що не згадуються не в вітчизняних ні в закордонних джерелах, мабуть тому що в децентралізованому вигляді це зробити дуже важко. Але на даний час ПКМ набувають велику популярність [8 - 10]

Виклад основного матеріалу статті

Дослідження архітектури мережі 5 g. Необхідність впровадження мережі 5G

Мережі 5G значно розширюють обмежений функціонал мобільних мереж попередніх поколінь. Основними функціями мереж 5G є:

Вдосконалений мобільний широкосмуговий доступ eMBB (enhanced MBB).

Надійні комунікації з низькою затримкою ULLRC (Ultra Low Latency Reliable Communication).

Масивні міжмашинні комунікації Massive IoT / IIoT, мMTC (massive Machine Type Communication).

На основі цих трьох функціональних особливостей будується все різноманіття послуг і можливостей мереж IMT2020 (5G). На рисунку нижче зображені найпоширеніші можливості [1]:

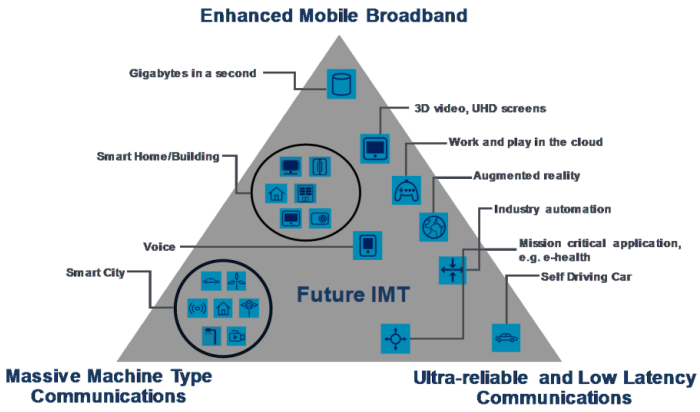

Рисунок 1 – Різноманіття функціональних можливостей мереж IMT2020 / 5G

Гігабайти в секунду. 5G мережі дають змогу значно підвищити швидкість передачі даних через різні технології радіодоступу (RAT), і за допомогою використання нових спектрів

радіочастот 5G NR (New Radio). Користувач отримує змогу користуватись практично необмеженою пропускною смугою, яка може бути використана для домашнього використання, так і для підприємств (Immersive Telepresence, Industrial IoT та ін.).

Розумний будинок. Для вирішення «Розумний будинок» (Smart Home) і «Розумна будівля» (Smart Building) буде доступний цілий спектр різних сервісів інтернету речей (IoT): відеоспостереження, управління та автоматизація побутової техніки, управління системами безпеки тощо.

Розумне місто. Рішення «Розумне місто» - розширення функціоналу та спектру сервісів «Розумного будинку». Основними сервісами «Розумного міста» є: безпечне місто, електронний банкінг e-Bank, електронний уряд e-Government, електронна освіта e-Education, електронна охорона здоров'я e-Health, «розумні електромережі» Smart Grid, тощо .

Робота в хмарі. Сервіс дає можливість не просто зберігати дані в хмарному сховищі і вилучати їх звідти, а й використовувати прикладні програми, які працюють безпосередньо в хмарі. До того ж, з можливістю їх використання на будь-якому пристрої і з будь-якого місця. Також існує можливість використання інтерфейсів прикладного програмування API, через які хмарні сервіс-провайдери можуть надавати свої послуги абонентам оператора мережі 5G.

Доповнена і віртуальна реальність (AR / VR). Сервіс віртуальної реальності VR (Virtual Reality) створює ілюзію переміщення людини в інший світ, впливаючи на органи чуття, перш за все на зір (VR-окуляри). Сервіс доповненої реальності AR (Augmented Reality) комбінує реальне оточення з віртуальними предметами. Ці сервіси призначені не лише для розваг, а й для науки.

Промислова автоматизація. Мережа 5G, разом з технологією інтернету речей IoT, за допомогою промислових датчиків IIoT (Industrial Internet of things), а також за допомогою штучного інтелекту II (AI, Artificial Intelligence) здатні істотно підвищити ступінь автоматизації виробництва. При цьому з'являється можливість в режимі реального часу аналізувати великі обсяги різноманітних даних (Big Data) як на основі отриманих висновків (insights), так і з використанням машинного та глибокого навчання (Machine learning, Deep learning).

Бізнес-критичні додатки (Mission Critical Applications). До цих програм можуть відноситися, наприклад, електронна медицина (e-Health), зв'язок при надзвичайних ситуаціях (Mission Critical Communication), тактильний інтернет (Tactile Internet) та інші.

Безпілотний транспорт (Driverless Vehicles). Безпілотний транспорт може використовуватись як частина послуги «Розумне місто», однак, може існувати і окремо. Також на платформі 5G можлива реалізація систем допомоги водієві ADAS (Advanced Driver-Assistance Systems).

В загальному, мережа 5G вбирає в себе не тільки мобільні, але також і фіксовані послуги зв'язку, а також високошвидкісний доступ в інтернет з малою затримкою (див. рис. нижче), і, крім того, спеціалізовані та корпоративні мережі для вертикальних галузей економіки [2].

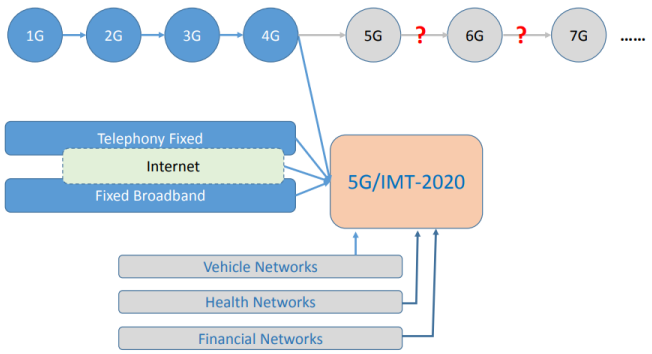

Рисунок 2 –Універсальність платформи 5G / IMT2020

У проектах «розумних міст» платформа 5G дозволить в режимі реального часу передавати інформацію з набагато більшого числа сенсорів на різних об'єктах. Старший

директор Qualcomm з продуктового менеджменту мобільних технологій Санджив Аталі (Sanjeev Athalye) відзначає, що можна буде розгорнути тисячу сенсорів замість сотні, для обслуговування яких буде достатньо меншої кількості базових станцій, ніж при існуючих нині мережах. Це можуть бути, наприклад, сенсори моніторингу стану об'єктів, сенсори «розумного освітлення» або сенсори звуку, встановлені з метою безпеки і дотримання порядку в місті. В останньому випадку сенсори можуть фіксувати підозрілі або занадто гучні звуки, і дана інформація буде автоматично передаватися в служби охорони правопорядку.

Сервіси 5G можуть бути застосовані і в медицині для організації віддаленого моніторингу стану пацієнтів. Лікар зможе оперативно отримувати інформацію з спеціальних сенсорів і стежити за станом пацієнтів цілодобово.

Завдяки дуже низьким затримкам передачі даних 5G також дасть можливість для віддаленого проведення операцій за допомогою робота. Такий сервіс особливо актуальний для невеликих населених пунктів, де немає хірургів на місцях: керуючи маніпуляціями робота, операцію може провести фахівець, який перебуває в абсолютно іншому місці. За рахунок 5G такий сервіс можна буде розгорнути в бездротових мережах.

Практичні переваги 5G

Платформа мережі 5G надає для операторів значні переваги, що виражаються перш за все, в розширенні функціональних можливостей, збільшенні пропускної здатності мережі (performance) та підвищенні рівня задоволеності користувачів (User Experience). На малюнку нижче показані основні параметри мережі IMT2020 (5G), в порівнянні з показниками IMT-Advanced (4G), які дозволяють цього досягти.[3]

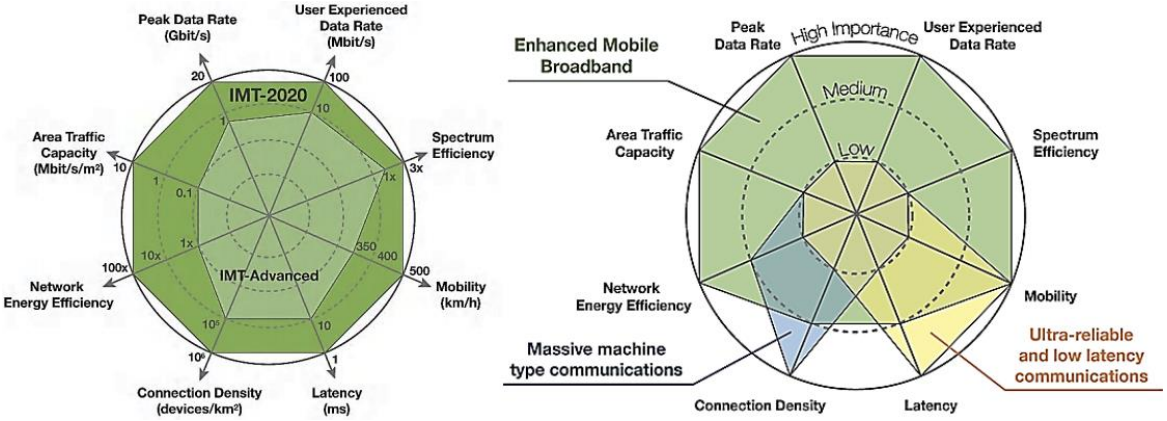

Рисунок 3 – Практичні переваги 5G

Рекомендація 3GPP TR 38.913 визначає наступні ключові показники мереж 5G:

Пікова швидкість: на лінії вгору (Uplink) 10 Гбіт / с (спектральна ефективність 15 біт / с / Гц); на лінії вниз (Downlink) 20 Гбіт / с (спектральна ефективність 30 біт / с / Гц);

***Швидкість*:** може досягати 100 Мбіт / с і більше на одного користувача.

Ефективність використання спектру: кількість інформації, яку можна передати на одиницю частотного діапазону, в мережі 5G буде принаймні в 3 рази вище, ніж в 4G.

Мобільність користувача: швидкість, з якою може переміщатися користувач з терміналом 5G по площі покриття мережі без втрати хендоверу між базовими станціями, в мережі 5G досягає 500 км / год, що дає можливість користуватися послугами 5G в швидкісних поїздах.

Затримка в мережі 5G: знижується до 1 мс і менше, в той час як в мережі 4G можна досягти мінімум 10-мілісекунди затримки.

Щільність терміналів в мережі 5G підвищується і може досягати декількох мільйонів пристроїв на 1 кв. км (наприклад, сенсорів IoT).

Дані показники інколи є несумісними і навіть взаємовиключними. Тому різним пристроям в різні моменти часу будуть доступні тільки певні сервіси з певними показниками (в рамках концепції Network Slicing).

Частоти. Станом на 2019 рік 5G передбачається використовувати в різних спектрах радіочастот. Однак, в діапазоні до 6 ГГц, в тому числі виділеного під Wi-Fi діапазону 5 ГГц, поки існують серйозні проблеми з наявністю вільних частот. Виділення частот для 5G в спектрі до 6 ГГц вже погоджено на Всесвітній конференції радіозв'язку ВКР (WRC-15, World radiocommunication conference) в 2015 році.

Делегати Всесвітньої конференції радіозв'язку 2019 роки (ВКР-19) визначили додаткові смуги радіочастот для Міжнародного рухомого електрозв'язку (IMT), які сприятимуть розвитку мереж мобільного зв'язку п'ятого покоління (5G). [3]. При визначенні смуг частот 24,25-27,5 ГГц, 37-43,5 ГГц, 45,5-47 ГГц 47,2-48,2 і 66-71 ГГц для розгортання мереж 5G, ВКР-19 також вжила заходів для забезпечення належного захисту супутникової служби дослідження Землі (EESS). В цілому делегати конференції визначили 17,25 ГГц спектру для IMT в порівнянні з пропускною спроможністю 1,9 ГГц, доступної до проведення ВКР-19. Спектр в 14,75 ГГц був гармонізований у всьому світі, досягнувши 85% глобальної гармонізації.

Низькі частоти забезпечують гарне проникнення радіохвиль в приміщення, що дуже важливо для IoT. Особливо важливий діапазон 700 МГц, який призначений для систем зв'язку M2M, «розумного міста» і «розумних будинків». *Високочастотний спектр* необхідний мережам 5G для досягнення швидкості передачі даних до 20 Гбіт / с, зокрема, для надання послуг 3D-відео, AR / VR, хмарні сервіси для роботи та ігор та ін.

Технології 5G New Radio (5G NR)

Для того, щоб задовольнити всі зростаючі вимоги до мобільного зв'язку, для 5G були розроблені технології, об'єднані під загальною назвою «нове радіо 5G», 5G New Radio (5G NR).

Основні відмінні риси радіо-технології 5G NR :

Додавання нових діапазонів радіо-спектра, згідно з вимогами до швидкості передачі сигналів, числа пристроїв, зростання трафіку численних додатків 5G.

Оптимізована технологія OFDM (Orthogonal frequency-division multiplexing - мультиплексування з ортогональним частотним поділом каналів). Ця технологія вже була успішно застосована в 4G / LTE-A, а також в останніх версіях Wi-Fi.

Формування променів (Beamforming). Це технологія здатна реалізувати багато переваг 5G. Вона дає можливість направляти промінь радіохвиль від базової станції на певні пристрої, як рухомі, так і нерухомі, без впливу на інші промені, спрямовані на ті ж пристрої.

Рисунок 4 – Beamforming

MIMO (Multiple Input Multiple Output). MIMO - Метод просторового кодування сигналу, що дозволяє збільшити смугу пропускання каналу, який вже застосовувався в Wi-Fi і 4G, в 5G був значно вдосконалений, зокрема, в розрахованому на багато користувачів режимі MU-MIMO (Multi-User- MIMO) в базових станціях 5G gNnodeB (gNB), антени яких складаються з матриці випромінюючих елементів. Це дає можливість посилювати рівень сигналу для конкретного користувача, в той же час мінімізуючи вплив даного сигналу на інших користувачів.

Технології спільного використання спектру (Spectrum sharing). Дуже часто спектри радіочастот не використовуються ефективно. Для вирішення цього завдання були розроблені технології Spectrum sharing.

Уніфікована міжчастотна взаємодія (Unified design across frequencies). Оскільки в 5G NR додано безліч нових частотних діапазонів, важливо забезпечити інтерфейс взаємодії при переході каналу з однієї частоти на іншу при хендовері між базовими станціями.

Small cells. Ущільнення мережевого покриття веде до того, що число базових станцій має збільшуватися. Тому було запропоновано рішення Small Cells - недорогі, прості в установці та обслуговуванні базові станції невеликої потужності. Їх можна розвішувати на щоглах вуличного освітлення, на стінах будинків та інших об'єктах. Мережа 5G здатна ефективно координувати їх роботу, перерозподіляючи навантаження між антенами (рис. 5).

Рисунок 5 – Рішення small cells (зліва), в порівнянні зі звичайною базовою станцією Macro BTS в мережі попередніх поколінь

Архітектура мережі 5G. Особливістю мережі 5G є те, що традиційне поняття «архітектура мережі», яка заснована на апаратних рішеннях, втрачає актуальність.

Тому 5G частіше називають не мережею, а системою, або «платформою», під якою мається на увазі платформа програмна, а не апаратна. Якщо мережі 1/2/3 / 4G будувалися на базі апаратних рішень (обладнання), то платформа 5G будується на базі програмних рішень, зокрема, програмної конфігурації мереж SDN (Software Defined Network), а також віртуалізації мережевих функцій NFV (Network Function Virtualization).

Функції 5G реалізуються в віртуальних програмних функціях VNF (Virtual Network Function), які працюють в інфраструктурі NFV. У свою чергу, NFV реалізується у фізичній інфраструктурі дата-центрів (data center, DC, центр обробки даних, ЦОД), на базі стандартного комерційного обладнання COTS (Commercial Off The Shelf). Устаткування COTS включає лише три види стандартних, відносно недорогих пристроїв - сервер (обчислювальний пристрій), комутатор (мережевий пристрій) і система зберігання даних (пристрій зберігання).

Таким чином, обладнання традиційних мереж мобільного зв'язку замінюється на програмні модулі, які розташовані в дата-центрах на стандартних серверах і віртуальних машинах VM (virtual machines).

Для реалізації програмних функцій, крім віртуальних машин, також будуть використовуватися програмні контейнери (containers), а також програмна архітектура мікросервісів (microservice).

Розподілена архітектура мережі мобільного доступу D-RAN (Distributed RAN) в мережах 4G поступово еволюціонує до централізованої архітектури C-RAN (Centralized RAN).

В архітектурі 5G функції опорної мережі реалізуються в Central Cloud (Cloud RAN), на віртуальних машинах VM.

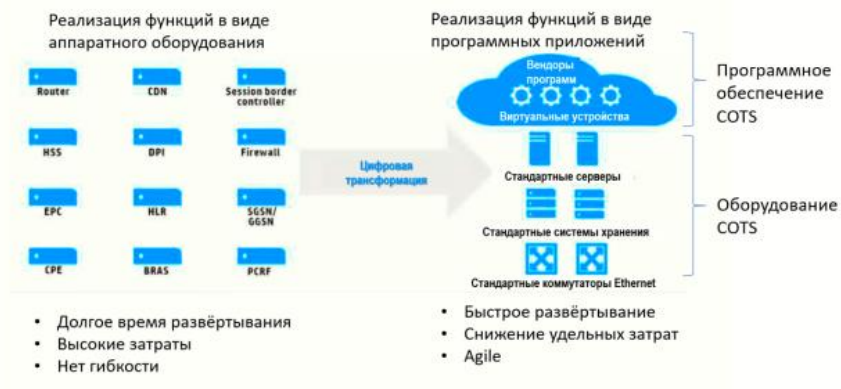

Рисунок 6 – Перехід до віртуальних платформі SDN / NFV в 5G (Джерело: HPE, TAdviser)

Важливу роль у розвитку мереж 5G грає також Edge Cloud, зокрема, технологія MEC (Mobile Edge Cloud), а також Fog Cloud.

Віртуалізація мережі на базі NFV / SDN необхідна також для логічного мережевого шарування (Network Slicing).

Технологія Network Slicing дозволяє на базі єдиного пулу мережевих ресурсів виробляти логічний поділ мереж для різних типів послуг 5G, яким потрібні різні технології радіодоступу RAT (Radio Access Technology), з різними характеристиками середовищ передачі даних. Це, наприклад, послуги:

Високоякісне відео UHD

Голосові послуги (5G Voice)

Інтернет речей з великою кількістю датчиків, сенсорів і виконавчих пристроїв (Massive IoT)

Інтернет речей для відповідальних додатків, таких, наприклад, як безпілотний транспорт (V2X), електронна медицина (Mission Critical IoT)

і багато інших.

Всі ці послуги надаються на базі технології Network Slicing та працюють на єдиній фізичній інфраструктурі дата-центрів центральної та граничної хмари, а також «туманної» інфраструктури (Fog Computing), необхідної для Massive IoT і промислового інтернету речей IIoT (Industrial IoT).

Це дає можливість багаторазового використання створеної колись програмно-апаратної інфраструктури, а також гнучке перепризначення її наявних ресурсів. Крім того, такий підхід дозволяє знизити не тільки значні витрати на будівництво мережі, а й операційні витрати на її обслуговування.

Програмні модулі або мережеві функції мережі 5G

На рис. 2 зображена архітектура мережі 5G з точки зору сервіс-орієнтованої взаємодії різних мережевих функцій на площині управління [6].

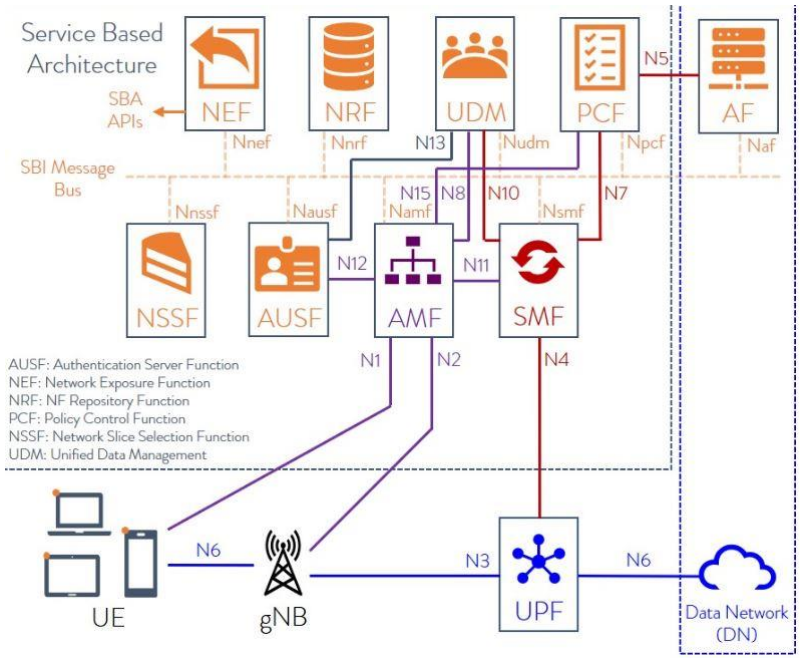

Рисунок 6 – Архітектура мережі 5G. Взаємодія мережевих функцій

Функція управління доступом і мобільністю (AMF - Access and Mobility Management Function)

Функція управління доступом і мобільностю (AMF) забезпечує:

організацію інтерфейсів площини управління N1, N2;

організацію обміном сигналізації NAS через інтерфейс N1, шифрування і захист цілісності сигналізації NAS;

управління реєстрацією обладнання користувача (UE) в мережі і контроль можливих станів реєстрації (RM-DEREGISTERED, RM-REGISTERED);

управління з'єднанням між обладнанням користувача (UE) з мережею та контроль можливих станів з'єднання (CM-IDLE, CM-CONNECTED);

управління доступністю обладнання користувача (UE) в мережі в стані CM-IDLE;

управління мобільністю обладнання користувача (UE) в мережі в стані CM-CONNECTED;

передачу коротких повідомлень між обладнанням користувача (UE) і SMF;

управління службами визначення місця розташування;

передачу повідомлень між UE і функцією управління місцем розташування LMF (Location Management Function), а також між RAN і LMF;

виділення ідентифікатора потоку даних EPS (Evolved Packet System) для взаємодії з EPS;

взаємодія з невизначеними стандартами 3GPP мережами доступу за допомогою модуля взаємодії N3IWF (Non-3GPP InterWorking Function).

Також AMF може включати в себе підфункції управління безпекою, в т.ч. якірну функцію безпеки (SEAF), функцію управління контекстом безпеки (SCMF) і функцію управління політикою безпеки (SPCF).

Незалежно від кількості мережевих функцій, в мережі доступу 5G є тільки один екземпляр інтерфейсу сигналізації NAS між призначеним для користувача обладнанням і мережею, який термінується на одній з мережевих функцій, яка в свою чергу реалізує захист сигналізації NAS і управління мобільністю.

Функція управління сесіями (SMF - Session Management Function)

Функція управління сесіями зв'язку (SMF) забезпечує: управління сесіями зв'язку (створення, зміна та звільнення сесії, включаючи підтримку тунелю між мережею доступу (AN) і UPF);

розподіл та управління IP-адресами терміналів користувачів (UE);

вибір використовуваного шлюзу UPF;

організація взаємодії з функцією управління політиками (PCF);

управління роботою шлюзу UPF, в тому числі управління застосуванням політик QoS;

динамічне налаштування терміналів користувача за допомогою протоколів DHCPv4 (сервер і клієнт) і DHCPv6 (сервер і клієнт);

проксінг ARP (Address Resolution Protocol) запитів;

контроль та збір тарифікаційних даних та організація інтерфейсу з системою білінгу;

безперервність надання послуг SSC (Session and Service Continuity);

взаємодія з гостьовими мережами в рамках процедур роумінгу.

