МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ ІМЕНІ С. П. КОРОЛЬОВА

ПРОБЛЕМИ СТВОРЕННЯ, ВИПРОБУВАННЯ, ЗАСТОСУВАННЯ ТА ЕКСПЛУАТАЦІЇ СКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

17

Житомир
2019

Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : збірник наукових праць. Вип. 17 / Житомирський військовий інститут імені С. П. Корольова. – Житомир : ЖВІ, 2019. – 188 с. – ISSN 2076-1546. https://doi.org/10.46972/2076-1546.2019.17.

Наказом Міністерства освіти і науки України від 11.07.2016 № 820 збірник наукових праць включений до Переліку наукових фахових видань України, у якому можуть бути опубліковані основні результати дисертаційних робіт з технічних наук.

Рекомендовано до друку рішенням вченої ради Житомирського військового інституту імені С. П. Корольова, протокол № 6 від 26.12.2019.

Науковий профіль видання:
122 – Комп'ютерні науки
125 – Кібербезпека
172 – Телекомунікації та радіотехніка
255 – Озброєння та військова техніка

ISSN 2076-1546

Наукові статті, включені до збірника наукових праць, пройшли рецензування.

Свідоцтво про державну реєстрацію КВ № 21859-11759 ПР від 21.12.2015.

ЗМІСТ

УДК 004.047 DOI: 10.46972/2076-1546.2019.17.01

А. А. Завада, М. М. Павленко, О. М. Наумчак, С. А. Ратушний

УДОСКОНАЛЕНА ФУНКЦІОНАЛЬНА СХЕМА АВТОМАТИЗОВАНОЇ СИСТЕМИ ВИЯВЛЕННЯ ТА ОЦІНЮВАННЯ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ В ЕЛЕКТРОННИХ ЗАСОБАХ МАСОВОЇ ІНФОРМАЦІЇ

У статті проаналізовано сучасне спеціалізоване програмне забезпечення моніторингу інформаційного простору (контент-моніторингу), призначене для виявлення інформаційних загроз та деструктивних інформаційно-психологічних впливів, які розповсюджує противник. Досліджено основні функції систем контент-моніторингу та розглянуто проблемні питання, що виникають у ході роботи з ними. Проаналізовано технічні концепції, які використовують для вирішення проблем обробки надвеликих об'ємів даних, пошуку і навігації в динамічних інформаційних потоках. Також вказано на основні недоліки відомих програмних засобів моніторингу відкритих електронних інформаційних ресурсів, що не дозволяють працювати з надвеликими об'ємами неструктурованих даних. Основними їх негативними особливостями є: робота з малими, середніми, великими об'ємами інформації; простота пошукових можливостей; відсутність механізмів якісного аналізу. Визначено мету розроблюваного програмного продукту, яка полягає в підвищенні оперативності інформаційно-аналітичної роботи органів військового управління щодо пошуку й аналізу документів, отриманих із відкритих джерел інформації, наведено його загальну структуру та окреслено основні функції. Запропоновано підхід до створення спеціалізованого програмного забезпечення виявлення та оцінювання деструктивного інформаційно-психологічного впливу в електронних засобах масової інформації органам військового управління, який повинен полегшити роботу оператора: забезпечити його обмеженою вибіркою документів, відсіявши за встановленими фільтрами зайве; надати зручний інструментарій для проведення оцінювання. Запропоновано удосконалену функціональну схему автоматизованої системи, яка складається з трьох основних блоків: інформаційного, трансляційного, обчислювального.

Ключові слова: *автоматизована система*; *електронні засоби масової інформації; моніторинг; деструктивний інформаційно-психологічний вплив; органи військового управління; спеціалізоване програмне забезпечення.*

Постановка проблеми в загальному вигляді. На даний час електронні засоби масової інформації (ЗМІ) нарощують свою аудиторію, а отже, перетворюються на потужний ресурс масштабного розповсюдження відповідного контенту серед населення, охоплюючи практично всі категорії та вікові групи. В умовах агресії Російської Федерації (РФ) проти України, проведення операції Об'єднаних сил на території Донецької та Луганської областей електронні ЗМІ широко використовуються противником для здійснення деструктивного інформаційно-психологічного впливу (ІПсВ) на військово-політичне керівництво, військовослужбовців Збройних Сил України та цивільне

населення нашої держави. Інформаційний фон, що створюється в суспільстві під час війни, позначається на ставленні громадян до політики свого уряду та дій силовиків, на комплектуванні армії, функціонуванні воєнної економіки та інших сфер, що безпосередньо впливають на хід бойових дій. Більше того, зусилля органів військового управління (ОВУ) щодо захисту військ (сил) від ворожої пропаганди можуть бути нівельованими, якщо аналогічна робота з населенням не проводиться чи проводиться на недостатньому рівні, оскільки суспільне ставлення до війни буде впливати на Збройні Сили [1]. Отже, виявлення деструктивного ІПсВ в електронних ЗМІ є важливим та актуальним науково-практичним завданням.