Функція передачі даних користувачів (UPF - User Plane Function)

Функція передачі даних користувачів (UPF) забезпечує:

інтерфейс підключення до зовнішніх мереж передачі даних та до глобальної мережі Інтернет;

маршрутизацію та передачу пакетів даних користувачів;

буферизацію пакетів та ініціацію повідомлення терміналів користувачів (UE) про наявність даних для передачі по лінії вниз (DL);

маркування пакетів даних відповідно з необхідними параметрами QoS;

діагностику пакетів інформації (наприклад, виявлення додатків на основі шаблону потоку даних) і застосування мережевих політик відповідно до вказівки, сформованої PCRF;

надання звітів про використання трафіку;

проксінг ARP (Address Resolution Protocol) запитів.

Також UPF є точкою для підтримки мобільності як всередині однієї, так і між різними технологіями радіодоступу (якщо є).

Модуль управління даними користувачів (UDM - Unified Data Management)

Модуль управління даними користувачів (UDM) забезпечує:

управління даними профілів користувачів, включаючи зберігання та модифікацію переліку доступних користувачам послуг і відповідних їм параметрів;

управління ідентифікаторами користувачів (SUPI);

генерацію облікових даних аутентифікації 3GPP AKA;

авторизацію доступу на основі даних профілю користувача (наприклад, обмеження роумінгу);

управління реєстрацією користувача (тобто, зберігання обслуговуючого AMF);

підтримку безперервності обслуговування / сеансу зв'язку, тобто зберігання призначених SMF / DNN для поточних сеансів зв'язку;

управління доставкою SMS повідомлень.

При цьому кілька різних UDM можуть обслуговувати одного і того ж користувача для різних транзакцій.

Уніфікована база даних (UDR - Unified Data Repository)

UDR здійснює зберігання різних абонентських даних і має прикладні інтерфейси Nudr з елементами доступу UDM FE, PCF FE, NEF FE.

Система зберігання неструктурованих даних (UDSF - Unstructured Data Storage Function)

Концепція побудови мережі 5G передбачає поділ мережевих функцій NF (Network Function) та систем зберігання даних, які обробляють ці функції (Storage). При цьому визначені системи зберігання і обробки як структурованих, так і неструктурованих даних (UDSF - Unstructured Data Storage Function), тобто даних, які або не мають чітко визначеної структури, або даних, структура яких невідома. Мережеві функції NF взаємодіють з системами зберігання даних USDF - через інтерфейс N18.

Одним з способів застосування UDSF є збереження модулями управління доступом і мобільністю (AMF) поточних контекстів зареєстрованого обладнання користувача (UE). Дана інформація може бути використана для забезпечення безобривності абонентських сесій як при

плановому виведенні з сервісу одного з AMF групи моделей (AMF Set), так і при виникненні аварійної ситуації. В обох випадках резервний AMF буде працювати, використовуючи контексти, збережені попередником в UDSF.

Найбільш типовою реалізацією є поєднання на одній фізичній платформі системи зберігання неструктурованих даних (UDSF) та уніфікованої бази даних (UDR).

Типова структура організації UDR / UDSF зображена на рис. 7.

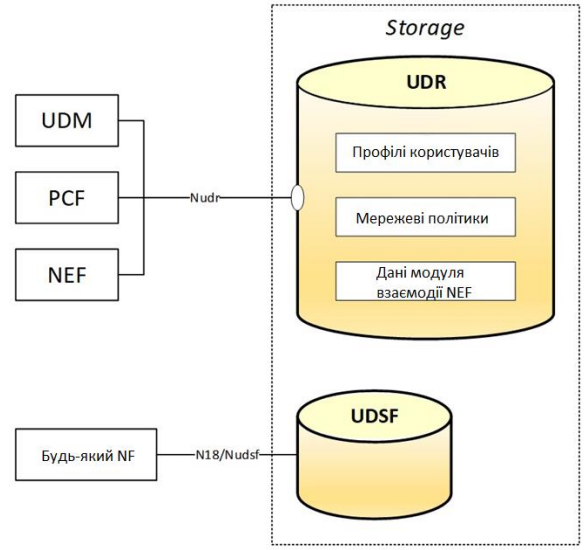

Рисунок 7 – Типова структура організації UDR / UDSF

Функція вибору мережевого шару (NSSF - Network Slice Selection Function)

Функція вибору мережевого шару (NSSF) забезпечує:

вибір необхідного набору мережевих шарів (Network Slices) в процесі реєстрації UE в мережі (в залежності від типу послуги, типу обладнання, його місця розташування і т.д.);

визначення модулів AMF, які будуть використовуватися для подальшого обслуговування UE або, на основі конфігурації, визначення переліку модулів AMF, шляхом запиту в NRF;

зберігання інформації про доступні мережеві шари (NSSAI - Network Slice Selection Assistance Information).

Функція управління політиками (PCF - Policy Control Function)

Функція управління політиками (PCF) в реальному часі формує та призначає обладнанню користувача певні політики, включаючи параметри якості обслуговування (QoS) та правила тарифікації. Так, для передачі того чи іншого типу трафіку можуть динамічно створюватися віртуальні канали з різними характеристиками. При цьому до уваги можуть прийматися вимоги сервісу, профіль, місцерозташування, рівень завантаження мережі, обсяг спожитого трафіку і т.д. PCF звертається до UDR, що знаходиться в тій же PLMN, що і PCF.

Функція забезпечення взаємодії з зовнішніми додатками (NEF - Network Exposure Function)

Для взаємодії з опорною мережею 5G NEF дозволяє платформам і додаткам підписуватися на певні події, які генеруються різними елементами мережі, і надалі отримувати повідомлення про виникнення таких подій (див. рис. 5). наприклад:

- Loss of connectivity - детектування мережею втрати пов'язаності з конкретним UE (детектується AMF);
- UE reachability - відновлення пов'язаності з конкретним UE (детектується AMF);
- Location Reporting - звіти про місцезнаходження (детектується AMF);
- Change SUPI-PE association - зміна терміналу абонентом мережі = зміна зв'язку IMSI - IMEI (детектується UDM).

Дозволяє здійснювати провіжінінг інформації по конкретним UE в мережі 5G.

Дозволяє управляти параметрами QoS і правилами тарифікації (PCC) з конкретних UE.

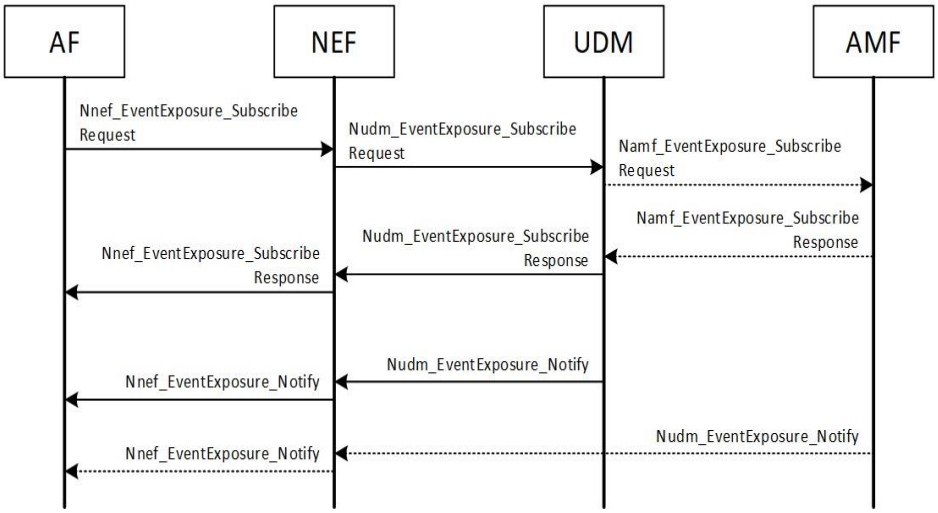

Рисунок 8 – Повідомлення про виникнення подій, створеними різними елементами мережі

NEF може підтримувати підмножину прикладних програмних інтерфейсів API. Це необхідно для взаємодії з різними елементами, платформами та додатками (або мережевими функціями NFs). Безпека взаємодії забезпечується за допомогою реалізованих NEF механізмів безпеки (включаючи аутентифікацію та авторизацію відповідних платформ і додатків). Таким чином, функція забезпечення взаємодії з зовнішніми додатками є логічним продовженням елемента SCEF архітектури вузькосмугового інтернету речей (NB-IoT), анонсованого в релізі 13 3GPP.

NEF може зберігати інформацію, отриману від NFs, у вигляді структурованих даних в UDR, використовуючи стандартний інтерфейс Nudr, і в подальшому використати її її для трансляції іншим NFs, або з метою аналізу.

Сховище мережевих функцій (NRF - NF Repository Function)

Сховище мережевих функцій (NRF) є еволюційним розвитком сервера доменних імен DNS. NRF забезпечує зберігання профілів всіх розгорнутих на мережі екземплярів мережевих функцій та вибір одного або декількох екземплярів в рамках процедури "NF Discovery Request" процесу управління абонентськими сесіями. При цьому кожна послуга мережі дозволяє при включенні повинна "прописати" в NRF свій статус, а також свої функціональні можливості і підтримувані опції.

Профіль екземпляра NF, який підтримується в NRF, включає наступну інформацію:

ідентифікатор екземпляра яких мережевих функцій;

тип мережевих функцій;

ідентифікатор PLMN;

ідентифікатор (и), що пов'язані з мережевим шаром, наприклад, S-NSSAI, NSI ID;

FQDN або IP-адресу мережевої функції;

інформація про ємності мережевих функцій;

інформація про дозволені сервіси;

імена підтримуваних сервісів;

інформація про точки обміну інформацією для кожної підтримуваної служби;

ідентифікація збережених даних / інформації;

інші параметри сервісів, наприклад, DNN (Data Network Name), параметри інтерфейсів для повідомлень;

рівень PLMN (NRF налаштований для роботи на всій PLMN);

рівень мережевих шарів спільного використання (NRF налаштований таким чином, що він належить кільком мережевим шарам);

рівень мережевих шарів певного використання (NRF налаштований з приналежністю до S-NSSAI);

При організації роумінгу кілька NRF можуть бути розгорнуті в різних мережах:

NRF (и) в гостьовій PLMN (відомі як vNRF), сконфігуровані для роботи в гостьовій PLMN;

NRF (и) в домашній PLMN (відомі як hNRF), сконфігуровані для роботи в гостьовій PLMN, з яким взаємодіє vNRF через інтерфейс N27.

Прикладна функція (AF - Application Function)

Прикладна функція (AF) мережі 5G взаємодіє з опорною мережею і, як приклад, може вирішувати такі завдання:

управління маршрутизацією трафіку;

надання доступу до модуля забезпечення взаємодії з елементами мережі (NEF);

взаємодія з функцією управління політиками.

Залежно від конкретного впровадження на мережі оператора зв'язку, окремим зовнішнім платформам та додаткам може бути дозволений прямий доступ до мережевих функцій 5G. Інші системи будуть здійснювати доступ до мережевих функцій 5GC через прикладні програмні інтерфейси API, що надаються модулем забезпечення взаємодії мережевих функцій.

CUPS (control and user plane separation)

Згідно з архітектурою SDN для мереж 5G визначено поділ шлюзу пакетної передачі даних на дві складові - площину управління (SMF) і площину призначеного для користувача трафіку (UPF) - control and user planes separation (CUPS). Концепція CUPS 14 3GPP визначена і для мереж 4G-LTE, де передбачено поділ SGW на C-SGW (control plane) і U-SGW (user plane), а PGW відповідно - на C-PGW і U-PGW.

Спрощення архітектури UPF в порівнянні з PGW мережі 4G-LTE дозволяє зменшити вартість розробки і виробництва самих вузлів та витрати на їх експлуатацію. В результаті, це відкриває шлях до "примежових обчислень" (edge computing) за рахунок можливості встановлення на мережі великої кількості шлюзів, розміщуючи їх в безпосередній близькості до мережі доступу. Але такий підхід створює проблему мобільності, оскільки переміщення обладнання користувача з активною сесією передачі даних буде супроводжуватися частою зміною UPF. 3GPP вирішує дану проблему шляхом введення нової функціональності - безшовних абонентських сесій і послуг - SSC (Session and Service Continuity).

Network Slicing

Network slicing надає змогу забезпечити ефективність використання мережевих ресурсів, гнучкість розгортання та підтримку швидкого зростання у верхніх (over the top (OTT)) додатках та сервісах. 3GPP розглядає Network slicing як одну з ключових особливостей 5G.

Network Slicing передбачає поділ фізичної архітектури 5G на безліч віртуальних мереж або шарів. Кожен мережевий шар(слайс) включає в себе функції рівня управління, функції рівня трафіку користувача та мережу радіодоступу (5G-NR, або non-3GPP). Базуючись на архітектурі NFV / SDN, кожен шар має свої характеристики і призначений для вирішення того чи іншого бізнес-завдання. 3GPP визначає три стандартні мережеві шари:

над-широкосмуговий доступ (eMBB, Enhanced Mobile Broadband) - користувачі глобальної мережі Інтернет, камери відеоспостереження,

ультра-надійність і низькі затримки (URLLC, Ultra Reliable Low Latency Communication) - транспорт без водія, доповнена і віртуальна реальність;

інтернет речей (IoT, Internet of Things) - мільйони пристроїв, що передають малі обсяги даних від випадку до випадку.

Кожен оператор може визначати додаткові мережеві шари, наприклад, виділений мережевий шар для критичних комунікацій, для внутрішньокорпоративного зв'язку і т.д.

Обладнання користувача (UE) може обслуговуватися одночасно одним або декількома мережевими шарами (максимум - 8). При цьому модуль AMF є загальним для всіх шарів, а от інші елементи (в т.ч. SMF, UPF) можуть відрізнятися. Також різні шари можуть включати в

себе різні мережі радіодоступу, або єдину мережу, але з відмінними характеристиками. Також мережеві шари можуть мати різні параметри безпеки.

При реєстрації в мережі в рамках процедури встановлення RRC з'єднання (і далі - в повідомленні NAS) термінал (UE) передає список запитуваних мережевих шарів (S-NSSAI - Single Network Slice Selection Assistance Information). На першому кроці, на підставі отриманих від UE даних, списку мережевих шарів, що містяться в UDM профілі користувача і розташування абонента здійснюється вибір елемента AMF, який може забезпечити необхідний набір послуг. Вибір AMF здійснюється із залученням модуля вибору мережевого шару (NSSF) і сховища мережевих функцій (NRF).

Network Function layer

Мережевий функціональний рівень відповідає за створення кожного мережевого фрагмента відповідно до запитів екземпляра служби, що надходять із верхнього рівня. Він складається з набору мережевих функцій, які втілюють чітко визначені поведінки та інтерфейси. Кілька мережевих функцій розміщуються над інфраструктурою віртуальної мережі та з'єднуються між собою для створення екземпляру відрізка мережі до кінця, який відображає характеристики мережі, запитувані службою [9]. Конфігурація мережевих функцій виконується за допомогою набору мережевих операцій, що дозволяють керувати їхнім повним життєвим циклом (від їх розміщення, коли створений слайс, до їх розмежування, коли надана функція більше не потрібна) [6].

Для підвищення ефективності використання ресурсів однакові мережеві функції можуть одночасно ділитися різними фрагментами за рахунок збільшення складності управління операціями. І навпаки, відображення одного на одного між кожною функцією мережі та кожним фрагментом полегшує процедури конфігурації, але може призвести до поганого та неефективного використання ресурсів [7].

Висновки. Було розглянуто необхідність впровадження мережі п’ятого покоління та її архітектуру. Так як в сучасному світі неможливо обійтись без розумних технологій, мережі 5G дозволяють проводити аналіз великих даних (Big Data), користуватись інтернетом речей (IoT) та покликані стати однією з основ цифрової економіки, головною особливістю якої повинен стати штучний інтелект.

Платформа мережі 5G надає операторам значні переваги, що виражаються перш за все, в розширенні функціональних можливостей, збільшенні пропускної здатності мережі (performance) та підвищенні рівня задоволеності користувачів (User Experience).

5G дозволяє домогтися наступного:

У 20 разів збільшити пропускну здатність каналів зв'язку. Це дозволить обмінюватися великими обсягами даних в лічені секунди. Пікова швидкість в мережах 4G досягає всього лише 1 Гбіт / с, а для 5G - 20 Гбіт / с.

Мінімізувати перешкоди. 5G дозволяє використовувати нові діапазони частот, які зараз майже вільні. Мінімальні перешкоди забезпечать безперебійну роботу каналів зв'язку.

Network slicing. Мобільні оператори зможуть розгортати ізольовані один від одного мережі, які можна використовувати для різних завдань. Наприклад, забезпечення зв'язком користувачів, робота з Інтернетом речей (IoT), передача «важкого» мультимедійного контенту і т. д.

Створити єдину IoT-систему з мільйонами підключених пристроїв.

Зменшити затримки з приблизно 10 мс в разі 4G до 1 мс для 5G. Це критично важливий момент для багатьох сфер, включаючи бізнес, технології, науку.

Особливість архітектури мережі 5G полягає в тому, що традиційне поняття «архітектура мережі», яка заснована на апаратних рішеннях, в 5G втрачає актуальність. Тому 5G частіше називають не мережею, а системою, або «платформою», під якою мається на увазі платформа програмна, а не апаратна. Якщо мережі 1/2/3 / 4G будувалися на базі апаратних рішень (обладнання), то платформа 5G будується на базі програмних рішень, зокрема, програмної

конфігурації мереж SDN (Software Defined Network), а також віртуалізації мережевих функцій NFV (Network Function Virtualization).

В архітектурі 5G взаємодія обладнання користувача (UE) з мережами передачі даних (Data Network) здійснюється в рамках PDU сесій (PDU Session-s). UE може мати одночасно кілька створених PDU сесій для зв'язку з різними мережами передачі даних та отримання різних сервісів.

Функції 5G реалізуються в віртуальних програмних функціях VNF (Virtual Network Function), які працюють в інфраструктурі NFV. У свою чергу, NFV реалізується у фізичній інфраструктурі дата-центрів (data center, DC, центр обробки даних, ЦОД), на базі стандартного комерційного обладнання COTS. Таким чином, обладнання традиційних мереж мобільного зв'язку замінюється на програмні модулі, які працюють в дата-центрах на стандартних серверах і віртуальних машинах VM (virtual machines).

ЛІТЕРАТУРА:

1. П’яте покоління мобільного зв’язку:URL: http://www.tadviser.ru/index.php/

2. Geneva Mission Briefing Series, 5G Related Aspects in ITU-R Working Party 5D, Emerging Trends in 5G/IMT2020

3. Частоти для 5G і сроки для супутниковых систем: URL; https://www.rspectr.com/articles/574/chastoty-dlya-5g-i-sroki-dlya-sputnikovyh-sistem

4. 5G: URL; https://www.metaswitch.com/knowledge-center/reference/what-is-the-5g-service-based-architecture

5. SDN: URL; https://sdn.ieee.org/newsletter/december-2017/network-slicing-and-3gpp-service-and-systems-aspects-sa-standard

6. Yousaf, F. Z.; Bredel, M.; Schaller, S.; Schneider, F. (2017). "NFV and SDN-Key Technology Enablers for 5G Networks". *IEEE Journal on Selected Areas in Communications*. 35 (11): 2468–2478. arXiv:1806.07316.

7. Ordonez-Lucena, J.; Ameigeiras, P.; Lopez, D.; Ramos-Munoz, J. J.; Lorca, J.; Folgueira, J. (2017). "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges". *IEEE Communications Magazine*. 55 (5): 80–87. arXiv:1703.04676. Bibcode:2017arXiv170304676O. doi:10.1109/MCOM.2017.1600935. hdl:10481/45368. ISSN 0163-6804.

8. Yousaf, F. Z.; Bredel, M.; Schaller, S.; Schneider, F. (2017). "NFV and SDN-Key Technology Enablers for 5G Networks". *IEEE Journal on Selected Areas in Communications*. 35 (11): 2468–2478. arXiv:1806.07316

9. РС Одарченко, ЮВ Беженар, АО Ксендзенко, Аналіз вразливостей систем захисту інформації в мережах Wi-Max та методів їх усунення, захист інформації. *Сбірник наукових трудів.-К.: НАУ*, 2011D

10.R.S. Odarchenko, Dakov S, The method of the project for the SDN version of the Operator class // Science and Technology. - 2017. - No.4 (36)

11.С. Одарченко, С.Ю. Даков, В. В. Полищук, А. М. Тырсенко, Моделирование сетей наложения SDN и их основные характеристики Исследования // *Технологии знаний* № 3 (31), 2016 с. 284

12.Ndiaye, M.; Hancke, G.P.; Abu-Mahfouz, A.M. Software Defined Networking for Improved // *Wireless Sensor Network Managemen,* A Survey. Sensors 2017, 17, 1031.

13.Tomas Hegr, Leos Bohac, Impact of Nodal Centrality Measures to Robustness in, Software-Defined Networking // Advances in Electrical and Electronic Engineering. 2014;12(4):252-259 DOI 10.15598/aeee.v12i4.1208.

REFERENCES:

1. Fifth Generation Mobile: URL: http://www.tadviser.com/index.php/

2. Geneva Mission Briefing Series, 5G Related Aspects in ITU-R Working Party 5D, Emerging Trends in 5G / IMT2020

3. Frequencies for 5G and terms for satellite systems: URL; https://www.rspectr.com/articles/574/chastoty-dlya-5g-i-sroki-dlya-sputnikovyh-sistem

4. 5G: URL; https://www.metaswitch.com/knowledge-center/reference/what-is-the-5g-service-based-architecture

5. SDN: URL; https://sdn.ieee.org/newsletter/december-2017/network-slicing-and-3gpp-service-and-systems-aspects-sa-standard

6. Yousaf, F.Z .; Bradel, M.; Schaller, S.; Schneider, F. (2017). "NFV and SDN – Key Technology Enablers for 5G Networks.*" IEEE Journal on Selected Areas in Communications*. 35 (11): 2468–2478. arXiv: 1806.07316.

7. Ordonez-Lucena, J.; Ameigeiras, P.; Lopez, D.; Ramos-Munoz, J. J.; Lorca, J.; Folgueira, J. (2017). "Network Slicing for 5G with SDN / NFV: Concepts, Architectures, and Challenges". IEEE Communications Magazine. 55 (5): 80–87. arXiv: 1703.04676. Bibcode: 2017arXiv170304676O. doi: 10.1109 / MCOM.2017.1600935. hdl: 10481/45368. ISSN 0163-6804.

8. Yousaf, F. Z .; Bradel, M.; Schaller, S.; Schneider, F. (2017). "NFV and SDN — Key Technology Enablers for 5G Networks." *IEEE Journal on Selected Areas in Communications*. 35 (11): 2468–2478. arXiv: 1806.07316

9. RS Odarchenko, Yu. Bezhenar, JSC Xendzenko, Analysis of vulnerabilities of information security systems in Wi-Max networks and methods of their elimination, protection of information. *Collection of scientific works.*-K .: NAU, 2011D

10. R.S. Odarchenko, Dakov S, The method of project design for the SDN version of the Operator class // *Science and Technology.* - 2017.- No.4 (35)

11. S. Odarchenko, S.Yu. Dakov, V.V. Polishchuk, A.M.Tirsenko, Modeling of SDN Overlay Networks and Their Basic Characteristics of the Study *// Knowledge Technologies* № 3 (31), 2016 p. 284

11. Ndiaye, M .; Hancke, G.P .; Abu-Mahfouz, A.M. Software Defined Networking for Improved // Wireless Sensor Network Managemen, *A Survey. Sensors* 2017, 17, 1031.

13. Tomas Hegr, Leos Bohac, Impact of Nodal Centrality Measures to Robustness in Software-Defined Networking *// Advances in Electrical and Electronic Engineering.* 2014; 12 (4): 252-259 doi 10.15598 / aeee.v12i4.1208

д.т.н., проф. Оксиюк О.Г., д.т.н., доц. Одарченко Р.С.,
к.т.н. Даков С.Ю., Бурмак Ю.А., Федюра Т.В.

СТАНДАРТИ ТА ТЕХНОЛОГІЙ МЕРЕЖІ 5G І МОЖЛИВІСТЬ ЇЇ РЕАЛІЗАЦІЇ

В работе были исследованы архитектуру сети 5G и предложен вариант системы мониторинга параметров на базе SCOM. Данную систему можно использовать для сбора и анализа информации о производительности сети, выявление отклонений, оповещение о них для своевременного устранения. Были представлены технологии для использования мобильной сети стандарта 3 GPP пятого поколения. Были проанализированы и предлагаемые к внедрению. Также были исследованы современные возможности сети 5го поколения и технологии для их внедрения. В работе проанализированы и даны рекомендации к внедрению следующих серверов. 5G сети позволяют значительно повысить скорость передачи данных через различные технологии радиодоступа (RAT), и с помощью использования новых спектров радиочастот 5G NR (New Radio). Для решения «Умный дом» (Smart Home) и «Умная здание» (Smart Building) доступен целый спектр различных сервисов интернета вещей (IoT): видеонаблюдение, управление и автоматизация бытовой техники, управления системами безопасности и тому подобное. Сервис виртуальной реальности VR (Virtual Reality) создает иллюзию перемещения человека в другой мир, воздействуя на органы чувств, прежде всего на зрение (VR-очки). Сервис дополненной реальности AR (Augmented Reality) комбинирует реальное окружение с виртуальными предметами. Эти сервисы предназначены не только для развлечений, но и для науки. Сеть 5G, вместе с технологией интернета вещей IoT, с помощью промышленных датчиков IIoT (Industrial Internet of things), а также с помощью искусственного интеллекта ИИ (AI, Artificial Intelligence) способны существенно повысить степень автоматизации производства. При этом появляется возможность в режиме реального времени анализировать большие объемы разнообразных данных (Big Data) как на основе полученных выводов (insights), так и с использованием машинного и глубокого обучения (Machine learning, Deep learning). К этим программам могут относиться, например, электронная медицина (e-Health), связь при чрезвычайных ситуациях (Mission Critical Communication), тактильный интернет (Tactile Internet) и другие. Беспилотный транспорт может использоваться как часть услуги «Умный город», однако, может существовать и отдельно. Также на платформе 5G возможна реализация систем помощи водителю ADAS (Advanced Driver-Assistance Systems).

Ключевые слова: мобильная сеть, программное обеспечение, среда программирования, макро и микро уровень, стандарты мобильных сетей, сетевая архитектура, гипервизор, мониторинг, автоматизация процессов.

Doctor of Technical Sciences Oksiuk O.G., Ph.D., Doctor of Technical Sciences Odarchenko R.S., Ph.D. Dakov S.Yu., Burmak Yu.A., Fedyura T.V.

5G NETWORK STANDARDS AND TECHNOLOGIES AND THE POSSIBILITIES OF ITS IMPLEMENTATION

The paper investigates the architecture of the 5G network and proposed a variant of the SCOM based parameter monitoring system. You can use this system to collect and analyze network performance information, detect deviations, and notify them for timely removal. Technologies were introduced for the use of the fifth generation GPP mobile network of the fifth generation. Analyzed and proposed for implementation. The current capabilities of the 5th generation network and the technologies for their implementation were also explored. This paper analyzes and provides recommendations for the implementation of the following servers. 5G networks make it possible to significantly increase data rates through various radio access technologies (RATs), and through the use of new 5G NR (New Radio) radio spectrum. Smart Home and Smart Building are available in a variety of different Internet of Things (IoT) services: video surveillance, home automation and control, security management, and more. Virtual Reality (VR) service creates the illusion of moving a person to another world, affecting the sense organs, especially the sight (VR-glasses). Augmented Reality (Augmented Reality) Augmented Reality service combines a real environment with virtual objects. These services are intended not only for entertainment but also for science. The 5G network, along with IoT Internet of Things technology, with the help of Industrial IIoT (Industrial Internet of Things) sensors, as well as AI (Artificial Intelligence), can significantly increase the degree of automation of production. This gives the opportunity in real time to analyze large amounts of diverse data (Big Data), both on the basis of insights, and using machine and deep learning (Machine learning, Deep learning). These may include, for example, e-Health, Mission Critical Communication, Tactile Internet, and others. Unmanned transport may be used as part of the Smart City service, but may exist separately. Also on the 5G platform it is possible to implement ADAS (Advanced Driver-Assistance Systems) driver assistance systems.

Keywords: mobile network, software, programming environment, macro and micro level, standards of mobile networks, network architecture, hypervisor, monitoring, process automation.

ЗАГАЛЬНІ ПИТАННЯ

УДК 37.013.46

д.пед.н., доц. **Артемов В.Ю.** (Університет "КРОК")
к.т.н., с.н.с. **Литвиненко Н.І.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-12

ПРОФЕСІЙНИЙ РИЗИК ЯК СПОСІБ СОЦІАЛЬНОЇ ПОВЕДІНКИ В УМОВАХ НЕВИЗНАЧЕНОСТІ

У статті визначено місце і роль професійного ризику як способу соціальної поведінки в умовах невизначеності. Показано, що Міжнародна організація праці, Всесвітня організація здоров'я (International Standard Organization) опікується питаннями регулювання або управління професійними ризиками.

Професійний ризик являє собою складне явище, щодо визначення якого немає єдності в словниках, енциклопедіях, нормативно-правових документах та наукових публікаціях.

Визначається, що людина в процесі професійної, часто монотонної діяльності, звикає до ризику, не помічає й не оцінює професійний ризик. Доведено, що класи професійного ризику виробництва визначаються залежно від рівня виробничого травматизму і професійних захворювань за видами економічної діяльності, що визначає ступінь вірогідності втрати професійної працездатності або смерті працівника під час виконання трудових обов'язків з урахуванням результатів аналізу статистики надзвичайних подій.

Висувається припущення, що професійний ризик як психологічний феномен завжди пов'язаний із прийняттям рішення. Робиться акцент на тому, що поняття «професійний ризик» має переважно об'єктивний і перманентний характер, а службовий – суб'єктивний і ситуативний. Важливим є також те, що професійний, так само, як і службовий ризик, слід розглядати як спрямований на суб'єкт, і, окремо, на об'єкт ризикованої діяльності.

Таким чином, розглядаючи професійний ризик як спосіб соціальної поведінки в умовах невизначеності, можна зробити висновок, що в складі професійного ризику, слід виділити підклас службового ризику, який здійснюється в умовах підвищеної відповідальності, й несе інше, більш інтенсивне психологічне навантаження.

Ключові слова: ризик, професійний ризик, вимушений ризик, службовий ризик, поведінка.

Вступ та постановка задачі. Сьогодні словосполучення «професіональній ризик» почало постійно з'являтися у міжнародних наукових публікаціях, нормативних документах та стандартах. Це пояснюється тим, що людство в наш час, за словами Нікласа Лумана [1], від *індустріального суспільства* переходить у суспільство *ризику*. Перебуваючи в індустріальному суспільстві, ми створили та продовжуємо створювати для себе самих численні нові техногенні ризики. При цьому масштаби природних та соціальних ризиків ані трохи не зменшилися, а стали лише більшими. Актуальність нашого дослідження полягає в тому, що на сьогодні ми більш глибоко та грунтовно почали досліджувати ризик, відповідальніше ставитися до його наслідків та безпеки загалом, більш ретельно та наполегливо відшукувати шляхи ідентифікації та регулювання ризику.

Мета статті полягає у виявлення, дослідженні місця та ролі професійного ризику як способу соціальної поведінки в умовах невизначеності.

Аналіз останніх досліджень і публікацій. Незважаючи на значну кількість праць вітчизняних та іноземних вчених, присвячених питанням визначення місця та ролі ризику в суспільстві, [1 - 16] (насамперед, Н. Луман [1], Томанек Д. [12], Е. Ільїн [13], Л. Карпенко, А. Петровський [14], А. Сухарев [15], В. Войтко [16] та ін.) проблемі дослідження

професійного ризику як способу соціальної поведінки в умовах невизначеності, досліджені ще недостатньо.

Виклад основного матеріалу дослідження. Потужні міжнародні організації МОП (Міжнародна організація праці), ВОЗ (Всесвітня організація здоров'я) та ІСО (International Standard Organization) виявляють значний інтерес до проблем професійного ризику. МОП та ВОЗ опікуються питаннями ідентифікації ризиків, що виникають в процесі професійної діяльності, а також проблемами компенсації їх наслідків шляхом механізмів страхування, а ІСО опікується проблемами стандартизації заходів підвищення безпеки в процесах виробництва і споживання товарів та послуг шляхом регулювання або управління професійними ризиками.

В результаті їх спільної діяльності була вироблена серія директив, рекомендацій та стандартів. Основними, пов'язаними з поняттям «професійний ризик», є стандарт управління навколишнім середовищем ISO 14001 (Environmental Management Systems Standards) [2], стандарт якості ISO 9001 (Quality Systems: Model For Quality Assuranceindesign, Development, Production, Installationandservicing), система управління професійним здоров'ям і безпекою праці OHSAS 18001 [3] (Occupational Heal Thand Safety Assessmentseries).

Україна, вступивши в систему МОП, ВОЗ та ISO, реалізує програму затвердження міжнародних стандартів та рекомендацій. Прикладами можуть служити ДСТУ OHSAS 18001:2 010 «Система управління гігієною та безпекою праці», ДСТУ 2293-99 «Охорона праці», ДСТУ 2156-93 «Безпечність промислових підприємств», Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», Закон України «Про загальнообов’язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності» [4] тощо.

Професійний ризик являє собою складне явище, щодо визначення якого немає єдності в словниках, енциклопедіях, нормативно-правових документах та наукових публікаціях.

За словниковим визначенням, професійний ризик – це ризик, що виникає під час роботи за певним фахом на певному робочому місці. Професійний ризик виробництва – це ризик травмування людини, що виникає на певному виробництві [5].

Відповідно до Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», професійний ризик – це ймовірність виникнення негативних наслідків від провадження господарської діяльності та можливий розмір втрат від них, що вимірюється в кількісних та якісних показниках [6].

Професійний ризик *(risk)* відповідно до міжнародного стандарту ISO 14001:2004, 3.20 – це поєднання ймовірності виникнення небезпечної події чи впливу та істотності травми або погіршання здоров’я, які може бути зумовлено такою подією чи впливом [7].

Тобто, найчастіше поняття «професійний ризик» використовується для позначення ймовірності пошкодження (втрати) здоров'я або смерті в результаті несприятливого впливу факторів виробничого середовища й трудового процесу, пов'язаного з виконанням професійних обов'язків.

Термінологія професійного ризику трактується в англомовному середовищі досить цікаво. Так, професійний ризик *(professional/occupational risk)* – це оцінка ризиків для здоров'я від впливу різних рівнів небезпеки на робочому місці [8], або професійний ризик як *professional/occupational hazard*, тобто будь-який стан роботи, який може призвести до хвороби або травми. Тим самим начебто зрівнюються поняття ризику *(risk)* й загрози *(hazard)*. Більш того, поняття «загроза» в даному випадку, так би мовити, витісняє зі сфери дослідження поняття «ризик», натомість заміщує його. З позицій психології - це некоректно або, навіть, неприпустимо, адже ризик – це завжди суб'єктивне явище, яке виникає/існує в індивідуальній свідомості. Натомість, загроза – це явище найчастіше цілком об'єктивне, існуюче незалежно від нашої свідомості. Проте для вирішення завдань, які виникають у сфері охорони праці, страхування, таке зміщення понять вважається цілком припустимим [9].

Термінологічною особливістю є застосуванням в англомовному середовищі термінів «*professional*» та «*occupational*» в контексті ризику. *Professional* – це те, що пов'язане із отриманим фахом, спеціальністю, навчанням. *Occupational* – це те, що пов'язане із місцем, яке посідає особа но роботі. «Professional» характеризує скоріше особистість, тоді як «*occupational*» – посаду й фах. Ця тонка відмінність може відігравати важливу роль в ході укладання робочих контрактів наших співвітчизників за кордоном.

Професійний ризик в рекомендаціях МОП та в стандартах ISO розглядається як певна вимірювана в контексті теорії ймовірності величина. Такий підхід пояснюється прагненням створити умови для матеріальної компенсації фізичної чи іншої шкоди, отриманої суб'єктами в результаті їх професійної діяльності.

Очевидно, що професійний ризик, який береться до уваги в документах ВОЗ, МОП та ISO має перманентний характер. Саме такий ризик, на думку цих авторитетних організацій, отримує масовий та небезпечний характер. Це пояснюється тим, що людина в процесі професійної, часто монотонної діяльності, звикає до ризику, не помічає й не оцінює його. В результаті виникають професійні захворювання, виробничі травми. Разом з тим, саме такими ризиками відносно легко управляти, їх можна попереджати, страхувати, компенсувати та запобігати їм, використовуючи стандартні, логічно обґрунтовані заходи й засоби.

Це зовсім не виключає того, що професійні ризики можуть приймати ситуативний характер з критичними або катастрофічними наслідками. Такий характер професійний ризик набуває переважно там, де праця пов'язана з екстремальними умовами: робота випробувачів, пожежних, моряків, охоронців, співробітників спецслужб і правоохоронних органів. У таких випадках звичайна логіка часто втрачає сенс: кожен випадок розглядається як унікальний, на перше місце висувається психологія, яка допомагає виявляти причини, мотиви та природу події.

Актуальність вивчення питань професійного ризику з позицій **охорони праці та соціального захисту** пов’язана із становленням сучасних страхових механізмів у цілому світі. Одним з головних принципів створення страхових механізмів захисту від нещасних випадків на виробництві та професійних захворювань в Україні є обов’язкове страхування суб’єктів професійної діяльності відповідно до ст. 47 Закону України «Про загальнообов’язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності» [10]. За кожного застрахованого таким чином працівника роботодавець зобов'язаний сплачувати внески до фонду соціального страхування, диференційовано залежно від класу професійного ризику.

Класи професійного ризику й страхові тарифи – це взаємопов'язані поняття: чим вище професійний ризик, тим більше страхові внески[1] на обов'язкове соціальне страхування від надзвичайних подій на виробництві та професійних захворювань. Клас професійного ризику виробництва визначається залежно від рівня виробничого травматизму і професійних захворювань за видами економічної діяльності, що визначає ступінь вірогідності втрати професійної працездатності або смерті працівника під час виконання трудових обов'язків, з урахуванням результатів аналізу статистики надзвичайних подій, а також обсягів видатків Фонду соціального страхування України, пов'язаних із забезпеченням загальнообов'язкового державного соціального страхування від надзвичайних подій, які спричинили втрату працездатності.

В Україні професійний ризик на виробництві визначається Постановою Фонду соціального страхування «Про затвердження Порядку об'єднання видів економічної діяльності у страхові галузеві сукупності видів економічної діяльності для визначення класу професійного ризику виробництва» від 25.12.2012 № 44 [11], де визначається рівень виробничого травматизму й професійних захворювань за видами економічної діяльності, що визначає ступінь вірогідності втрати професійної працездатності або смерті працівника під час

[1] Страхові внески – це обов'язкові платежі, що розраховуються в залежності від класу ризику за спеціальним тарифом, які всі роботодавці повинні щомісяця перераховувати страховику.

виконання трудових обов'язків, з урахуванням результатів аналізу статистичних показників у цій сфері, а також обсягів видатків зазначеного Фонду на соціальне страхування в України. Класи професійного ризику й ставки єдиного внеску визначаються з урахуванням кодів КВЕД – Класифікатора видів економічної діяльності. В Україні станом на 2019 рік визначено 67 класів професійного ризику. Для прикладу, до 1-го класу професійного ризику відносяться такі види діяльності:

– оборона, охорона громадського порядку та безпеки, юстиція, правосуддя, сфера права;
– державне управління загального характеру, діяльність головних управлінь;
– технічні випробування, дослідження;
– консультування з питань керування та комерційної діяльності;
– регулювання у сферах економічної діяльності, освіти, культури, охорони здоров'я, та інших соціальних сферах, крім обов'язкового соціального страхування;
– інша соціальна допомога без забезпечення проживання;
– організації промисловців і підприємців; професійні громадські організації; професійні спілки; релігійні організації; політичні організації; екстериторіальні організації і органи; інші громадські організації, не віднесені до ін. угруповань.

Звичайно ж класи професійного ризику, види діяльності та ставки єдиного внеску за класами ризику в Україні періодично переглядаються.

Використання класів професійного ризику являє собою окрему проблему. Так, фахівці МОП виділяють більше 150 класів професійних ризиків і приблизно 1 тис. їх видів, які становлять реальну небезпеку для 2 тис. різних професій. При цьому вважається, що дана класифікація є неповною і охоплює тільки окремі аспекти безпеки і гігієни праці [12].

Такий стан проблеми залишає за межами дослідження природи професійного ризику (за розумінням МОП) представників багатьох спеціальностей, діяльність яких пов'язана з особливими формами і особливою інтенсивністю ризиків.

Викладене вище дає підстави стверджувати, що в даний час термін «професійний ризик» монополізований системами охорони праці та соціального захисту і у визначеннях для професійного ризику в більшості не міститься психологічної складової. Тому використання даного поняття у сфері психології вимагає спеціальних застережень та уточнень.

Це пояснюється тим, що завдання МОП не передбачає дослідження природи професійного ризику, а лише розслідування їх наслідків, визначення способів та інструментів компенсації.

Поняття «професійний ризик» тісно пов'язане із поняттями «*вимушений»* та «*службовий ризик»*.

Відповідно до базового визначення, вимушений ризик – це ризик професійної діяльності людини, що здійснюється у невизначених умовах [13]. Таким чином, вимушений ризик може ототожнюватися із професійним. Підставою для цього є розуміння того, що обираючи роботу, індивід сприймає пов'язаний з нею ризик виключно як вимушений. Проте й тут виникає проблема. Вимушеному ризику за логікою повинен протистояти ризик добровільний. Втім, поняття «добровільний» погано асоціюється з терміном «професійний». Відомо, що ризик може бути допустимим, критичним або катастрофічним. Якщо йдеться про допустимий ризик, то його можна розглядати як вимушений лише, якщо це обумовлено фахом. Проте, якщо мова йде про критичний або, тим більше, катастрофічний ризик, то фахівець часто повинен приймати рішення, які виходять за межі професійної норми. Вразі, якщо йдеться про життя та здоров’я того, хто ризикує, то ризик вже не буде ані вимушеним, ані добровільним. Критерієм тоді стає високий духовний обов'язок, професійний, громадянський або моральний, а умовою − воля, свобода прийняття рішення.

Існує ще одне визначення вимушеного ризику. Він виникає внаслідок неминучості, тобто, коли іншого виходу немає [14]. Із таким визначенням теж не можна погодитися. Ризик

завжди передбачає наявність вибору. Якщо вибору немає, то ситуація трактується як дії в умовах крайньої необхідності або вплив непереборної сили.

Невизначеність, яка виникає у зв'язку з поняттями «професійний», «добровільний» та «вимушений ризик» може бути знята, якщо ввести поняття «службовий ризик», але за умови, що під службою будемо розуміти «служіння». Служіння – це суворе й точне виконання своїх прямих професійних обов'язків з самовіддачею, виконання не з обов'язку, а з внутрішньої громадянської позиції [15]. Тоді як служба – це лише вид діяльності, не пов'язаний із матеріальним виробництвом, але пов'язаний з виконанням спеціальної, суспільно значущої роботи [16]. «Служіння породжує обов'язок, обов'язок породжує ризик», – сказав одного разу Луцій Анней Сенека (Молодший) [17].

Коли йдеться про службовий обов'язок, то слід знову звернутися до проблеми класифікації. Виконання службового обов'язку в умовах ризику вимагає прийняття відповідного обґрунтованого і правомірного рішення. Суб'єкт, який реалізує ризиковану дію на виконання службового обов'язку, зобов'язаний оцінити не лише розміри можливих негативних результатів, а й те, проти кого вони будуть спрямовані.

Цей аспект надзвичайно важливий тому, що результатами ризику можуть стати смерть, втрата здоров'я, престижу, інші матеріальні й моральні збитки для суб'єкта, який здійснює ризиковану дію, матеріальну, моральну шкоду для об'єктів ризикованого дії, інші втрати щодо матеріальних, моральних цінностей, життя й здоров'я людей, політичного престижу, іміджу громадських та комерційних організацій, міжнародних відносин тощо. Аналізуючи психологію професійного, тим більше службового ризику, важливо встановити, кому й чому загрожує та чи інша форма ризикованої діяльності, чиї інтереси можуть бути порушені. При цьому нами підтримується думка щодо того, що суб'єкт в своїй професійній та службовій діяльності ризикує, перш за все, не дотриматися вимог службового, професійного, громадянського або ж морального обов'язку й нанести тим самим самому собі шкоду.

Ситуації, що виникають при цьому, можна уявити у вигляді табл. 1.

Таблиця 1

Ситуації професійного ризику (збитки персональним інтересам - Contraipsum, збитки професійним, громадським інтересам, моральним цінностям - Contraalium)

Основний результат	Побічний результат	
	Збитки персональним інтересам (Contraipsum)	Збитки професійним, громадським інтересам, моральним цінностям (Contraalium)
Досягнуто	–	–
	+	–
	–	+
	+	+
Не досягнуто	–	–
	+	–
	–	+
	+	+

Наприклад, збираючись виконати складну операцію, сприятливий результат якої сумнівний, хірург ризикує не лише своєю репутацією і, можливо, свободою, а й життям пацієнта. Дослідник, роблячи експеримент, ризикує своїм життям і здоров'ям, в той же час усвідомлює, що невдача може принести оточенню величезної шкоди. У разі ж успішного

результату, відкривається, можливо, нова ера в історії людства. Правоохоронець, затримуючи злочинця, розуміє, що в результаті його дій можуть постраждати не причасні особи або їх майно. Охоронець супермаркету, затримуючи крадія-злодюжку, ризикує завдати йому шкоди, несумірної з масштабом злочину і понести за це покарання.

Професійний ризик як психологічний феномен завжди пов'язаний із прийняттям рішення. Прийнявши одного разу рішення вступити на роботу на хімічне підприємство зі шкідливими умовами праці або увійти на небезпечну територію, людина потім довгий час залишається під впливом перманентного ризику. Загроза в цьому випадку не є дуже великою або навіть малоймовірною. Саме такий ризик знаходиться у сфері дії системи охорони праці (Міжнародна організація праці та Всесвітня організація здоров'я). Інша справа, коли виникає екстремальна ситуація, що вимагає негайного реагування. В цьому випадку має місце ситуативний ризик як варіант професійного ризику. Викладене вище дозволяє побудувати модель, наведену на рис. 1.

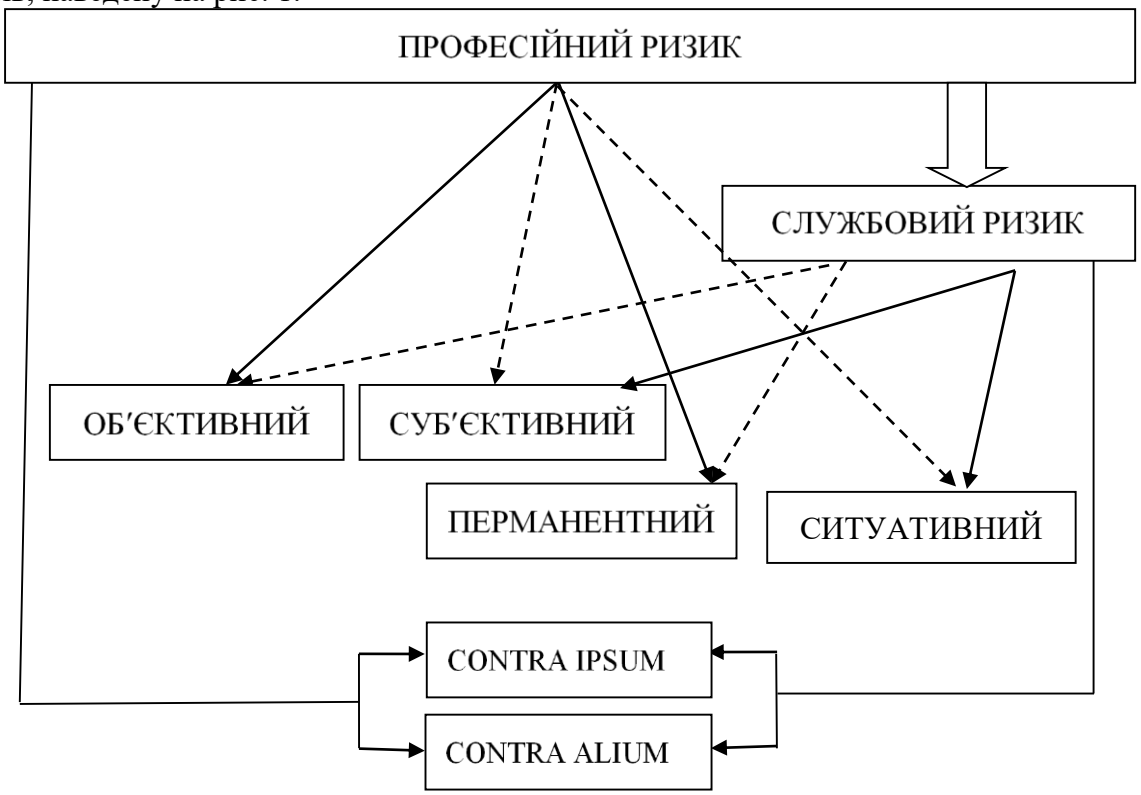

Рисунок 1 – Модель професійного і службового ризику

Висновки та перспективи подальших досліджень. У запропонованій моделі службовий ризик розглядається як частина професійного ризику. Причому професійний ризик має переважно об'єктивний і перманентний характер, а службовий – суб'єктивний і ситуативний. Важливим є також те, що професійний так само, як і службовий ризик, слід розглядати як спрямований на суб'єкт, і, окремо, на об'єкт ризикованої діяльності.

Розглядаючи професійний ризик як спосіб соціальної поведінки в умовах невизначеності, можна зробити висновок, що в складі професійного ризику, слід виділити підклас службового ризику, якій здійснюється в умовах підвищеної відповідальності, й несе інше, більш інтенсивне психологічне навантаження.

ЛІТЕРАТУРА:

1. Луман Н. Понятие риска. *THESIS: теория и история экономических и социальных институтов и систем*. 1994. № 5. С. 135-160.

2. Про внесення змін до Закону України "Про основні засади державного нагляду (контролю) у сфері господарської діяльності". URL: https://zakon.rada.gov.ua/laws/show/1726-1 (дата звернення: 15.03.2020).

3. Міжнародний стандарт OHSAS 18001 в системі менеджменту безпеки праці. URL: http://dspace.pdaa.edu.ua:8080/bitstream/123456789/1588/1.pdf (дата звернення: 15.03.2020).

4. Довідник спеціаліста з охорони праці. Харків, № 3, 2018.

5. Словарь терминов чрезвычайных ситуаций. URL: http://sbiblio.com/biblio/content.aspx (дата звернення: 16.03.2020).

6. Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності». URL: https://zakon.rada.gov.ua/laws/show/1726-1 (дата звернення: 16.03.2020).

7. Стандарт ISO 14001:2004, 3.20. URL: https://document.ua › sistemi-ekologichnogo-upravlinnja_-vimogi-ta-nastan (дата звернення: 16.03.2020).

8. The National Institute for Occupational Safety and Health (NIOSH) Dictionary. URL: https://www.cdc.gov/niosh/topics/riskassessment/default.html (дата звернення: 17.03.2020).

9. The Free Dictionary by Farlex. URL: https://www.thefreedictionary.com/occupational+risk (дата звернення: 16.03.2020).

10. Закон України «Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності. URL: https://zakon.rada.gov.ua/laws/show/1105-14/ed20100730 (дата звернення: 16.03.2020).

11. Постанова "Про затвердження Порядку об'єднання видів економічної діяльності у страхові галузеві сукупності видів економічної діяльності для визначення класу професійного ризику виробництва" від 25.12.2012 № 44. URL: https://zakon.rada.gov.ua/laws/show/z0126-13 (дата звернення: 17.03.2020).

12. Томанек Д. Соціальний захист працюючих від нещасних випадків на виробництві та професійних захворювань. Київ: Основа, 2006. 336 с.

13. Ильин Е.П. Психология риска. Санкт-Петербург, «Питер». 2012. 237 с.

14. Психологический лексикон. Энциклопедический словарь: в 6 т. / за ред.: Л.А. Карпенко, А.В. Петровского. Москва: ПЕР СЭ, 2006. 176 с.

15. Большой юридический словарь / общ. ред. А.Я. Сухарев. Москва, 2007, 858 с.

16. Психологічний словник / за ред. В.І. Войтка. Київ: Вища школа. 1982. 216 с.

17. Лозовицький О. Сенека Луцій Анней / Політична енциклопедія / за ред.: Ю. Левенець, Ю. Шаповал та ін. Київ: Парламентське видавництво, 2011. С.151–173.

REFERENCES:

1. Luman, N. (1994), "Ponyatie riska. THESIS: teoriya i istoriya ekonomicheskih i sotsialnyih institutov i sistem" [Risk concept], THESIS: Theory And History Of Economic And Social Institutions And Systems,No. 4, pp. 135-160.

2. "Pro vnesennia zmin do Zakonu Ukrainy "Pro osnovni zasady derzhavnoho nahliadu (kontroliu) u sferi hospodarskoi diialnosti"" [On Amendments to the Law of Ukraine "About the main ambush of the sovereign glance (control) of the sphere of state dariality], www.zakon.rada.gov.ua/go/167-2019-p (accessed 15 March 2020).

3. "Mizhnarodnyi standart OHSAS 18001 v systemi menedzhmentu bezpeky pratsi" [OHSAS 18001 International Standard in Occupational Safety Management System], www.dspace.pdaa.edu.ua:8080/bitstream/123456789/1588/1.pdf (accessed 15 March 2020).

4. "Dovidnyk spetsialista z okhorony pratsi" [Directory Of The Specialist On Labor Protection] (2018), Kharkiv, No 3.

5. "Slovar terminov chrezvyichaynyih situatsiy" [Glossary of Emergency Terms], www.sbiblio.com/biblio/content.aspx (accessed 16 March 2020).

6. "Zakon Ukrainy "Pro osnovni zasady derzhavnoho nahliadu (kontroliu) u sferi hospodarskoi diialnosti"" [The Law of Ukraine "On Basic Principles of State Supervision (Control) in the Field of Economic Activity], www.zakon.rada.gov.ua/laws/show/1726-1 (accessed 16 March 2020).

7. "Standart ISO 14001:2004, 3.20" [Standart ISO 14001:2004, 3.20], www.document.ua › sistemi-ekologichnogo-upravlinnja_-vimogi-ta-nastan (accessed 16 March 2020).

8. "The National Institute for Occupational Safety and Health (NIOSH) Dictionary", www.cdc.gov/niosh/topics/riskassessment/default.html (accessed 17 March 2020).

9. ”The Free Dictionary by Farlex”, www.thefreedictionary.com/occupational+risk (accessed 17 March 2020).

10. ”Zakonu Ukrainy ”Pro zahalnooboviazkove derzhavne sotsialne strakhuvannia vid neshchasnoho vypadku na vyrobnytstvi ta profesiinoho zakhvoriuvannia, yaki sprychynyly vtratu pratsezdatnosti”” [Law of Ukraine ”On Compulsory State Social Insurance against Industrial Accidents and Occupational Diseases that Caused Disability”], www.zakon.rada.gov.ua/laws/show/1105-14/ed20100730 (accessed 16 March 2020).

11. ”Postanova ”Pro zatverdzhennia Poriadku obiednannia vydiv ekonomichnoi diialnosti u strakhovi haluzevi sukupnosti vydiv ekonomichnoi diialnosti dlia vyznachennia klasu profesiinoho ryzyku vyrobnytstva” vid 25.12.2012 N 44” [Resolution ”On Approval of the Procedure for Combining Economic Activities in Insurance Sectoral Groups of Economic Activities for Determining the Occupational Risk Class of Production” of 25.12.2012 No. 44], (accessed 17 March 2020).

12. Tomanek, D. (2006), ”Sotsialnyi zakhyst pratsiuiuchykh vid neshchasnykh vypadkiv na vyrobnytstvi ta profesiinykh zakhvoriuvan” [Social Protection Of Workers Against Industrial Accidents And Occupational Diseases], Kyiv, 336 p.

13. Ylyn, E.P. (2012). ”Psykholohyia ryska” [Psychology of Risk], Sankt-Peterburh, ”Piter”, 237 p.

14. Karpenko, L.A., Petrovskiy, A.V. (2006). ”Psihologicheskiy leksikon. Entsiklopedicheskiy slovar: v 6 t.” [Psychological vocabulary. Encyclopedic Dictionary], Moscow, 176 p.

15. Suharev, A.Ya. (2007), ”Bolshoy Yuridicheskiy Slovar” [Great Law Dictionary], Moscow, 858 p.

16. Voitko, V.I. (1982), ”Psykholohichnyi slovnyk” [Psychological Dictionary], Kyiv, 216 p.

17. Lozovytskyi, O., Levenets, Yu., Shapoval, Yu. (2011),”Seneka Lutsii Annei” [Seneca Lucius Anney], Kyiv, pp. 151-173.

д.пед.н., доц. Артемов В.Ю., к.т.н., с.н.с. Литвиненко Н.И.

ПРОФЕССИОНАЛЬНЫЙ РИСК КАК СПОСОБ СОЦИАЛЬНОЙ ПОВЕДЕНИЯ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

В статье определено место и роль профессионального риска как способа социального поведения в условиях неопределенности. Показано, что Международная организация труда, Всемирная организация здравоохранения (International Standard Organization) занимается вопросами регулирования или управления профессиональными рисками.

Профессиональный риск представляет собой сложное явление, по определению которого нет единства в словарях, энциклопедиях, нормативно-правовых документах и научных публикациях.

Определяется, что человек в процессе профессиональной, часто монотонной деятельности, привыкает к риску, не замечает и не оценивает профессиональный риск. Доказано, что классы профессионального риска производства определяются в зависимости от уровня производственного травматизма и профессиональных заболеваний по видам экономической деятельности, что определяет степень вероятности потери профессиональной трудоспособности или смерти работника при исполнении трудовых обязанностей с учетом результатов анализа статистики происшествий.

Выдвигается предположение, что профессиональный риск как психологический феномен всегда связан с принятием решения. Делается акцент на том, что понятие «профессиональный риск» имеет преимущественно объективный и перманентный характер, а служебный - субъективный и ситуативный. Важно также то, что профессиональный, так же, как и служебный риск, следует рассматривать как направленный на субъект, и, отдельно на объект рискованной деятельности.

Таким образом, рассматривая профессиональный риск как способ социального поведения в условиях неопределенности, можно сделать вывод, что в составе профессионального риска, следует выделить подкласс служебного риска, которой осуществляется в условиях повышенной ответственности, и несет другое, более интенсивное психологическое напряжение.

Ключевые слова: риск, профессиональный риск, вынужден риск, служебный риск, поведение.

Doctor of Pedagogical Sciences Artemov V.U., Ph.D. Lytvynenko N.I.

PROFESSIONAL RISK AS A WAY OF SOCIAL BEHAVIOR IN TERMS OF UNCERTAINTY

The article defines the place and role of professional risk as a way of social behavior in conditions of uncertainty. It is shown that the International Labor Organization, the World Health Organization (International Standard Organization) deals with regulation issues or occupational risks management.

Occupational risk is a complex phenomenon, by the definition of that there is no unity in dictionaries, encyclopedias, regulatory documents and scientific publications.

It is determined that a person in the process of professional, often monotonous activity, gets used to risk, doesn't notice and doesn't evaluate professional risk. It is proved that the classes of occupational risk are determined depending on the level of occupational injuries and occupational diseases by type of economic activity, determines the degree of probability of the professional loss ability to work or death of an employee in the performance of labor duties, taking into account the results of the accident statistics analysis.

It is suggested that occupational risk as a psychological phenomenon is always associated with decision making. The emphasis is placed on the fact that the concept of "professional risk" has a predominantly objective and permanent character, while the service one is subjective and situational. It is also important that professional, as well as official risk, should be considered as aimed at the subject, and, separately, at the object of risky activity.

Thus, considering professional risk as a way of social behavior in conditions of uncertainty, we can conclude that in the composition of professional risk, it is necessary to distinguish a subclass of official risk, which is carried out in conditions of increased responsibility, and carries another, more intense psychological stress.

Keywords: risk, professional risk, forced risk, business risk, behavior.

УДК 32.973.202:07.681

к.т.н. **Бабіч О.М.** (ВІКНУ)
Матвієнко О.О. (ВІКНУ)
Глухова А.С. (КНТЕУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-13

ПІДХІД ДО АНАЛІЗУ ІНФОРМАЦІЙНОГО ПОТОКУ НОВИН ЗМІ З ОЦІНЮВАННЯМ ЙОГО ЕМОЦІЙНИХ ХАРАКТЕРИСТИК

Вивчення особливостей інформаційного середовища – важливий елемент інформаційно-аналітичної діяльності, який дозволяє сформувати аналітику більш повне і чітке уявлення про обстановку. Адже це важливий відправний пункт для реагування на інформацію про події. Підходи до опрацювання інформаційного потоку новин засобів масової інформації розробляються за різноманітними напрямами, у даній статті представлено підхід до опрацювання інформаційного потоку новин ЗМІ із аналізом емоційного компоненту, вимірюванням його інтенсивності та оцінюванням елементів, які формують емоційні характеристики тексту.

Новини ЗМІ є емоційно-насиченою інформацією, тому важливо вміти виявляти, що саме нагнітає в них емоційний стан, помічати властиві вислови та правильно їх оцінювати. У цьому аспекті важливим є правильний переклад кожної фрази, адже поряд із суспільно-політичною лексикою у мас-медіа наявні ідіоматичні вислови, які автори текстів новин вживають задля надання своєму повідомленню більш яскравої забарвленості. Тому вони повинні бути розпізнані і перекладені належним способом. Мовні одиниці, якими передаються у тексті емоції та емоційні стани, називаються концептами. У кожній мові використовується властива саме їй система концептів, яка невідривно пов'язана із культурою народу – носія мови.

Концепти, що передають певні емоції у тексті, формують його емоційну забарвленість. Оцінити її можна за кількісними і якісними показниками шляхом привласнення відповідних вагових коефіцієнтів окремим емоційним висловам, які представлені звичайними словосполученнями та ідіоматичними зворотами. Для оцінювання емоційної забарвленості доцільно з текстового корпусу сформувати базовий словник зі відповідним набором символів, які в подальшому беруть участь у розрахунку коефіцієнту емоційної забарвленості. За найбільш значущими критеріями, які формують характеристики повідомлення, оцінюється інтенсивність його інформаційного впливу із виведенням результатів у графічній формі на інтерфейс користувача.

Використання даного підходу дає можливість розглянути різні аспекти інформаційного потоку новин ЗМІ та оцінити його за різноманітними характеристиками, що збільшує практичні можливості з опрацювання потоку новин ЗМІ в інтересах забезпечення безпеки.

Ключові слова: безпека, інтенсивність, концепт, емоційна забарвленість.

Вступ. Важливим фактором інформаційно-аналітичної діяльності є інформаційне середовище та його властивості. Їх вивчення забезпечує здатність як експерта, так і пересічної людини до розуміння навколишніх інформаційних процесів та реагування на події відповідним чином. Адже особливості їх подання є одним з інструментів інформаційної війни і своєрідною невоєнною тактикою, що відноситься до елементів безпеки, зокрема політики стратегічного стримування [1].

Такі фактори як умови невизначеності, разом із сильним інформаційним тиском, які часто супутні інформаційно-аналітичній роботі, супроводжують процес прийняття рішення. Надходження хибної інформації вимагає увімкнення критичного мислення, яке дозволяє побачити, які саме засоби використовуються у засобах масової інформації (ЗМІ) для привертання уваги і формування потрібної думки про подію. З урахуванням цього, останні дослідження свідчать про зростання потреби розвитку нових методів опрацювання інформаційних потоків і дослідження особливостей інформаційного середовища.

Аналіз останніх досліджень. Проблеми аналітичного опрацювання новин ЗМІ в інтересах національної безпеки всебічно вивчались у вітчизняних і зарубіжних дослідженнях [1 - 6]. Використання засобів інформаційної війни для завоювання противника зсередини з перспективою забезпечення власних стратегічних інтересів вивчалось у [1]. Розгляд проблеми активізації наступальних інформаційних ресурсів країн потенційного противника та способи їх стримування запропоновані у [2]. Засоби подання інформаційного матеріалу, зокрема сюжетів новин на тему війни, через аудіовізуальні канали із задіянням спеціальних прийомів донесення інформації до аудиторії, розглянуті у [3]. Дослідження новин ЗМІ щодо активності аудиторій відносно публікацій та відповідність реагування на зміст новин у соцмережах залежно від типу інтернет-аудиторії (стать, регіон проживання тощо) проведено у [4]. Проблема домінування в інформаційному полі за наявності політичного протистояння з визначенням необхідних для цього інформаційних засобів розглядались у [5]. Використання лексики та спеціальних мовних засобів у новинах ЗМІ з урахуванням їх особливостей для інформування закордонної аудиторії під час ведення війни представлені у [6].

При цьому у розгляді різних аспектів опрацювання інформації не приділялось достатньо уваги вивченню емоційного фактору, який передається лінгвістичними засобами, та його впливу на зміст тексту новин ЗМІ.

З огляду на це, **метою і основним змістом статті** є визначення підходу до аналізу емоційного компоненту інформаційного потоку новин ЗМІ і до вимірювання його інтенсивності, з оцінюванням складових, які формують емоційні характеристики тексту.

Викладення основного матеріалу. Емоції – невід'ємна частина більшості новин і емоційних висловів, що активно використовуються у ЗМІ. Їх присутність всередині новин забезпечує тривалу фіксацію всередині пам'яті людини та залишення у її психіці назавжди [7]. Тому для відстеження емоційного впливу в емоційно-насиченій інформації, зокрема новинах

ЗМІ, важливо вміти виявляти, що саме нагнітає емоційний стан, помічати властиві вислови та правильно їх оцінювати.

Для цього в ході вивчення текстів новин ЗМІ експертами були відібрані основні властиві їм емоції, які базуються на класифікації К. Ізарда [8]. Це, зокрема:

1. Радість
2. Здивування
3. Сум
4. Гнів
5. Відраза
6.Зневага
7. Горе
8. Сором
9. Інтерес
10. Провина
11. Спантеличення.

Інші емоційні стани утворюються поєднанням цих емоцій.

Для передачі емоцій та емоційних станів у тексті використовуються відповідні мовні одиниці – концепти. Широко відомо, що система концептів, що використовується у повсякденному житті, міститься у лексичному компоненті мови. Ця система концептів невідривно пов'язана із культурою аутентичних носіїв мови та має етно-семантичні ознаки.

Одним з розповсюджених лексичних засобів, що передають емоції у тексті, є ідіоматичні звороти. Вони є часткою системи культурних цінностей країни, яка базується на її самобутніх складових. Ідіоматичні звороти – це емоційно-оцінні засоби, які є своєрідними маркерами відношення людей до певних явищ суспільного життя, прийнятого в даній національній культурі. Назва походить від грецької idioma – "своєрідний вираз" – це стійкий мовний зворот, неподільне словосполучення, значення якого відрізняється від значення слів, що входять до його складу [9].

У текстах новин, як вітчизняних, так і іншомовних, трапляються випадки, коли для створення більш яскравого враження вживаються не лише звичайні емоційні вирази, а й ідіоматичні звороти. Їх емоційна забарвленість, на перший погляд, є нейтральною, проте при більш ретельному розгляді виявляється, що буквальний переклад є помилковим, у даного мовного звороту існує ще друге значення, яке і слід враховувати як правильне. При цьому таке значення є емоційно-забарвленим і впливає на формування враження від того, про що йдеться у тексті повідомлення. Тому при опрацюванні тексту іншомовних новин важливим є орієнтування у лінгвістичній складовій і правильний переклад змісту тексту.

Так, в англійській мові, за наявності зазначених фраз слід відрізняти буквальний переклад наступних ідіом від того змісту, який закладений у них насправді. Наприклад, емоційні реакції, такі як гнів, роздратування, ігнорування, або стан від здобуття перемоги передаються наступними ідіоматичними зворотами [10, 11]:

To be on the warpath / ram page – шукати бійки, бути дуже розлюченим або засмученим кимось/чимось;

A bad blood – погані відчуття;

To play hardball – робити/працювати агресивно чи грубо;

To see red – розсердитись;

To get someone's goat – роздратувати когось або набриднути;

To have the last laugh – отримати реванш над кимось, хто вважав себе сильнішим/розумнішим;

To turn a deaf ear – ігнорувати когось.

To give someone the cold shoulder – навмисно ігнорувати когось;

Get off one's high horse – припинити вести себе зверхньо.

Їх правильний переклад показує справжній зміст і відповідну емоційну забарвленість, закладені у текст.

Як слідує з вищевикладеного, емоційна забарвленість – важлива характеристика тексту новин ЗМІ. Вона відображає його характер і є складовою інформаційного потоку. На її формування впливають засоби, які розглядаються у даній статті.

Характер емоційної забарвленості тексту новин можна визначати як за вмістом певних емоцій (якісно), так і за їх числовим показником (кількісно). Це досягається привласненням відповідних вагових коефіцієнтів окремим емоційним висловам, які представлені як звичайними словосполученнями, так і вищезгаданими мовними зворотами.

Оцінювання повідомлень за кількісними і якісними показниками характеризує стан певного предмету або проблеми.

Метод оцінювання їх емоційної забарвленості передбачає формування базового словника на основі текстового корпусу:

$$V{:}= \langle w_i (k_i V p_i) \rangle, \; i = 1, \; \ldots n \; \ldots\ldots \tag{1}$$

де: *V:* – множина словоформ у вигляді текстового корпусу;

w_i – словникова одиниця у нормалізованому вигляді;

k_i – ваговий коефіцієнт емоційної забарвленості словоформи w_i;

p_i – ваговий коефіцієнт посилення емоційної забарвленості словоформи w_i;

Знак *V* – логічна операція «або», яка означає, що словоформі w_i може бути приписаний лише один з визначених коефіцієнтів.

Наступні кроки з оцінювання емоційної забарвленості включають:

привласнення кожній емоції з визначеного набору вагового коефіцієнту для ідентифікації фрагменту тексту, якому вона відповідає;

формування синтаксичної структури для кожного речення тексту та міжфразових синтаксичних структур;

послідовний підрахунок значень коефіцієнтів у тексті за правилом сумації коефіцієнтів:

$$k(R) = \frac{\sum_{i=1}^{N} k(S_i)}{N}, \tag{2}$$

де: *R* – довільне речення в тексті;

k(R) – ваговий коефіцієнт емоційної забарвленості довільного речення в тексті;

$\sum_{i=1}^{N} k(S_i)$ – сума вагових коефіцієнтів словоформ у даному реченні;

N – кількість словоформ у даному реченні.

Найбільш пріоритетні критерії формують інтенсивність інформаційного впливу новини, яка визначається за формулою [12]:

$$I = \frac{\sum_{i=1}^{m} G}{n}, \tag{3}$$

Де *I* – загальна інтенсивність інформаційного впливу новини, що включає усі наявні параметри;

G – показники інформаційного впливу, що включають кількісні і якісні показники;

n – кількість елементів з оціненим на попередніх етапах ступенем важливості.

Результати оцінювання властивостей новини і її емоційної забарвленості доцільно виводити на інтерфейс користувача у графічному вигляді.

Висновки. Таким чином, емоційна забарвленість тексту – його важлива характеристика, яка має вирішальне значення у розповсюдженні тексту новин ЗМІ для поширення необхідних поглядів на суспільно-політичні процеси та формування у цільової аудиторії заданого

ставлення. Представлена на лексичному рівні, вона тісно пов'язана із фразовими словосполученнями та іншими мовними засобами, що створюють характер тексту і забезпечують краще сприйняття змісту новини аудиторією. Ця характеристика формується в ході взаємодії у тексті різноманітних лексичних засобів, які її передають, з іншими словоформами речення, і може бути визначена за допомогою належних правил. Завдяки цьому інформаційний потік новин ЗМІ може бути розглянутий у різних аспектах, а його оцінювання – проводитись за набором різнопланових характеристик. Використання даного підходу сприяє зростанню практичних можливостей інформаційно-аналітичної діяльності щодо вивчення матеріалів ЗМІ в інтересах вирішення широкого спектру проблем національної безпеки.

ЛІТЕРАТУРА:

1. D. Lewis. Russia's "Strategic Deterrence" in Ukraine. // [Електр. Ресурс] – Режим доступу: https://www.marshallcenter.org/mcpublicweb/mcdocs/security_insights_29_-_updated_-_lewis_-_david_lewis_-_strat_deterrence_in_ukr_-_april_2019_-aug_26.pdf

2. J. Clarke. Defeating the Russian Cyber Challenge, Loisach Group Note 3, 2018). // [Електр. Ресурс] – Режим доступу: https://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/loisach_group/loisach-group-note-3.pdf

3. L. Doucet. Syria & the CNN Effect: What Role Does the Media Play in Policy-Making? // [Електр. Ресурс] – Режим доступу: https://www.mitpressjournals.org/doi/pdf/10.1162/DAED_a_00480

4. G. King1, B. Schneer, A. White. How the news media activate public expression and influence national agendas. // [Електр. Ресурс] – Режим доступу: https://gking.harvard.edu/files/gking/files/776.full_.pdf

5. Инфовойны в современном контексте. Золотухін Д.Ю. Міжнародний форум з кризових комунікацій "Комунікаційно-контентна безпека в умовах гібридно-месіанських агресій путінської Росії". 9-10 червня 2016 р. К., 2016. ВІКНУ.— С.124.

6. Особливості формування суспільної думки у провідних зарубіжних ЗМІ стосовно військового конфлікту на Сході України. Марченко-Бабіч О.М. Міжнародний форум з кризових комунікацій "Комунікаційно-контентна безпека в умовах гібридно-месіанських агресій путінської Росії". 9-10 червня 2016 р. К., 2016. ВІКНУ. – С.47.

7. Шутов Р. Як меседжі російської пропаганди перетікають в український інфопростір. // [Електр. Ресурс] – Режим доступу: http://osvita.mediasapiens.ua/monitoring/advocacy_and_influence/yak_mesedzhi_rosiyskoi_propagandi_peretikayut_v_ukrainskiy_infoprostir

8. Ізард К. Психология эмоций. – Спб.: Питер, 2012. – 464 с.

9. Комлев Н.Г. Словарь иностранных слов. –2006. // [Електр. Ресурс] – Режим доступу: https://dic.academic.ru/dic.nsf/dic_fwords/16750/%D0%

10. Як викликати емоції через текст // [Електр. Ресурс] – Режим доступу: (https://euprostir.org.ua/practices/134839)

11. Г. Кузенко. Мовні засоби вираження емотивності. Movni zasoby vyragiennya emotivnosty. // [Електр. Ресурс] – Режим доступу: http://ekmair.ukma.edu.ua/bitstream/handle/123456789/9836/Kuzenko_Movni_zasoby_vyrazhennya.pdf?sequence=1&isAllowed=y

12. O. Babich, N. Popov, S. Glukhov. "The basics for development of mass media information stream classifier". 8 – 10 August 2019. Proceedings of AC2019 in Prague. Czech Technical University in Prague. P.157–164.

REFERENCES:

1. D. Lewis, Russia's "Strategic Deterrence" in Ukraine. [Online]. Available: https://www.marshallcenter.org/mcpublicweb/mcdocs/security_insights_29_-_updated_-_lewis_-_david_lewis_-_strat_deterrence_in_ukr_-_april_2019_-aug_26.pdf

2. J. Clarke, Defeating the Russian Cyber Challenge, Loisach Group Note 3. [Online]. Available: https://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/loisach_group/loisach-group-note-3.pdf

3. L. Doucet. Syria & the CNN Effect: What Role Does the Media Play in Policy-Making? [Online]. Available: https://www.mitpressjournals.org/doi/pdf/10.1162/DAED_a_00480

4. G. King1, B. Schneer, A. White. How the news media activate public expression and influence national agendas. [Online]. Available: https://gking.harvard.edu/files/gking/files/776.full_.pdf

5. Infovojny v sovremennom kontekste. Zolotuhin D.Yu. Mizhnarodnij forum z krizovyh komunikacij "Komunikacijno-kontentna bezpeka v umovah gibridno-mesians'kih agresij putins'koï Rosiï". 9-10 chervnya 2016 r. K., 2016. VIKNU.— S.124.

6. Osoblivosti formuvannya suspil'noï dumki u providnih zarubizhnih ZMI stosovno vijs'kovogo konfliktu na Skhodi Ukraïni. Marchenko-Babich O.M. Mizhnarodnij forum z krizovih komunikacij "Komunikacijno-kontentna bezpeka v umovah gibridno-mesians'kih agresij putins'koï Rosiï". 9-10 chervnya 2016 r. K., 2016. VIKNU.- S.47.

7. Shutov R. Yak mesedzhi rosijs'koï propagandi peretikayut' v ukraïns'kij infoprostir. // [Elektr. Resurs] – Rezhim dostupu: http://osvita.mediasapiens.ua/monitoring/advocacy_and_influence/yak_mesedzhi_rosiyskoi_propagandi_peretikayut_v_ukrainskiy_infoprostir

8. Izard K. Psihologiya emocij. - Spb.: Piter, 2012. - 464 s.

9. Komlev N.G. Slovar' inostrannyh slov. –2006. // [Elektr. Resurs] – Rezhim dostupu: https://dic.academic.ru/dic.nsf/dic_fwords/16750/%D0%

10. Yak viklikaty emociï cherez tekst // [Elektr. Resurs] – Rezhim dostupu: (https://euprostir.org.ua/practices/134839)

11. G. Kuzenko. Movni zasobi virazhennya emotivnosti. Movni zasoby vyragiennya emotivnosty. // [Elektr. Resurs] – Rezhim dostupu: http://ekmair.ukma.edu.ua/bitstream/handle/123456789/9836/Kuzenko_Movni_zasoby_vyrazhennya.pdf?sequence=1&isAllowed=y

12. O. Babich, N. Popov, S. Glukhov. "The basics for development of mass media information stream classifier". 8 – 10 August 2019. Proceedings of AC2019 in Prague. Czech Technical University in Prague. P.157–164.

Ph.D. Babich O.M., Matviyenko O.O., Gluhova A.S.

APPROACH TO MASS MEDIA NEWS INFORMATION WORKFLOW ANALYSIS IN VIEW OF ITS EMOTIONAL CHARACTERISTICS

Research of information environment features is a vital element of information and analytical activity that makes possible to form the situation view more complete and precise. It is an important benchmark to react events information. Development of approaches to the information workflow processing concerns different aspects. The approach to mass media news information workflow processing with regard to its emotional component analysis and its intensity measurement is presented in this article. The elements which form emotional characteristics of news texts are also included.

The nature of mass media news is emotionally saturated, so it is important to identify the factors which pressurize emotional state, notice relative phrases and evaluate them in a proper way. Therefore, proper translation of each phrase is critical due to the presence of idioms next to social and political lexis in mass media, which are used by news texts authors to impart a message a brighter character. With this in view these phrases demand a proper translation. The name for lingual units that transmit emotions and emotional states is concepts. Each language disposes its own concepts system related inseparably to the national culture of the native speaker's language.

Concepts which transmit certain emotions in the text form its emotional coloring. It can be evaluated by quantitative and qualitative indexes by appropriation of respective weighting ratios to particular emotional expressions. These expressions are transmitted with conventional phrases or idioms. It is advisable to form basic vocabulary of the text corpora with corresponding characters set which is a part of emotional coloring rate assessment procedure. The intensity of information impact is assessed by the most significant criteria, which form news nature. Outcome is graphically performed at the user's display.

This approach application enables examination of different aspects of mass media information stream and makes possible to estimate it by various characteristics. In this way the presented application extends practical opportunities of news information workflow processing with the view of national security interests.

Keywords: security, intensity, concept, emotional coloring.

УДК 355.233:37.018.43(045)

к.е.н., доц. **Городянська Л.В.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-14

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО НАВЧАННЯ У СИСТЕМІ ВИЩОЇ ВІЙСЬКОВОЇ ОСВІТИ

У статті визначено, що підґрунтям забезпечення дистанційного навчання у системі військової освіти є суб'єктно-діяльнісний підхід. Узагальнено позитивні аспекти застосування технології дистанційного навчання з позиції викладача та з позиції суб'єкта навчання. Процеси організації й впровадження дистанційного навчання обумовлені специфікою військового навчального закладу та залежать від психолого-педагогічних особливостей викладача, його професійної майстерності використовувати сучасні інтерактивні методики навчання й інформаційно-комунікаційні технології. Здійснено спробу визначити основні психолого-педагогічні риси викладача, які потрібні в процесі організації дистанційного навчання. Це – висока мотивація до пізнавальної діяльності, набуття нових професійних компетенцій, вміння уникати суб'єктивізму під час оцінювання. Застосування дистанційного навчання дозволяє суттєво знизити витрати на навчання, активізувати процес пізнання завдяки різноманітним наочним засобам представлення нової навчальної інформації з використанням сучасних інформаційних технологій.

Доведено, що перспективним напрямом навчання у системі вищої військової освіти є змішане навчання. Це інтерактивна форма, яка дозволяє оптимально поєднати формат очного й дистанційного навчання. Організація змішаного навчання дає змогу створити відповідне середовище для успішного виконання військових обов'язків під час навчання у військовому закладі, самостійної підготовки до аудиторних занять і самостійного опрацювання навчального матеріалу у зручний час. Застосування такої форми навчання сприятиме активізації пізнавальної діяльності, розширенню можливостей набуття як професійних компетенцій, так і «м'яких» навичок, які є підґрунтям виховання та гармонійного розвитку особистості у системі військової освіти.

Розвиток системи вищої військової освіти пов'язано саме з дистанційним навчанням як пріоритетної технології, що базується на системі управління навчальним контентом Moodle. Належна організація навчання дозволяє створити умови для підвищення мотивації суб'єкта навчання до розумової діяльності й до набуття якісної військово-професійної освіти.

Ключові слова: суб'єктно-діяльнісний підхід, дистанційне навчання, інформаційно-комунікаційні технології, змішане навчання, суб'єкт навчання, система вищої військової освіти.

Вступ. Підвищення якості та конкурентоспроможності освіти в умовах глобалізації цифрової економіки, прискорення інтеграції України у міжнародний освітній простір супроводжується поширенням інноваційних інформаційних технологій в навчальному процесі. Сучасна система вищої освіти, що забезпечує формування людського потенціалу, передбачає використання як традиційних, так і інноваційних методів навчання. Вважається, шо система української вищої освіти є досить розвиненою, однак цифровізація економіки, інтеграція освіти і практики потребують модернізації освітнього процесу в контексті змінювання підходів до ролі людини, що навчається, з пасивного учасника навчального процесу до активного залучення його до навчальної діяльності. З розвитком загальнодержавної системи освіти в Україні нерозривно пов'язані координація, розвиток і впровадження дистанційного навчання у систему вищої військової освіти.

Постановка проблеми. Одним із кроків України на шляху інтеграції до Європейського освітнього простору й реформування системи вищої освіти в цілому та військової освіти зокрема, було прийняття низки документів [1-4] та ін. Щодо військової освіти, то у Концепції дистанційного навчання у Збройних Силах України [4] підкреслюється потреба у реформуванні системи військової освіти в контексті впровадження безперервної ступеневої системи навчання військових фахівців «протягом усього життя». Разом з тим розвиток і поширення інтернетизації в усіх сферах життєдіяльності суспільства, висока динамічність

військово-політичних подій, постійна потреба у ротації особового складу Збройних Сил на усіх рівнях потребують підготовки військових фахівців у стислі терміни без зниження компетентнісних показників і на сучасному рівні. Тому зазначені напрями модернізації освітнього процесу, зокрема у системі вищої військової освіти, мають бути переосмислені з позицій сучасних реалій та особливо з урахуванням особистісних якостей, здібностей і спрямованості суб'єкта навчання до певних видів діяльності та самонавчання, що складає методологічні засади технології дистанційного навчання.

Аналіз останніх досліджень і публікацій. Інформаційною базою для проведення дослідження стали чинні нормативно-правові документи у галузі вищої освіти [1-5] та праці таких вчених, як К.Ф. Боряк, С.В. Гахович, Ю.О. Гунченко, В.М. Кухаренко, С.В. Лєнков, В.Є. Лукін та інші [6-8].

У колективній монографії С.В. Лєнкова, С.В. Гаховича, Ю.О. Гунченко та ін. [6] значну увагу приділено особливостям побудови систем дистанційного навчання, розкриттю дидактичних можливостей, визначенню методологічних підходів до підготовки та/або адаптації навчального матеріалу до умов викладання й до інших проблем, що виникають у процесі дистанційного навчання та виховання студентів.

Враховуючи сучасні тенденції розвитку освітніх технологій у системі вищої освіти, динамічний розвиток і доступність до інформаційних технологій, основні напрями державної політики в галузі освіти, розвиток дистанційного навчання стає дієвим інструментом реалізації моделі безперервного навчання протягом усього життя. Цей напрям є особливо актуальним в екстремальних умовах або наближених до них, коли виникає нагальна потреба набувати знання на відстані від навчального закладу й мають місце фізичні та/або територіальні обмеження. Тут на перше місце виходять автоматизовані навчальні системи, технічні й методологічні засади яких вже розроблені й запроваджені у навчальний процес на усіх рівнях.

Під автоматизованою навчальною системою розуміється узгоджена сукупність навчальних матеріалів, засобів їх розробки, зберігання, передачі і доступу до них, призначена для цілей навчання і заснована на використанні сучасних інформаційних технологій. Методики планування й організації проведення занять із застосуванням засобів автоматизованої навчальної системи розкриті у праці [7]. Вважаємо дуже слушною думку авторів К.Ф. Боряка, Ю.О. Гунченко, С.В. Лєнкова та ін. щодо застосування систем дистанційного навчання в процесі вивчення технічних дисциплін. Спираючись на методичні основи, які розкриті у праці [7, с. 30-71], обґрунтування вимагають особливості практичного застосування систем дистанційного навчання у системі військового навчального закладу (ВНЗ).

Огляд фахової літератури [6-8] показав, що теоретичні питання застосування систем дистанційного навчання та методик професійної підготовки військових фахівців є досить дослідженими науковцями. Але, незважаючи на це, проблеми організації дистанційного навчання у ВНЗ в сучасних умовах, розробки дистанційних курсів спеціальних дисциплін, їх впровадження у навчальний процес в реаліях сьогодення є актуальними і потребують подальшого дослідження. Так, згідно з оперативною ціллю 5.2 Стратегічного оборонного бюлетеня України [5] передбачено впровадження технологій дистанційного навчання в освітній процес задля поліпшення системи військової освіти та підготовки кадрів.

Посилення вимог держави до рівня кваліфікації суб'єктів навчання, які визначені у соціальному замовленні, зростання потреб користувачів до професійної підготовки з врахуванням навичок володіння технічними засобами навчання зумовлюють необхідність розкриття підходів до організації дистанційного навчання у системі вищої військової освіти та уточнення особливостей викладання дисциплін на базі сучасних інтерактивних технологій.

Метою статті є визначення особливостей організації дистанційного навчання в системі вищої військової освіти з урахуванням суб'єктно-діяльнісного підходу.

Досягнення мети зумовлює необхідність вирішення комплексу таких завдань:

- визначити роль суб'єктно-діяльнісного підходу як підґрунтя забезпечення дистанційного навчання у системі військової освіти;

- визначити основні позитивні аспекти впровадження технології дистанційного навчання з позиції суб'єкта навчання та викладача;

- сформувати основні позитивні психолого-педагогічні аспекти впровадження дистанційного навчання в освітній процес ВНЗ;

- обґрунтувати оптимальну форму організації та активізації навчально-пізнавальної діяльності курсантів з врахуванням специфіки навчання у вищому військовому закладі.

Теоретичні основи дослідження. Одним із важливих напрямів модернізації системи вищої освіти вважаємо її інформатизацію. Інтенсифікація процесів інформатизації у вітчизняній освіті відбувається з початку 2000-х років. До них належать заходи із забезпечення вищих навчальних закладів комп'ютерною технікою і створення програмного забезпечення навчального призначення, доступ до інформаційних ресурсів Інтернету та інших навчально-інформаційних мереж, інформатизацію документообігу й керування навчальним процесом тощо.

Наразі система вищої освіти має забезпечувати координуючі функції щодо розвитку потенціалу людини – суб'єкту навчання з використанням засобів інтернет-технологій. Проведене нами дослідження [9] дозволило визначити, що в контексті організації дистанційного навчання пріоритетності набуває суб'єктно-діяльнісний підхід, застосування якого дозволяє активізувати навчально-пізнавальну діяльність суб'єкта навчання, інтенсифікувати навчальний процес, сформувати стійку зацікавленість військових фахівців до самовдосконалення у системі вищої військової освіти.

Опанування вимог нормативно-правових документів [1-5] та використання суб'єктно-діяльнісного підходу у забезпеченні організації дистанційного навчання у системі вищої військової освіти дозволило нам узагальнити такі особливості:

- забепечення системності та керованості процесів розробки та впровадження технологій дистанційного начання;

- доступ військового навчального закладу до сучасних інформаційних технологій;

- розроблення власних та адаптація існуючих ресурсів дистанційного навчання;

- поєднання традиційного, он-лайн навчання та самостійного навчання;

- дотримання режиму безпеки інформації у процесі використання технологій дистанційного начання, мережі Internet тощо.

З питаннями інформатизації, створення та використання нових методик і форм навчання в системі вищої освіти пов'язаний об'єкт нашого дослідження – дистанційне навчання. Опанування вимог нормативно-правових документів [1-4] показало, що використання технологій дистанційного начання може відбуватись під час проведення окремих занять, вивчення окремих навчальних дисциплін (тем) або блоків дисциплін і поєднувати традиційні та інтерактивні технології за змішаною формою.

Основними перевагами застосування курсів дистанційного навчання є можливість їх необмеженого використання та вільного доступу у будь-який час. Дистанційне навчання є інтерактивною формою, організація якого передбачає зміну підходів до курсанта як майбутнього військового фахівця не з позиції об'єкта навчання, а з позиції суб'єкта навчання [9, с. 205]. Така технологія навчального процесу передбачає перетворення суб'єкта навчання з пасивного учасника та його активне залучення до процесу навчання, до самостійного засвоєння ним нового матеріалу.

Особливістю дистанційного навчання є взаємодія віддалених один від одного суб'єктів навчального процесу, яка відбувається у спеціалізованому середовищі, що функціонує на базі сучасних інноваційних психолого-педагогічних технологій та інформаційно-комунікаційних технологій.

Результати дослідження. Головною метою створення та впровадження технології дистанційного навчання є надання учасникам освітніх послуг за певними освітніми або

освітньо-кваліфікаційними рівнями відповідно до державних і галузевих стандартів освіти. Основними завданнями застосування технологій дистанційного навчання є:

- розширення можливостей доступу різних категорій учасників до якісного навчання за відповідними рівнями;
- забезпечення індивідуалізації навчального процесу у відповідності до потреб, особливостей і можливостей тих, хто навчається;
- підвищення якості та ефективності навчального процесу шляхом застосування інформаційно-комунікаційних й інноваційних освітніх технологій;
- забезпечення систематичного моніторингу якості освіти.

Вважаємо, що позитивними рисами дистанційної форми навчання є можливість опановувати навчальний матеріал в індивідуальному темпі, автономно від викладача, самостійно формуючи власну оцінку, враховуючи притаманний суб'єкту навчання природний темперамент і зручні способи сприйняття інформації. В контексті цього, на нашу думку, сильними сторонами дистанційного навчання у військовому навчальному закладі є виникнення у суб'єкта навчання позитивних емоцій, уникнення фактору порівняння себе з іншими та, як наслідок, зростання мотивації до навчання.

Організація дистанційного навчання вимагає від викладача оволодіння додатковими професійними якостями й розвитку в нього професійно важливих рис характера, які у загальному вигляді наведені на рис. 1.

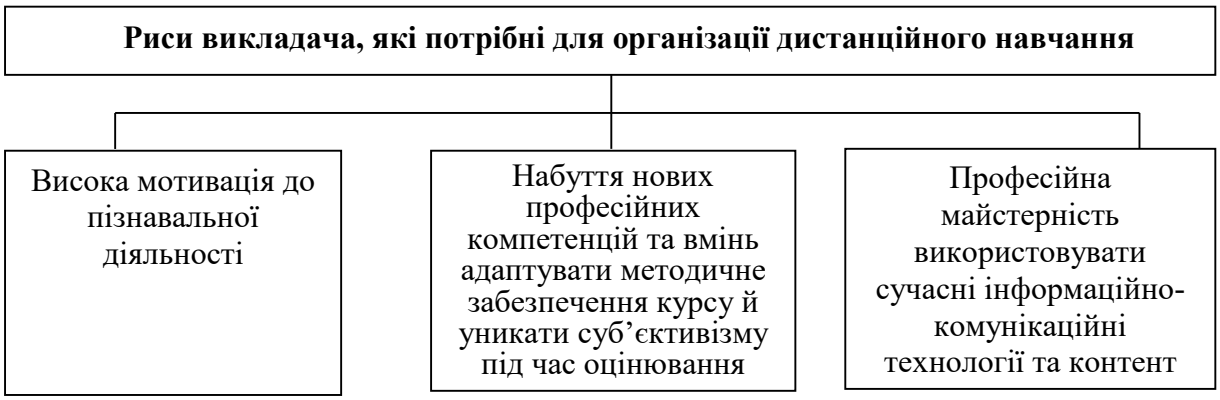

Рисунок 1 – Психолого-педагогічні особливості викладача, які потрібні для організації дистанційного навчання (розробка автора)

Розкриємо основні позитивні психолого-педагогічні аспекти впровадження дистанційного навчання в освітній процес ВНЗ, які на нашу думку передбачають:

- дисциплінованість, організованість і мотивованість до розвитку педагогічної майстерності та пізнавальної діяльності викладача;
- творчий підхід, системність та здатність розробляти навчальний курс і використовувати в освітньому процесі нові інформаційні технології;
- формування вмінь й навичок щодо використання інформаційно-комунікаційних технологій і сучасних програмних продуктів;
- здатність оперативно адаптувати до дистанційного формату методичне забезпечення навчальної дисципліни та вміння організувати процес навчання за змішаною формою;
- уникнення суб'єктивності з боку викладача та негативізму з боку суб'єкту навчання при оцінюванні рівня знань і формуванні загальної оцінки за курс;
- уникнення тиску на викладача та маніпулювання з боку суб'єкту навчання.

Враховуючи динамічний процес розвитку системи вищої освіти, широку доступність інформаційних ресурсів і засобів (програмне забезпечення, соціальні мережі Інтернет, гаджети та ін.), змінювання підходів до самостійної підготовки та чималий рівень обізнаності й освідченості молоді, що навчається у вищих військових закладах освіти, застосування лише традиційних або дистанційних методів навчання є недостатнім.

Вважаємо, що інтеграція очної та дистанційної форм навчання у змішану – є сучасним і перспективним підходом до організації навчання у військовому навчальному закладі тому, що це дозволить використати багато цікавих для молоді інтерактивних, наочних засобів представлення навчального матеріала, оперативно оновлювати інформацію та активізувати процес пізнання. Оптимальним варіантом автоматизованого створення курсів, тестів, системи опитування та контролю в умовах змішаного навчання є різноманітний контент (об'єктно-орієнтовані програмні оболонки та платформи для проведення онлайн-занять). У системі вищої освіти здебільшого використовують платформу Moodle, яка є підґрунтям створення курсів дистанційного навчання. Доступ до платформи Moodle зазвичай є вільним. Розробка дистанційного навчального курсу вимагає чималих витрат часу на етапі його створення, а також відповідного рівня володіння викладачем педагогічними, методичними та креативними знаннями і вміннями, а також спеціальними навичками користування комп'ютером. Враховуючи це, використання такого курсу у подальшому дозволить суттєво скоротити трудовитрати викладача на організацію методичної роботи та проведення навчальних занять.

Витрати на створення традиційного та дистанційного курсів за сукупністю критеріїв розглянуто у праці [5, с. 41-46], де науковцями С.В. Лєнковим, С.В. Гаховичем, Ю.О. Гунченко та ін. вдало підкреслюється цінність фахівця, який здійснив профільну підготовку.

Дійсно, кадрові питання у системі військової освіти та формування належного рівня людського потенціалу є важливими завданнями, розв'язання яких неможливо без належної організації дистанційного курсу з одного боку та можливості отримання якісної освіти очно та, у разі потреби, на відстані. Розв'язання цих завдань можуть забезпечити курси підвищення кваліфікації та професійного рівня науково-педагогічних працівників для вищих військових навчальних закладів. Це особливо актуально останнім часом, коли наша країна, як й інші, опинилась під впливом низки світових негативних факторів. Як вже зазначалось, це екстремальні й інші фактори, які призвели до поглиблення кризи економічної системи та до зниження рівня інтелектуального потенціалу за рахунок систематичного зменшення загальної чисельності населення країни, особливо її працездатної складової.

Загальні принципи й вимоги до організації змішаного навчання розкриті у монографії [10], однак особливості його практичного застосування з врахуванням специфіки військового навчального закладу в сучасних реаліях вимагають уточнення.

Вважаємо, що організація змішаного навчання вимагає крім високої мотивації викладача до пізнавальної діяльності, набуття ним нових професійних компетенцій та професійної майстерності використовувати сучасні інформаційно-комунікаційні технології також додатково оволодіння професійними якостями й наявності в нього особистих важливих рис характера (рис. 2). Так, креативність у XXI столітті є головною якістю викладача. Креативність (англ. create – створювати, creative – творчий) – це здатність створювати нове з того що вже є, це гнучкість та оригінальність, вміння додати до існуючого курсу цікаві деталі, зробити його різноманітним.

Рисунок 2 – Психолого-педагогічні особливості викладача, які потрібні для організації змішаного навчання (розробка автора)

Креативне мислення викладача під час створення курсу дозволить реалізувати творчий задум і професійно використати цікаві інтерактивні методики навчання, які здатні допомогти суб'єкту навчання знайти шляхи до саморозвитку та до самореалізації тощо.

Розвиток системи вищої військової освіти пов'язано саме з дистанційним навчанням як пріоритетної технології, що базується на системі управління навчальним контентом Moodle шляхом створення інтерактивного середовища. Практичні пропозиції щодо створення інтерактивного середовища наведено на прикладі провідного військового навчального закладу. Специфіка навчання у вищому військовому навчальному закладі, наприклад, у ВІКНУ імені Тараса Шевченка, полягає в тому, що крім основних навчальних занять в аудиторії, курсанти зазвичай залучаються до планованих військово-професійних заходів, передбачених військовими статутами. У цих випадках вони вимушені пропускати навчальні заняття з поважних причин, до переліку яких також належать хвороби, карантинні заходи та/або сімейні обставини.

Змішана форма навчання дає змогу оптимально поєднати формат очного та дистанційного навчання під час аудиторних занять і самостійної підготовки. Належна організація цієї форми навчання надасть можливість суб'єкту навчання у вільний час дистанційно опрацьовувати пропущений навчальний матеріал, отримати у разі необхідності пояснення викладачем окремих складних питань, а також уникнути «прогалин» у разі пропуску навчального матеріалу та ін.

Змішане навчання доцільно організувати у зручному форматі, коли навчальний процес здійснюється на рівні денного з можливостями поєднання он-лайн навчання, традиційного навчання та самостійної підготовки. Це передбачає отримання в разі необхідності консультацію викладача; спілкування курсантів між собою протягом усього періоду навчання; проведення обговорень, проміжного і підсумкового тестів; виконання спільних завдань, у тому числі дослідницького і творчого характеру тощо.

Дистанційне навчання як форма навчального процесу сприятиме:

- активізації пізнавальної діяльності кожного курсанта;
- забезпеченню ефективного зворотного зв'язку, інтерактивності;
- індивідуалізації і диференціації процесу навчання;
- прозорості у формуванні поточної та підсумкової оцінки;
- формуванню стійкої мотивації до навчально-пізнавальної діяльності.

Необхідно підкреслити, що організація дистанційного навчання вимагає значних початкових витрат на обладнання навчальних аудиторій для проведення занять та самопідготовки курсантів. Це, зокрема, потребує забезпечення навчальних аудиторій мережею Internet, комп'ютерною технікою, гаджетами, навушниками з мікрофонами, веб-камерами та ін. для проведення навчальних занять у форматі відеоконференцій тощо.

Як, приклад, задля підвищення якості сучасної військової освіти курсантів рівня бакалавр ВІКНУ імені Тараса Шевченка упродовж останніх трьох років на кафедрі фінансового забезпечення військ було розроблено адаптовані до дистанційного навчання методики викладання економічної статистики та успішно запроваджено їх у 2019 році до навчального процесу у форматі навчального посібника «Статистика для економістів» [11]. Враховуючи досвід викладання циклу дисциплін економічного напряму у ВІКНУ імені Тараса Шевченка задля створення в майбутньому оптимальних умов пізнавальної діяльності суб'єктів навчання та реалізації концепції освіти протягом усього життя доцільним є подальше розроблення цього навчального курсу засобами дистанційного навчання у формі електронного курсу. Використання електронного навчального курсу сприятиме усуненню «білих плям» у знаннях курсантів, надасть можливість поглибити рівень знань й одержати професійну допомогу викладача з метою формування навичок та вмінь, а також вчасного відпрацювання пропущених занять.

Загалом, організація навчального процесу з використанням засобів дистанційного навчання та форми змішаного навчання у вищому військовому навчальному закладі

сприятиме активізації розумової діяльності суб'єкта навчання, дозволить оптимізувати загальні витрати на підготовку та навчання майбутніх військових фахівців протягом усього життя.

Висновки. Отже, можна стверджувати, що особливістю організації дистанційного навчання в системі військової освіти є застосування суб'єктно-діяльнісного підходу та змішаної форми навчання. Процес організації дистанційного навчання пов'язаний з уміннями використовувати інформаційно-комунікаційні технології, психолого-педагогічними особливостями викладача та специфікою військового навчального закладу.

Розкрито позитивні аспекти впровадження технології дистанційного навчання з позиції викладача та з позиції суб'єкта навчання, загальними з яких є підвищення мотивації до пізнавальної діяльності курсантів і викладачів; можливість само формування як спеціальних компетенцій, так і розвитку «м'яких» навичок; можливість вибору зручного формату та методу навчання й формування критичного мислення; спроможність уникати негативного тиску і маніпулювання з боку суб'єкту навчання під час формування загальної оцінки за курс та ін.

Здійснено спробу визначити основні психолого-педагогічні риси викладача, які є важливими для успішного впровадження технології дистанційного навчання. Це – зростання мотивації до пізнавальної діяльності, набуття нових професійних вмінь, можливість уникнути суб'єктивізму під час оцінювання.

Організація змішаного навчання дозволяє створити відповідне середовище, де можна вдало поєднати виконання військових обов'язків під час навчання у військовому навчальному закладі з можливістю самостійної підготовки до аудиторних занять та належного опрацювання навчального матеріалу у зручний час.

Майбутній розвиток системи вищої військової освіти пов'язаний саме з дистанційним навчанням. Це перспективна й сучасна форма організації навчального процесу з використанням відповідних технологій на базі системи управління навчальним контентом Moodle в контексті якісного набуття вищої військово-професійної освіти.

ЛІТЕРАТУРА:

1. Закон України «Про вищу освіту» від 01.07.2014 р. № 1556-VII (зі змінами та доповненнями) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1556-18 – назва з титул. екрана.

2. Указ Президента України «Про Національну стратегію розвитку освіти в Україні на період до 2021 року» від 25.06.2013 р. № 344/2013 (зі змінами та доповненнями) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/344/2013 – назва з титул. екрана.

3. Наказ Міністерства освіти і науки України «Про затвердження Положення про дистанційне навчання» від 25.04.2013 р. № 466 (зі змінами та доповненнями) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0703-13 – назва з титул. екрана.

4. Наказ Міністерства оборони України «Про затвердження Концепції дистанційного навчання у Збройних Силах України» від 21.12.2015 р. № 744 (зі змінами та доповненнями) [Електронний ресурс] – Режим доступу: http://www.viti.edu.ua/files/npb/dfn3.pdf – назва з титул. екрана.

5. Стратегічний оборонний бюлетень України : Указ Президента України від 06.06.2016 р. № 240/2016 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/240/2016#n10 – назва з титул. екрана.

6. Побудова та використання систем дистанційного навчання з елементами штучного інтелекту : монографія / [С.В. Лєнков, С.В. Гахович, Ю.О. Гунченко та ін.]. – Одеса, Вид-во ВМВ, 2013. – 324 с.

7. Автоматизовані навчальні системи з елементами штучного інтелекту для вивчення технічних дисциплін : монографія / [К.Ф. Боряк, Ю.О. Гунченко, С.В. Лєнков та ін.]. – Одеса, Вид-во ВМВ, 2012. – 296 с.

8. Гунченко Ю.О. Модель функціонування адаптивної тренажерної системи для підготовки фахівців спецпідрозділів / Ю.О. Гунченко, С.В. Лєнков // Інформатика та математичні методи в моделюванні. – Одеса, 2011. – № 3. – С. 260-265.

9. Городянська Л.В. Суб'єктно-діяльнісний підхід в організації підготовки військових фахівців у системі вищої освіти / Л.В. Городянська, А.І. Сизов : тези доповідей Всеукраїнської науково-

практичної конференції молодих вчених, ад'юнтів, слухачів, курсантів і студентів «Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка» (м. Київ, 24.04.2020р.) [Текст]. – К.: ВІКНУ, 2020. – С. 204-206.

10. Теорія та практика змішаного навчання : монографія / [В.М. Кухаренко, С.М. Березенська, К.Л. Бугайчук та ін.]; за ред. В.М. Кухаренка – Х.:«Міськдрук», НТУ «ХПІ», 2016. –284 с.

11. Городянська Л.В. Статистика для економістів: навч. посіб. / Л.В. Городянська, А.І. Сизов. – К.: [Київ. нац. ун-т ім. Т.Шевченка], 2019. – 350 с.

REFERENCES:

1. Pro vyshchu osvitu: Zakon Ukrainy № 1556-VII. (2014, July 01). URL: https://zakon.rada.gov.ua/laws/show/1556-18 [in Ukrainian].

2. Pro Natsionalnu stratehiiu rozvytku osvity v Ukraini na period do 2021 roku: Ukaz Prezydenta Ukrainy № 344/2013. (2013, June 25). URL: https://zakon.rada.gov.ua/laws/show/344/2013 [in Ukrainian].

3. Pro zatverdzhennia Polozhennia pro dystantsiine navchannia: Nakaz Ministerstva osvity i nauky Ukrainy № 466. (2013, April 25). URL: https://zakon.rada.gov.ua/laws/show/z0703-13 [in Ukrainian].

4. Pro zatverdzhennia Kontseptsii dystantsiinoho navchannia u Zbroinykh Sylakh Ukrainy: Nakaz Ministerstva oborony Ukrainy № 744. (2015, December 21). URL: http://www.viti.edu.ua/files/npb/dfn3.pdf [in Ukrainian].

5. Strategichnyj oboronnyj bjuleten' Ukrai'ny: Ukaz Prezydenta Ukrai'ny № 240/2016. (2016, June 06) URL: https://zakon.rada.gov.ua/laws/show/240/2016#n10 [in Ukrainian].

6. Ljenkov, S.V., Gahovych, S.V., Gunchenko, Ju.O. et al. (2013) *Pobudova ta vykorystannja system dystancijnogo navchannja z elementamy shtuchnogo intelektu*. Odesa: VMV [in Ukrainian].

7. Borjak, K.F., Gunchenko, Ju.O. Ljenkov S.V. et al. (2012) *Avtomatyzovani navchal'ni systemy z elementamy shtuchnogo intelektu dlja vyvchennja tehnichnyh dyscyplin*. Odesa: VMV [in Ukrainian].

8. Gunchenko, Ju.O. Ljenkov, S.V. (2011) Model' funkcionuvannja adaptyvnoi' trenazhernoi' systemy dlja pidgotovky fahivciv specpidrozdiliv. *Informatyka ta matematychni metody v modeljuvanni*, 3, 260-265 [in Ukrainian].

9. Gorodianska, L.V., & Syzov, A. I. (2020). Sub'jektno-dijal'nisnyj pidhod v organizacii' pidgotovky vijs'kovyh fahivciv u systemi vyshhoi' osvity. *Molodizhna vijs'kova nauka u Kyi'vs'komu nacional'nomu universyteti imeni Tarasa Shevchenka:* Abstracts of Papers *(pp. 204-206).* Kyiv: VIKNU [in Ukrainian].

10. Kuharenko, V.M., Berezens'ka, S.M., Bugajchuk, K.L. et al. (2016) *Teorija ta praktyka zmishanogo navchannja.* HARKIV: «Mis'kdruk», NTU «HPI» [in Ukrainian].

11. Gorodianska, L. V., & Syzov, A. I. (2019) *Statystyka dlia ekonomistiv.* Kyiv: Kyivskyi natsionalnyi universytet imeni Tarasa Shevchenka [in Ukrainian].

к.е.н., доц. Городянська Л.В.

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО НАВЧАННЯ У СИСТЕМІ ВИЩОЇ ВІЙСЬКОВОЇ ОСВІТИ

У статті визначено, що підґрунтям забезпечення дистанційного навчання у системі військової освіти є суб'єктно-діяльнісний підхід. Узагальнено позитивні аспекти застосування технології дистанційного навчання з позиції викладача та з позиції суб'єкта навчання. Процеси організації й впровадження дистанційного навчання обумовлені специфікою військового навчального закладу та залежать від психолого-педагогічних особливостей викладача, його професійної майстерності використовувати сучасні інтерактивні методики навчання й інформаційно-комунікаційні технології. Здійснено спробу визначити основні психолого-педагогічні риси викладача, які потрібні в процесі організації дистанційного навчання. Це – висока мотивація до пізнавальної діяльності, набуття нових професійних компетенцій, вміння уникати суб'єктивізму під час оцінювання. Застосування дистанційного навчання дозволяє суттєво знизити витрати на навчання, активізувати процес пізнання завдяки різноманітним наочним засобам представлення нової навчальної інформації з використанням сучасних інформаційних технологій.

Доведено, що перспективним напрямом навчання у системі вищої військової освіти є змішане навчання. Це інтерактивна форма, яка дозволяє оптимально поєднати формат очного й дистанційного навчання. Організація змішаного навчання дає змогу створити відповідне середовище для успішного виконання військових обов'язків під час навчання у військовому закладі,

самостійної підготовки до аудиторних занять і самостійного опрацювання навчального матеріалу у зручний час. Застосування такої форми навчання сприятиме активізації пізнавальної діяльності, розширенню можливостей набуття як професійних компетенцій, так і «м'яких» навичок, які є підґрунтям виховання та гармонійного розвитку особистості у системі військової освіти.

Розвиток системи вищої військової освіти пов'язано саме з дистанційним навчанням як пріоритетної технології, що базується на системі управління навчальним контентом Moodle. Належна організація навчання дозволяє створити умови для підвищення мотивації суб'єкта навчання до розумової діяльності й до набуття якісної військово-професійної освіти.

Ключові слова: суб'єктно-діяльнісний підхід, дистанційне навчання, інформаційно-комунікаційні технології, змішане навчання, суб'єкт навчання, система вищої військової освіти.

Ph.D. Gorodyanska L.V.

FEATURES OF THE ORGANIZATION OF REMOTE TRAINING IN THE SYSTEM OF HIGHER MILITARY EDUCATION

The article determines that the basis for providing distance learning in the military education system is the subject-activity approach. The positive aspects of the application of distance learning technology from the perspective of a teacher and from the perspective of a learning subject are summarized. The processes of organization and implementation of distance learning are determined by the specifics of a military educational institution and depend on the psychological and pedagogical characteristics of the teacher, his professional skills to use modern interactive teaching methods and information and communication technologies. An attempt was made to determine the main psychological and pedagogical features of the teacher, which are needed in the process of organizing distance learning. This is a high motivation for cognitive activity, the acquisition of new professional competencies, the ability to avoid subjectivity during assessment. The use of distance learning can significantly reduce the cost of training, to intensify the process of learning thanks to a variety of visual means of presenting new educational information using modern information technologies.

It is proved that a promising direction of training in the system of higher military education is blended learning. This is an interactive form that optimally combines the format of full-time and distance learning. The organization of blended learning makes it possible to create an appropriate environment for the successful fulfillment of military duties while studying at a military educational institution, self-preparation for classroom studies and self-assimilation of training material at a convenient time. The use of this form of training will contribute to enhancing cognitive activity, expanding the possibilities of forming both professional competencies and "soft" skills, which are the basis for the upbringing and harmonious development of the individual in the military education system.

The development of the military higher education system is connected specifically with distance learning as a priority technology based on the Moodle educational content management system. The proper organization of training allows you to create the conditions for increasing the motivation of the subject of training to mental activity and to obtain high-quality military-vocational education.

Keywords: subject-activity approach, distance learning, information and communication technologies, blended learning, subject of training, higher military education system.

УДК 629.734.7

к.військ.н. **Думенко М.П.** (ГШ ЗСУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-15

ПОРЯДОК ПРАКТИЧНОГО ВИКОРИСТАННЯ КОМПЛЕКСНОЇ МЕТОДИКИ ОЦІНЮВАННЯ СИСТЕМИ КАДРОВИХ ОРГАНІВ ЗБРОЙНИХ СИЛ УКРАЇНИ ОРГАНАМИ ВІЙСЬКОВОГО УПРАВЛІННЯ

У статті розглядається методичні підходи до практичного використання методики комплексного оцінювання ефективності функціонування системи кадровик органів Збройних Сил України на прогнозованому періоді забезпечення боєздатності військ за показником персонал.

Надається порядок формування вихідних даних, врахування позитивних і негативних факторів комплектування Збройних Сил України персоналом і оцінювання ефективності у цьому процесі функціонування системи кадрових органів.

Надають практичні приклади використання розробленого методичного підходу для отримання значень показників ефективності у функціонування системи кадрових органів за різними варіантами формування пропозицій до прийняття рішень на комплектування частин і підрозділів обраного умовного військового формування.

Новизною обраного підходу є оцінювання функціонування системи кадрових органів за кінцевим вкладом в боєздатність органів управління, частин і підрозділів ЗС України на оцінюваному періоді за показником укомплектованості персоналу.

Розроблений методичний підхід до використання розробленої методики оцінювання функціонування системи кадрових органів дозволяє його використовувати у практичній діяльності органів військового управління для оцінювання варіантів структур і змісту функціонування системи кадрових органів.

Ключові слова: система кадрових органів, система комплектування збройних сил, персонал, комплексне оцінювання ефективності, комплектування військ

Постановка проблеми: потреба в оцінюванні ефективності функціонування системи кадрових органів Збройних Сил України (ЗС України) існує у практичній діяльності органів військового управління безперервно. Разом з цим методики і методичні підходи до використання існуючих методів оцінюванні ефективності функціонування системи кадрових органів (СКО) ЗС України, у теперішній час знаходяться у процесі розробки і вдосконалення.

Вклад в ефективність функціонування СКО ЗС України вносять складові кадрових органів (КО) в усіх рівнях від Головного управління персоналу Генерального штабу Збройних Сил України (ЗС України) до відділень і окремих посад з кадрової роботи.

Система кадрових органів ЗС України забезпечує прогнозування чисельних і якісних показників укомплектованості окремих підрозділів, військових формувань, органів військового управління і ЗС України у цілому для формування управлінських рішень органами військового і державного управління на підтримання боєздатності військових формувань у потрібний (загрозливий) період і у мирний час. Це робить необхідним адекватно оцінювати ефективність СКО на усіх етапах відпрацювання управлінських рішень на комплектування ЗС України, що у свою чергу потребує не тільки розробки науково-методичного апарату, а і методичних підходів до його використання у практичній діяльності органами військового управління.

У роботі [1] розроблений науково-методичний апарат оцінювання ефективності функціонування кадрових органів ЗС України, наступним кроком стала робота з розробки методичних підходів до використання цього апарату у практичній роботі органів військового управління ЗС України, чим забезпечується практична оптимізація процесу функціонування СКО і покращення результатів укомплектованості військ персоналом у потрібний час вирішення ними покладених завдань.

Аналіз останніх досліджень і публікацій. Досвід практичного виконання вимог законодавчих і нормативних актів України, що регламентують проходження військової

служби громадянами України [2-4], що накопичений у Головному управлінні персоналу ЗС України виявив необхідність вдосконалення науково-методичних підходів щодо використання накопичених наукових результатів оцінювання функціонування СКО ЗС України у практичній діяльності органів військового управління.

У результаті практичного апробування були використані наукові здобутки відомих авторів, що досліджували теорію кадрового менеджменту у ЗС України, таких як І.О. Романенко [5], В.М. Артюх, І.С. Романченко, Ю.А. Гусак [6], О.В. Яцино [7], М.П. Думенко [8], управління кар'єрою персоналу [9], проблемних питань відтоку персоналу з збройних сил [10].

При використанні результатів розробки вказаних науково-методичних підходів оцінювання СКО у практичній роботі Головного управління персоналу ЗС України отримані оцінки функціонування СКО, які дозволяли проводити детальний аналіз ефективності функціонування більшості відокремлених складових СКО, без врахування їх впливу на кінцевий результат функціонування СКО у цілому, при наявності достатнього часу на аналіз і обробку результатів оцінювання. Були отримані оцінки, що дозволяли сформувати пропозиції вдосконалення окремих важливих елементів комплектування та збереження персоналу, що вказані у працях [11], але залежність цих умов від ефективності функціонування СКО у цілому підтверджено не було.

У роботі використовувались результати вказаних наукових досліджень та результати, що отримані автором в ході практичного використання цих підходів для вдосконалення організаційної структури і змісту роботи СКО ЗС України в період останніх п'яти років.

Тому у статті розглянуте актуальне питання розробки методичного апарату для практичного використання науково-методичного апарату [1] комплексного оцінювання ефективності функціонування СКО ЗС України.

Мета статті. Подання результатів розробки методичних підходів до практичного використання розроблених методичних підходів до комплексного оцінювання ефективності функціонування СКО ЗС України.

Виклад основного матеріалу. Для практичного комплексного оцінювання ефективності функціонування СКО ЗС України в органах військового управління використовувались методичні підходи, що отримані автором у роботах з розробки комплексної методики оцінювання ефективності функціонування СКО ЗС України [12, 13] та інших працях, що присвячені прогнозуванню комплектування ЗС України персоналом.

Для оцінювання обрана система показників, що визначена у керівних документах [14], що використовують органи військового управління (ОВУ) у практичній діяльності з організації роботи із забезпечення персоналом ЗС України.

У проведених практичних дослідженнях оцінювання ефективності функціонування СКО використовувались групи показників оцінювання реалізації військової кадрової політики на яку впливає СКО шляхами залучення персоналу на військову службу, забезпечення ефективного кадрового менеджменту і оптимізацією підготовки кадрів.

За напрямком залучення персоналу на військову службу розглядались показники: загальний рівень укомплектування Збройних Сил професійним особовим складом відповідно до визначеної потреби військ (сил), збільшення (підтримання) рівня укомплектування бойових військових частин військовослужбовцями військової служби за контрактом, рівень укомплектування військовослужбовцями за контрактом, співвідношення категорій особового складу відповідно до їх структури та штатної чисельності та інші.

Оцінювання СКО за напрямком кадрового менеджменту здійснювалось за рівнем укомплектування бойових військових частин військовослужбовцями військової служби за контрактом, загальним рівнем нормативно-правових, програмних та керівних документів з питань комплектування Збройних Сил, загальним рівнем охоплення посад за якими здійснюється управління кар'єрою військовослужбовців, рівнем удосконалення планування кадрових ресурсів та іншими.

Оцінювання функціонування СКО за напрямком підготовки кадрів здійснювалось за загальним рівнями охоплення посад за якими здійснюється управління кар'єрним зростанням протягом всієї служби та підтримання високої бойової готовності військ (сил), розміщення випускників ВВНЗ (НЗ) згідно обсягів державного замовлення, підготовленого резерву громадян України за програмою підготовки офіцерів запасу та іншими.

Система кадрових органів розглянута у складі системи комплектування персоналом (СКП) ЗС України і оцінювалась за її вкладом у результат її функціонування. Метою оцінювання ефективності функціонування СКО є визначення шляхів забезпечення бойової готовності органів військового управління, військових частин, підрозділів ЗС України за складовою укомплектованості і підготовки персоналу у визначений період виконання завдань за призначенням.

При прогнозуванні укомплектованості ЗС України і ефективності СКО у прогнозованих умовах комплектування органам військового управління необхідно враховувати у першу чергу наступні негативні фактори:

змінність національних інтересів та політики держави у сфері національної безпеки і оборони, державної кадрової політики у військовій сфері, внутрішньополітичної діяльності органів державної влади з питань розвитку ЗС України;

значні економічні обмеження у розвитку ЗС України;

недосконаліть соціальних гарантій для військовослужбовців;

ускладнення демографічної ситуації у майбутньому;

значне звільнення і значна ротація військовослужбовців;

недосконалі управлінські рішення щодо управління кар'єрним ростом персоналу.

Для прогнозування можливостей поповнення ЗС України підготовленим персоналом повинні бути розглянуті усі джерела поповнення і їх можливості, а саме – це призов підготовленого персоналу з складу резерву і військовозобов'язаних, у тому числі і цивільних, з їх подальшою підготовкою у навчальних закладах і навчальних підрозділах, а також перерозподілу осіб персоналу в межах ЗС України.

Для визначення ефективності функціонування СКО у комплектуванні ЗС України підготовленим персоналом необхідно використовувати результати оцінювання долі впливу КО на загальний результат функціонування СКП.

Основним критерієм оцінювання СКП є перевищення значення (К) співвідношення чисельності підготовленого персоналу (S) до штатної чисельності військового часу H_m ОВУ, військових частин і підрозділів, з урахуванням військових-облікових спеціальностей і відмінностей у штатах різних індексів. Особливості комплектування ОВУ, військових частин і підрозділів враховуються у встановлених нормах їх укомплектованості (нормативних документах) (К). К – нормативно встановлене значення співвідношення укомплектованості (встановлюється у відсотках) для окремої m-ї структурної одиниці (військового формування підрозділу). Результат укомплектованості K_m оцінюється за наступним виразом

$$K_m = \frac{S_m}{H_m} \times 100\%,$$

де S_m – чисельність особового складу за списком (при наявності обмежень на укомплектованість за спеціальностями визначається окремо для спеціальностей, які визначають бойову готовність, здатність);

H_m – кількість посад за штатом (при наявності обмежень на укомплектованість за спеціальностями визначається окремо для спеціальностей, які визначають бойову готовність, здатність);

m – індекс структурної одиниці.

Структурні одиниці m пропонується визначати при проведенні оцінювання наступним чином:

1 – органи військового управління (ОВУ), 1.1 – ОВУ1, 1.2 – ОВУ2 … 1. n – ОВУn;

2 – військові частини (в/ч), 2.1 – в/ч 1, 2.3 – в/ч 2, …, 2.k – в/ч k.

3 – підрозділи, 3.1 – підрозділ 1, 3.2 – підрозділ 2, …, 3.l – підрозділ l,

й інші;

n, k і l – кількість структурних одиниць у групі.

Рівень укомплектованості K_m оцінюється окремо у поточний час $t_{пот}$ і плановому періоді (періодах) застосування ЗС України ($T_{пл}$).

Період оцінювання обраний 5 років, за який забезпечується підготовка офіцерів у ВВНЗ, і який є найбільш тривалим з періодів підготовки військових фахівців. Дискретність проведення оцінювань обрано один раз на півроку $\Delta T_{оцін}$ =(0; 0,5; 1; 1,5; 2; 2,5; 3; 3,5; 4; 4,5; 5).

СКП має забезпечувати підтримання K_m на рівні не менше ніж заданий на протязі усього періоду оцінювання.

СКО впливає на укомплектованість персоналом ЗС України через виконання покладених на них функцій, які визначаються у [14, 15].

Критерієм позитивного оцінювання діяльності КО на відповідному рівні їх функціонування є забезпечення боєздатності військових формувань за складовою персонал, а у випадку їх небоєздатності, їх чисельність персоналу не зараховується C_m до позитивної оцінки укомплектованості ОВУ, військових частин і підрозділів. Тому для загального оцінювання ефективності СКО можливо використовувати узагальнений показник, який враховує негативні і позитивні результати комплектування персоналом. Вплив КО на результати комплектування персоналом органів військового управління і військових частин оцінюється через показники, що вказують на готовність органів управління (A_i), військових частин (A_n) (підрозділів) (A_m) до застосування, і вимірюється показниками їх готовності до виконання завдань за призначенням, що мають дискретні значення: 1 (готові) або 0 (не готові). Ці значення враховуються для визначення чисельності персоналу, що буде зарахована для позитивного або негативного оцінювання результату функціонування СКП.

Для вказаних показників і критеріїв оцінювання складових функціонування СКО використовується загальні показники оцінювання ефективності у поточний час ($t_{пот}$) і за період оцінювання ($T_{оцін.}$)

$$W_{m\, t_{пот}} = \frac{S_m - C_m}{H_m} .$$

Цей показник характеризує долю персоналу, що використовується за призначенням та його чисельність забезпечує боєздатність m-х структурних елементів (ОВУ, частин, підрозділів) за показником укомплектованості персоналом.

При проведенні оцінювання на певному періоді ($T_{оцін.}$) проводиться усереднення значення W_m у *i*-х періодах $\Delta T_{оцін}$ =(0; 0,5; 1; 1,5; 2; 2,5; 3; 3,5; 4; 4,5; 5) із визначенням значення показника на кожному інтервалі оцінювання.

$$W_{\Delta T оцін} \le \frac{\sum_{i=1}^{n} W_{i\ m}}{n} \cdot 100\% ,$$

i=1…n

n – кількість періодів оцінювання.

При сумарному оцінюванні такий підхід дозволить отримати значення відносних оцінок ефективності функціонування СКО за складовою персонал та оцінювати ефективність функціонування на рівнях комплектування від підрозділів до з'єднання (об'єднання) і виду Збройних Сил.

Загальним показником оцінювання ефективності функціонування СКО за усіма вище вказаними складовими є зважена сума значень вказаних показників за період застосування ЗС України ($T_{пл}$):

$$W_{\text{персонал}} = \frac{1}{n} \sum_{i=1}^{n} V_m W_m ,$$

де *n* – кількість використаних для оцінювання структурних одиниць, з m індексами, що описані вище.

Слід зазначити, що значення $W_{\text{персонал}}$ буде мати обмеження, з причини нормування його складових, а тому для порівняння варіантів СКО необхідно оцінювати отримане значення відносно його максимуму $W_{\text{персонал max}}$. Максимальні значення показників укомплектованості $W_{\text{персонал max}}$. визначаються експертним шляхом за досвідом функціонування СКО у три попередні періоди.

Нижче (у табл. 1) наведені результати практичних розрахунків значення показника ефективності функціонування СКО для обраного складу військ.

Таблиця 1

Розрахункові значення показників ефективності функціонування СКО за її складовими

	V_1	$W_у$	V_2	$W_{в/ч}$	V_3	$W_{підр}$	W/3
$W_{\text{персонал}}$	0,4	0,28	0,4	0,30	0,2	0,12	0,23
$W_{\text{персонал max}}$	0,4	0,38	0,4	0,38	0,2	0,19	0,32
$W_{\text{персонал}} / W_{\text{персонал max}}$	1	0,74	1	0,79	1	0,63	0,71

Значення $W_{\text{персонал}}$=0,71 вказує на те, що існуюча СКО використовує можливості на 71% від максимальних.

Значення коефіцієнтів V_m обираються за ступенем значущості вкладу ОВУ, військової частини або підрозділу у боєздатність вищого.

У роботі визначені наступні градації важливості щодо вкладу у боєздатність вищого військового формування:

визначає боєздатність;

впливає на боєздатність;

суттєво не впливає на боєздатність;

не впливає на боєздатність.

На початковому етапі вагові коефіцієнти V_m встановлюються метод експертних оцінок, але у подальшому уточняються методами статистики з урахуванням практично отриманих результатів (наприклад на навчаннях або за результатами бойового застосування військ). Сума V_m, що використовуються в оцінюванні має дорівнювати 1. Значення V_m приведені у табл. 2.

Таблиця 2

Значення V_m, що використовуються у роботі

№ з/п	Градації важливості коефіцієнтів V_m	V_m	
		Мирний час	Особливий період
1.	Визначає боєздатність	0,6	0,8
2.	Впливає на боєздатність	0,4	0,6
3.	Суттєво не впливає на боєздатність	0,2	0,4
4.	Не впливає на боєздатність	0	0,2

Критерій оцінювання ефективності функціонування СКО – це не зменшення (утримання) потрібного рівня чисельності боєздатних ОВУ, військових частин, підрозділів у видах, родах

і спеціальних військах ЗС України, за період застосування Збройних Сил.

Вказаний підхід дозволив отримати кількісні оцінки ефективності функціонування СКО для порівняння варіантів її структур і варіантів рішень на організацію функціонування СКО, що дозволяє керівникам кадрових органів вищого рівня приймати рішення на організацію функціонування СКО ЗС України.

Проведене імітаційне моделювання процесу комплектування персоналом ЗС України. Сформовані бази даних для їх окремого ведення і уточнення за усією номенклатурою військових формувань, категорій військових звань, спеціальностей і спеціалізацій. Експеримент проведений на прикладі чотирьох умовних бригад і їх підрозділів.

Для прогнозування зменшення і поповнення чисельності персоналу обрані лінійні закони, що корегуються по чотирьох контрольних періодах. Параметри законів зменшення чисельності персоналу встановлюються коефіцієнтами $К_{\Delta T03}$, $К_{\Delta T06}$, $К_{\Delta T09}$, $К_{\Delta T12}$ кожного підрозділу окремо, а поповнення чисельності персоналу $К_{призив\ \Delta T03(\Delta T06,\ \Delta T09,\ \Delta T12)}$, $К_{менедж\ \Delta T03(\Delta T06,\ \Delta T09\ \Delta T12)}$, $К_{підгот\ \Delta T03(\Delta T06,\ \Delta T09\ \Delta T12)}$ корегуються за результатом комплектування попередніх періодів.

Оцінювання ефективності функціонування СКО здійснюється за алгоритмом, що приведений на рис. 1.

1) Блок 1. В базу даних вносяться:

період прогнозування ефективності функціонування СКО;

періоди контролю ефективності функціонування СКО;

штатна чисельність ОВУ, військових частин, підрозділів за категоріями по різних індексах штатів (початкова);

спискова чисельність ОВУ, військових частин, підрозділів за категоріями (початкова);

норми (коефіцієнти) звільнення (переміщення) особового складу ОВУ, військових частин, підрозділів за категоріями по періодам ΔТ03, ΔТ06, ΔТ09, ΔТ12;

норми (коефіцієнти) поповнення особового складу у залежності від його некомплекту для ОВУ, військових частин, підрозділів за категоріями по періодам ΔТ03, ΔТ06, ΔТ09 (для врахування призиву, кадрового менеджменту, підготовки;

значення коефіцієнтів, що визначають боєздатність ОВУ, військових частин, підрозділів на показником укомплектованості підготовленим персоналом, які встановлюється для кожного окремо.

2) Блок 2. Обчислення прогнозованих значень укомплектованості ОВУ, частин і підрозділів.

Враховується, що комплектування ОВУ і підрозділів буде здійснюватися з урахуванням їх пріоритетів і наявних ресурсів. Ресурси розподіляються між ОВУ і підрозділами для забезпечення максимального забезпечення боєздатних ОВУ, частин і підрозділів по показнику укомплектованості підготовленим персоналом.

3) Блок 3. Обчислення значення комплексного показника ефективності функціонування СКО W_i вирази 4 і 5.

4) Блок 4. Зміна початкових даних списової чисельності, за якими введено категорії оцінювання комплектування.

5) Блок 5. Вибір варіанту функціонування СКО, фіксація чисельних значень вхідних та значень показників оцінювання ефективності функціонування СКО. Порівняння отриманих даних з тими, значеннями що володіє існуюча СКО.

6) Блок 6. Обирання структури і параметрів функціонування СКО для наступного періоду оцінювання.

Фіксація вхідних даних попереднього за період, для збільшення періоду планування (аналізу) укомплектованості частин і підрозділів ЗС України персоналом.

Для змінювання функції (залежності) комплектування персоналом передбачена можливість зміни законів комплектування і зменшення чисельності персоналу.

На прикладі комплектування персоналом чотирьох бригад, що різні за штатом, початковою списковою чисельністю, умовами їх комплектування, і критеріями укомплектованості отримані наступні результати.

У табл. 3 приведені результати розрахунків укомплектування офіцерським (керівним) складом управління і командного складу підрозділів чотирьох бригад, ефективність функціонування СКО складає W_1=0,71.

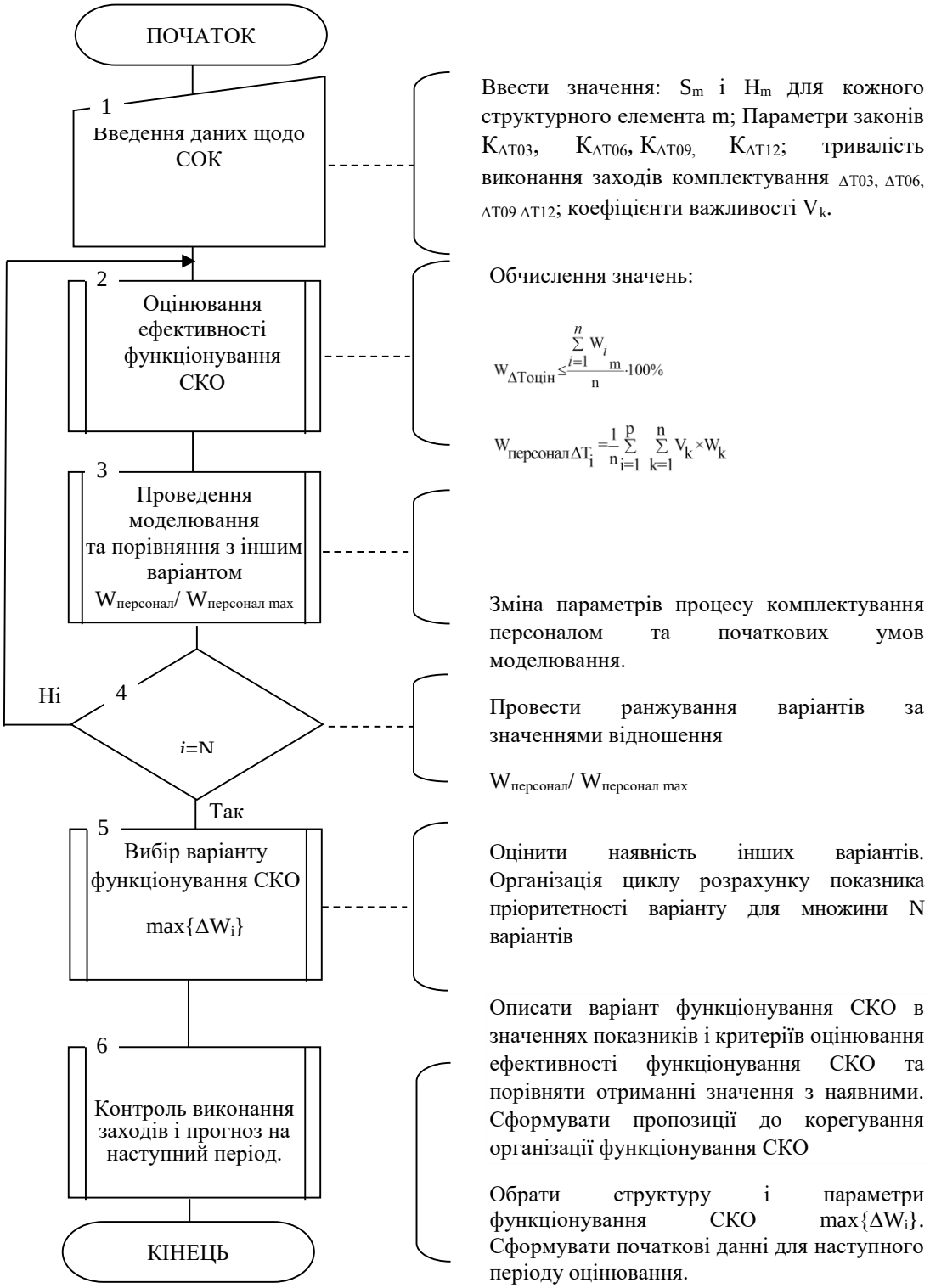

Рисунок 1 – Алгоритм моделювання процесу оцінювання функціонування СКО

Таблиця 3

Результати розрахунків укомплектування офіцерським (керівним) складом управління і командного складу бригад

Керівний (офіцерський склад)										
Середня укомплектованість 0,93, ефективність СКО за ΔT_1-ΔT_4 W_1=0,71										
Призив: К призив ΔТ			0,3	0,5	0,5	0,5				
			8	9	7	7				
Менеджмент: К менедж ΔТ			0,1	0,1	0,1	0,1				
			3	3	3	3				
Навчання К навчан. ΔТ			0,1	0,1	0,1	0,1		Зменшення чисельності персоналу		
			3	3	3	3				
Всього			**13**	**14**	**12**	**12**				
Штат		ΔТ01	ΔТ03	ΔТ06	ΔТ09	ΔТ12		0,02	0,04	0,01
1 бр	239	214	221	225	234	245		**5,4**	**9,94**	**3,52**
Укомплектовані			**220**	**222**	**230**	**221**		**ΔТ03**	**ΔТ06**	**ΔТ09**
Не розміщені			**1**	**3**	**4**	**25**	**0,71**			
У 1 бр	35	33	35	33	35	34	+	0	3	0
У11 бат	10	9	9	9	10	9	+	1	0	0
У12 бат	10	8	9	9	9	8	Небоєздатна	0	0	1
У13 бат	10	10	10	10	9	9	+	0	0	1
У14 бат	10	7	8	8	8	7	Небоєздатна	0	0	1
У 2 бр	30	29	28	29	31	30	+	3	0	0
У21 бат	9	8	8	8	9	8	+	0	1	0
У22 бат	9	7	7	8	8	7	Небоєздатна	0	0	1
У23 бат	9	6	6	7	7	7	Небоєздатна	0	0	0
У 3 бр	25	24	25	23	24	24	+	0	3	0
У31 бат	8	8	7	8	8	7	+	1	0	0
У32 бат	8	7	7	8	8	7	+	0	0	0
У33 бат	8	7	7	8	8	7	+	0	0	0
У 4 бр	34	29	31	30	31	32	Небоєздатна	0	3	0
У41 бат	8	8	7	8	8	7	+	1	0	0
У42 бат	8	7	7	8	8	7	+	0	0	0
У43 бат	8	7	7	8	8	7	+	0	0	0

Результати вказують на те, що на четвертому етапі комплектування не були використані резерви 25-х осіб, хоча кількість персоналу, що була надана системою комплектування була достатня. Початкові умови комплектування вимагали диференційованого підходу до звільнення персоналу і перерозподілу між бригадами і їх підрозділами.

Для подальшого оцінювання необхідно отримати прогнозовані значення максимальних показників комплектування і максимальні значення показника ефективності $W_{персонал\ max}$ та обчислити їх відношення $W_{персонал}$ / $W_{персонал\ max}$.

У табл. 4 приведені результати розрахунків укомплектування підрозділів бригад персоналом за і-ю спеціальність, що визначають боєздатність підрозділу (частини). Ефективність функціонування СКО складає W_2=0,75.

Таблиця 4

Результати розрахунків укомплектування підрозділів бригад персоналом за *i*-ю спеціальність

Посади, що визначають боєздатність (і-ї спеціальності)										
Середня укомплектованість – 0,81, ефективність СКО за ΔT_1-ΔT_4 W_2=0,75										
Призив К призив ΔТ			0,03	0,03	0,03	0,03				
			20	20	25	25				
Менеджмент К менедж ΔТ			0,1	0,1	0,1	0,1				
			68	68	68	68				
Навчання К навчан. ΔТ			0,1	0,1	0,1	0,1		Зменшення чисельності персоналу		
			68	68	68	68				
Всього			**156**	**156**	**161**	**161**				
Штат		ΔТ01	ΔТ03	ΔТ06	ΔТ09	ΔТ12		0,03	0,08	0,08
1 бр	**4268**	**3588**	3615	3419	3206	3367	0,81	**130**	**351**	**374**
Комплект			**3514**	**3245**	**3032**	**3137**				
Резерв			**101**	**174**	**174**	**231**	0,75	ΔТ03	ΔТ06	ΔТ09
1 бр	43	43	43	39	36	37	+	0	4	4
11	12	12	11	10	10	9	+	1	1	1
111 р	95	95	86	80	76	79	+	10	9	8
112 р	95	95	86	80	60	63	+	10	9	24
113 р	95	95	86	80	76	79	+	10	9	8
12	12	12	12	11	11	11	+	0	1	0
121 р	95	95	95	86	81	83	+	0	10	9
122 р	95	95	95	86	81	83	+	0	10	9
123 р	95	95	95	86	81	83	+	0	10	9
13	12	12	12	11	10	10	+	0	1	1
131 р	95	90	93	88	82	85	+	0	9	9
132 р	95	50	53	52	50	53	НБГ	0	5	5
133 р	95	50	53	52	50	53	НБГ	0	5	5
134 р	95	50	53	52	50	53	НБГ	0	5	5
14	2	2	2	2	2	1	+	0	0	0
141 р	12	12	11	10	10	9	+	1	1	1
142 р	12	12	11	10	10	9	+	1	1	1
143 р	12	12	11	10	10	9	+	1	1	1
2 бр	43	43	43	39	36	37	+	0	4	4
…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…

Результати вказують на те, що стратегія рівномірно-пропорційного комплектування підрозділів персоналом за і-ю спеціальність не дозволила відновити боєздатність 132, 134, 133 рот, але дозволила утримувати боєздатність інших, при досить щільному звільнення персоналу.

Початкові умови комплектування були сприятливими, але КО не обрали потрібних параметрів закону комплектування і не забезпечили диференційований підхід до використання резерву для його перерозподілу між бригадами і їх підрозділами.

Для подальшого оцінювання необхідно отримати прогнозовані значення максимальних показників комплектування і максимальні значення показника ефективності $W_{персонал\ max}$ та обчислити їх відношення $W_{персонал}$ / $W_{персонал\ max}$.

В роботі проведені оцінювання ефективності СКО за усіма спеціальностями і спеціалізаціями посад, що визначають боєздатність підрозділів бригад і бригад у цілому.

Результати вказують на те, що КО необхідно ретельно врахувати початкові умови комплектування.

У табл. 5 приведені результати розрахунків узагальненого показника ефективності функціонування СКО за чотири періоди за складовими укомплектування офіцерським складом і посадами, що визначають боєздатність частин і підрозділів, з урахуванням їх специфіки. Значення узагальненого показника ефективності функціонування СКО складає W=0,23. Для оцінювання відносної ефективності, як реалізації від максимальних можливостей СКО з комплектування, проведене умовне визначення максимальних значень показників укомплектованості усіх вище вказаних структурних елементів з таблиць 1-4, що дозволило отримати W_{max}=0,32. Значення W/ W_{max} приведене у табл. 5.

Таблиця 5

Результати розрахунків значення узагальненого показника ефективності функціонування СКО

Оцінювання значення узагальненого показника ефективності функціонування СКО за чотири періоди							
	K_1	W_1	K_2	W_2	K_3	W_3	W/3
W	0,4	0,28	0,4	0,30	0,2	0,12	0,23
W_{max}	0,4	0,38	0,4	0,38	0,2	0,19	0,32
W/ W_{max}	1	0,74	1	0,79	1	0,63	0,71

Значення W/W_{max} = 0,71 вказує на те, що СКО реалізовує власні можливості з урахуванням результатів функціонування зовнішньої системи комплектування за 71%.

Висновки. Розроблений методичний підхід до оцінювання ефективності функціонування СКО ґрунтується на методах системного аналізу, аналізу ієрархій, кваліметрії, статистики, аналізу і синтезу складних систем військового призначення і дозволяє оцінювати ступінь реалізації можливостей СКО з урахуванням результатів функціонування зовнішніх системи (комплектування, управління, забезпечення і інших) і внутрішніх підсистем і ресурсів СКО.

Розроблений математичний апарат дозволяє зручно його використовувати у практичній діяльності органів військового управління і кадрових органах для оцінювання ефективності системи кадрових органі при вирішенні завдань з комплектування персоналом військових формувань на різних етапах виконання завдань ЗС України та для різних початкових умов комплектування.

ЛІТЕРАТУРА:

1. Думенко М.П. Комплексне оцінювання ефективності функціонування системи кадрових органів) "Збірник наукових праць Національного університету оборони України "Труди Університету". 2020. №1 (156) С. 217-232.

2. "Про Збройні Сили України": Закон України від 06.12.91 № 1934-XII.

3. "Про військовий обов'язок і військову службу": Закон України від 04.04.06 № 3597-IV.

4. Про соціальний і правовий захист військовослужбовців та членів їх сімей": Закон України від 20.12.91 № 2012-XII.

5. Романенко І.О. Формалізація процесів координаційного управління системою підготовки військ (сил) / І.О. Романенко // Наука і техніка Повітряних Сил Збройних Сил України. – 2009. – № 1(1). – С. 3-6.

6. Артюх В.М., Романченко І.С., Гусак Ю.А. Забезпечення комплектування Збройних Сил України особовим складом: стан, проблеми та напрями удосконалення // Наука і оборона №1, 2010. – С.13-21.

7. Яцино О.В. Система кадрового забезпечення у Збройних Силах України: проблемні питання та напрямки їх вирішення / О.В. Яцино // Системи озброєння і військова техніка. – 2012. – № 4(32). – С. 200-205.

8. Думенко М.П. Роль і місце кадрової політики у Збройних Силах України. [Електрон. ресурс].– Режим доступу: www.ualogos.kiev.ua/fulltext.html?id=1917.

9. Pradeep Sofat Human Resource Management in the Armed Forces Monograph, 2016 – 203 p. Режим доступу: https://idsa.in/monograph/human-resource-management-in-the-armed-forces

10. Агенство Bloomberg. Article. US military can improve personnel practices. Режим доступу: https://www.bloomberg.com/opinion/articles/2018-10-19/u-s-military-can-improve-personnel-practices

11. Self-organization and management of social system / Ulrich H. ed./ Springer Sériés in Synergetics: Springer-Verlag, 1984. - P. 26.

12. Думенко М.П. Методологічні основи системи комплектування ЗС України в умовах гібридної війни (особливого періоду) Науковий журнал / "Сучасні інформаційні технологій в сфері безпеки та оборони". Національний університет оборони України, 2019. - №1 (34) С. 167-174.

13. Думенко М.П. Методичний підхід до оцінювання ефективності системи комплектування персоналом ЗС України в умовах гібридної війни (особливого періоду) Науковий журнал / "Сучасні інформаційні технологій в сфері безпеки та оборони". Національний університет оборони України, 2019. - №2 (35) С. 127-133.

14. "Положення про кадрові органи Збройних Сил України та Типових нормативів утримання кадрових органів військового управління, з'єднань, військових частин, установ, організацій", що затверджені наказом Міністра оборони України від 05.06.2009 № 301.

15. "Про затвердження Концепції військової кадрової політики у Збройних Силах України", наказ Міністра оборони України від 26.06.2017 №342 (План дій (дорожня карта) реалізації Концепції військової кадрової політики у Збройних Силах України на період до 2020 року, затверджений тимчасово виконуючим обов'язки Міністра оборони України від 06.11.2017 року).

REFERENCES:

1. Dumenko M.P. (2020). Kompleksne ocinjuvannja efektyvnosti funkcionuvannja systemy kadrovyh organiv) "*Zbirnyk naukovyh prac' Nacional'nogo universytetu oborony Ukrai'ny "Trudy Universytetu*". no. 1 (156), pp. 217-232.

2. "Pro Zbrojni Syly Ukrai'ny": Zakon Ukrai'ny vid 06.12.91 № 1934-HII.

3. "Pro vijs'kovyj obov'jazok i vijs'kovu sluzhbu": Zakon Ukrai'ny vid 04.04.06 № 3597-IV.

4. Pro social'nyj i pravovyj zahyst vijs'kovosluzhbovciv ta chleniv i'h simej": Zakon Ukrai'ny vid 20.12.91 № 2012-XII.

5. Romanenko I.O. (2009). Formalizacija procesiv koordynacijnogo upravlinnja systemoju pidgotovky vijs'k (syl). *Nauka i tehnika Povitrjanyh Syl Zbrojnyh Syl Ukrai'n*, no. 1(1), p. 3-6.

6. Artjuh V.M., Romanchenko I.S. and Gusak Ju.A. (2010). Zabezpechennja komplektuvannja Zbrojnyh Syl Ukrai'ny osobovym skladom: stan, problemy ta naprjamy. *Nauka i oborona,* №1, pp.13-21.

7. Jacyno O.V. (2012). Systema kadrovogo zabezpechennja u Zbrojnyh Sylah Ukrai'ny: problemni pytannja ta naprjamky i'h vyrishennja. *Systemy ozbrojennja i vijs'kova tehnika,* no. 4(32), pp. 200-205.

8. Dumenko M.P. Rol' i misce kadrovoi' polityky u Zbrojnyh Sylah Ukrai'ny. [Elektron. resurs].– Rezhym dostupu: www.ualogos.kiev.ua/fulltext.html?id=1917.

9. Pradeep Sofat Human Resource Management in the Armed Forces Monograph, 2016 – 203 p. Режим доступу: https://idsa.in/monograph/human-resource-management-in-the-armed-forces

10. Агенство Bloomberg. Article. US military can improve personnel practices. Режим доступу: https://www.bloomberg.com/opinion/articles/2018-10-19/u-s-military-can-improve-personnel-practices

11. Self-organization and management of social system / Ulrich H. ed./ Springer Sériés in Synergetics: Springer-Verlag, 1984. - P. 26.

12. Dumenko M.P. (2019). Metodologichni osnovy systemy komplektuvannja ZS Ukrai'ny v umovah gibrydnoi' vijny (osoblyvogo periodu). *Suchasni informacijni tehnologij v sferi bezpeky ta oborony*. Nacional'nyj universytet oborony Ukrai'ny, no.1 (34), pp. 167-174.

13. Dumenko M.P. (2019). Metodychnyj pidhid do ocinjuvannja efektyvnosti systemy komplektuvannja personalom ZS Ukrai'ny v umovah gibrydnoi' vijny (osoblyvogo periodu). *Suchasni informacijni tehnologij v sferi bezpeky ta oborony*. Nacional'nyj universytet oborony Ukrai'ny, no. 2 (35), pp. 127-133.

14. "Polozhennja pro kadrovi organy Zbrojnyh Syl Ukrai'ny ta Typovyh normatyviv utrymannja kadrovyh organiv vijs'kovogo upravlinnja, z'jednan', vijs'kovyh chastyn, ustanov, organizacij", shho zatverdzheni nakazom Ministra oborony Ukrai'ny vid 05.06.2009 № 301.

15. "Pro zatverdzhennja Koncepcii' vijs'kovoi' kadrovoi' polityky u Zbrojnyh Sylah Ukrai'ny", nakaz Ministra oborony Ukrai'ny vid 26.06.2017 №342 (Plan dij (dorozhnja karta) realizacii' Koncepcii' vijs'kovoi' kadrovoi' polityky u Zbrojnyh Sylah Ukrai'ny na period do 2020 roku, zatverdzhenyj tymchasovo vykonujuchym obov'jazky Ministra oborony Ukrai'ny vid 06.11.2017 roku).

к.воен.н. Думенко Н.П.

ПОРЯДОК ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ КОМПЛЕКСНОЙ МЕТОДИКИ ОЦЕНКИ СИСТЕМЫ КАДРОВЫХ ОРГАНОВ ВООРУЖЕННЫХ СИЛ УКРАИНЫ ОРГАНАМИ ВОЕННОГО УПРАВЛЕНИЯ

В статье рассматриваются методические подходы к практическому использованию методики комплексной оценки эффективности функционирования системы кадровых органов Вооруженных Сил Украины на прогнозируемом периоде обеспечения боеспособности войск по показателю персонал.

Предоставляется порядок формирования исходных данных, учета положительных и отрицательных факторов комплектования Вооруженных Сил Украины персоналом и оценки эффективности в этом процессе функционирования системы кадровых органов.

Предоставляются практические примеры использования разработанного методического подхода для получения значений показателей эффективности в функционировании системы кадровых органов по различным вариантам формирования предложений к принятию решений на комплектование частей и подразделений избранного условного военного формирования.

Новизной выбранного подхода является оценка функционирования системы кадровых органов по конечному вкладу в боеспособность органов управления, частей и подразделений ВС Украины на оцениваемом периоде по показателю укомплектованности персонала.

Разработанный методический подход к использованию разработанной методики оценки функционирования системы кадровых органов позволяет его использовать в практической деятельности органов военного управления для оценки вариантов структур и содержания функционирования системы кадровых органов.

Ключевые слова: система кадровых органов, система комплектования вооруженных сил, персонал, комплексная оценка эффективности, комплектование войск.

Ph.D. Dumenko M.P.

THE ORDER OF PRACTICAL USE OF THE COMPLEX METHODOLOGY OF EVALUATION OF THE SYSTEM OF HUMAN BODIES OF THE ARMED FORCES OF UKRAINE

The article discusses methodical approaches to the practical use of the methodology of complex evaluation of the effectiveness of the personnel system of the personnel of the Armed Forces of Ukraine in the forecast period of ensuring the combat readiness of the troops in terms of personnel.

The procedure for the formation of baseline data, taking into account the positive and negative factors of staffing of the Armed Forces of Ukraine with personnel and assessing the effectiveness of the system of personnel bodies in this process are given.

Practical examples of the use of the developed methodological approach for obtaining the values of efficiency indicators in the functioning of the system of personnel bodies under different variants of the formation of proposals before deciding on the manning of units and units of the selected conventional military formation are provided.

The novelty of the chosen approach is to evaluate the functioning of the system of personnel bodies by the final contribution to the combat capability of the governing bodies, units and divisions of the Armed Forces of Ukraine for the estimated period according to the staffing level.

The developed methodical approach to the use of the developed methodology for evaluating the functioning of the personnel system allows it to be used in the practical activity of the military management bodies for evaluating variants of the structures and the content of the functioning of the personnel bodies system.

Keywords: system of personnel bodies, system of manning of armed forces, personnel, complex evaluation of efficiency, manning of troops.

ДАНІ ПРО АВТОРІВ

Артемов Володимир Юрійович, доктор педагогічних наук, доцент, професор кафедри, Університет "КРОК", https://orcid.org/0000-0002-5290-4496.

Бабіч Оксана Миколаївна, кандидат технічних наук, старший науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка https://orcid.org/0000-0001-8363-8613.

Бойчук Вадим Олександрович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету.

Бурдюг Олег Володимирович, науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-3703-6550.

Бурмак Юлія Анатоліївна, викладач Київського коледжу зв'язку, https://orcid.org/0000-0002-8090-5058.

Гаценко Сергій Станіславович, кандидат технічних наук, заступник начальника кафедри розвідки Національного університету оборони України імені Івана Черняховського, https://orcid.org/0000-0002-0957-6458.

Глухова Анна Сергіївна, магістр міжнародного права Київського національного торгівельно-економічного університету https://orcid.org/0000-0001-8211-5386.

Городянська Лариса Володимирівна, кандидат економічних наук, доцент, доцент кафедри фінасового забезпечення військ Військового інституту Київського національного університету імені Тараса Шевченко, https://orcid.org/0000-0002-4482-1690.

Даков Сергій Юрійович, кандидат технічних наук, асистент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0001-9413-3709.

Джулій Володимир Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, http://orcid.org/0000-0003-1878-4301.

Дружинін Володимир Анатолійович, доктор технічних наук, професор, професор кафедри радіотехніки та радіоелектронних систем факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-5340-6237.

Думенко Микола Петрович, кандидат військових наук, перший заступник начальника Головного управління персоналу Генерального штабу Збройних Сил України, https://orcid.org/0000-0001-5633-7700.

Жиров Генадій Борисович, кандидат технічних наук, старший науковий співробітник, доцент кафедри радіотехніки та радіоелектронних систем факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0001-7648-7992.

Зайцев Дмитро Володимирович, кандидат військовий наук, доцент, доцент кафедри, факультет післядипломної освіти, Військовий інститут Київського національного університету імені Тараса Шевченка, http://orcid.org/0000-0002-3784-5790.

Каблуков Олег Анатолійович, старший науковий співробітник Центрального науково-дослідного інституту Збройних Сил України, http://orcid.org/0000-0001-8611-084.

Кирпач Людмила Андріївна, кандидат технічних наук, доцент, завідувач кафедри Космічних систем та комплексів і супутникових телекомунікацій Державного університету телекомунікацій, https://orcid.org/0000-0001-9210-922X.

Кльоц Юрій Павлович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, https://orcid.org/0000-0002-3914-0989.

Комаров Володимир Олександрович, Заслужений винахідник України, начальник науково-дослідного відділу Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України, https://orcid.org/0000-0002-4929-4527.

Комарова Лариса Олексіївна, доктор технічних наук, старший науковий співробітник, професор кафедри «Телекомунікації» ОНАЗ ім.О.С. Попова, Лауреат Державної премії України в галузі науки і техніки, https://orcid.org/0000-0002-9776-0879.

Краснік Анатолій Васильович, кандидат технічних наук, старший науковий співробітник, науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка.

Лєнков Євген Сергійович, кандидат технічних наук, старший науковий співробітник наукового центру Центрального науково-дослідного інституту Збройних Сил України, http://orcid.org/0000-0001-5819-2656.

Лєнков Сергій Васильович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, головний науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0001-7689-239X.

Литвиненко Наталія Ігорівна, кандидат технічних наук, старший науковий співробітник, начальник науково-дослідної лабораторії науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-2203-2746.

Лук'янчіков Іван Миколайович, слухач командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняховського, https://orcid.org/0000-0003-3143-9556.

Матвієнко Олена Олександрівна, старший науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка (Київ, Україна), https://orcid.org/0000-0002-6767-315X

Мірошніченко Олег Вікторович, кандидат технічних наук, старший науковий співробітник, начальник науково-дослідного управління науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, http://orcid.org/ 0000-0002-3969-9758.

Муляр Ігор Володимирович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем та мереж Хмельницького національного університету, http://orcid.org/0000-0002-6659-605X.

Мясіщев Олександр Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, https://orcid.org/0000-0003-1269-425X.

Нікіфоров Микола Миколайович, кандидат військових наук, старший науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-2849-5688.

Нікіфоров Микола Миколайович, старший проектний менеджер, керівник проектів Global (IT галузь: BPM/CRM), приватний підприємець.

Ніколаєнко Віктор Павлович, слухач командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняховського, https://orcid.org/0000-0003-2176-8456.

Одарченко Роман Сергійович, доктор технічних наук, доцент, заступник декана факультету аеронавігації, електроніки та телекомунікацій національного авіаційного університету, https://orcid.org/0000-0002-7130-1375.

Оксіюк Олександр Глібович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0001-9797-6015.

Ошкодер Сергій Васильович, слухач командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняховського, https://orcid.org/0000-0003-1987-6432.

Пампуха Ігор Володимирович, кандидат технічних наук, доцент, начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, https://orcid.org/0000-0002-4807-3984.

Пархомей Ігор Ростиславович - доктор технічних наук, професор, професор кафедри технічної кібернетики факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», https://orcid.org 0000-0002-9510-7657.

Писаренко Роман Вікторович, доцент кафедри геоінформаційних систем і технологій Військового інституту Київського національного університету імені Тараса Шевченка. https://orcid.org/0000-0002-9807-0028.

Приходько Олексій Григорович, слухач командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняховського, https://orcid.org/0000-0003-7193-4336**.**

Семененко Олег Михайлович, доктор військових наук, старший науковий співробітник, начальник науково-дослідного відділу Центрального науково-дослідного інституту Збройних Сил України, https://orcid.org/0000-0001-6477-3414.

Сєлюков Олександр Васильович, доктор технічних наук, старший науковий співробітник, заступник директора ТОВ «Укрспецконсалтинг», https://orcid.org/0000-0001-7979-3434.

Тітова Віра Юріївна, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету, https://orcid.org/0000-0001-8668-4834.

Толок Ігор Вікторович, кандидат педагогічних наук, доцент, Заслужений працівник освіти України, начальник Військового інституту, Київський національний університет імені Тараса Шевченка, http://orcid.org/0000-0001-6309-9608.

Туровський Олександр Леонідович, кандидат технічних наук, доцент, доцент кафедри Космічних систем та комплексів і супутникових телекомунікацій Державного університету телекомунікацій, https://orcid.org/0000-0002-4961-0876.

Федюра Тетяна Вікторівна, инженер информационно-телекоммуникационных систем у компанії Киевстар, https://orcid.org/ 0000-0001-5330-0822.

Цьопа Наталія Володимирівна, кандидат технічних наук, доцент, доцент кафедри технічної кібернетики факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», https://orcid.org/0000-0002-3215-0711.

Чешун Віктор Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем та мереж Хмельницького національного університету, https://orcid.org/0000-0002-3935-2068.

Швалючинський Василь Володимирович, кандидат військовий наук, доцент, професор кафедри, командно-штабний інститут застосування військ (сил) Національного університету оборони України імені Івана Черняховського, http://orcid.org/0000-0002-8782-383X.

АЛФАВІТНИЙ ПОКАЗЧИК

Наукове видання

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Військового інституту

Київського національного університету імені Тараса Шевченка

№ 67

Усі матеріали надруковані в авторській редакції.
Деякі статті не рецензуються, у зв'язку з пріоритетною кваліфікацією авторів або через сумніви редколегії у змісті.

Підписано до друку 24.01.20 р.
Авт. друк. Арк. 11. Формат 60х90/8
Безкоштовно. Замовлення № 10-2012

Надруковано у навчальному картографічному комплексі ВІКНУ

03189, Київ, вул. Ломоносова 81

т. 521-32-89