Аналіз останніх досліджень та публікацій. Для виконання завдань, пов'язаних з оперативним аналізом обстановки, застосовують системи моніторингу інформаційного простору (контент-моніторингу) [2]. У процесі роботи з такими системами під час збирання, аналізу інформації виникають проблеми обробки надвеликих об'ємів даних, пошуку і навігації в динамічних інформаційних потоках. Для їх вирішення розробляються нові технологічні концепції, такі як Big Data (великі дані), Complex Networks (складні мережі), Cloud Computing (хмарні обчислення), Data/Text Mining (глибинний аналіз даних і тексту) [3, 4], які дозволяють виконувати завдання пошуку необхідної інформації в мережі. При цьому залишається проблема подальшої її аналітичної обробки, виокремлення необхідних фактографічних даних, виявлення тенденцій розвитку в окремих предметних областях, взаємозв'язків об'єктів, подій, розпізнавання змістовних аномалій, прогнозування тощо. Більшість із них – це актуальні питання семантичної обробки надвеликих динамічних текстових масивів інформації [5]. Відомі окремі спроби практичного вирішення цих проблем, які сьогодні зумовлюють успіх таких проектів, як Google, Яndex, Baidu (пошукові системи), Keyhole, Brandwatch, CyberAlert (системи моніторингу соціальних мереж), Palantir, Centrifuge (аналітичні системи) [4].

На сьогодні виробники програмного забезпечення (ПЗ) пропонують свої рішення щодо пошуку та аналізу інформації з електронних ресурсів, як правило, у вигляді масштабованих систем, у яких реалізовано математичні й лінгвістичні алгоритми аналізу текстових та інших даних [6–9]. Вони мають графічні інтерфейси, можливості візуалізації, маніпулювання з даними, функціонують за архітектурою "клієнт – сервер". Прикладом таких систем є: "Intelligent Miner for Text" (IBM), "TextAnalyst", "WebAnalyst" ("Megaputer Intelligence"), "Text Miner" (SAS), "SemioMap" (Semio Corp.), "Oracle Text" (Oracle), "Knowledge Server" (Autonomy), "Galaktika ZOOM" (корпорація "Галактика"), "InfoStream" (інформаційний центр "ЕЛВІСТІ") [10–12]. Багато з перерахованих систем забезпечені власними або вбудованими авторубрикаторами й анотаторами [13–15], а це означає, що вказані інструменти поступово стають стандартними для інформаційно-аналітичних систем. Постійною необхідністю для такого класу програм є вміння працювати з тезаурусом (словником синонімів) і враховувати морфологію мови.

Формулювання завдання дослідження. Основним завданням систем, які здійснюють моніторинг великих об'ємів неструктурованих даних, є виявлення в них знань для подальшого використання під час прийняття рішень. Щоб досягти цього, інформаційно-аналітичні системи повинні здійснювати не лише пошук інформації, але й робити її доступною для аналізу, виявляти класи понять та зіставляти їх із документами.

Наявні системи лише частково реалізовують функціонал інтелектуального пошуку та аналізу даних, що становлять інтерес для Збройних Сил (ЗС) України. Відповідно, метою статті є вдосконалення архітектури автоматизованої системи виявлення та оцінювання деструктивного інформаційно-психологічного впливу в електронних ЗМІ.

Виклад основного матеріалу. Для ефективного функціонування органам державного управління та ОВУ необхідно взаємодіяти з інформаційним полем, що динамічно змінюється та містить багато оперативних, оглядових матеріалів. Великі масиви даних повинні підлягати якісному аналізу, оскільки на основі інформації з відкритих джерел можна не лише аналізувати стан справ, але й виявляти та оцінювати деструктивні ІПсВ, які розповсюджуються противником із використанням мережі Інтернет, прогнозувати розвиток ситуації, що необхідно для прийняття правильних управлінських рішень, зокрема й у воєнній сфері.

Вирішують такі завдання завдяки застосуванню засобів автоматизації моніторингу електронних ЗМІ. Системи моніторингу інформаційного простору (контент-моніторингу) [2] забезпечують: оперативність, яку не можна отримати від традиційних пошукових систем (час індексації мережевого контенту може варіюватися від доби до декількох тижнів); повноту (як щодо самих джерел, так і щодо надання матеріалів), яку не забезпечують агрегатори новин; задіяння аналітичних засобів автоматизованого проектування, моделювання і прогнозування процесів/подій. Проблеми розмірності та динаміки багатомовних інформаційних ресурсів у глобальних мережах потребують здійснення фундаментальних досліджень у галузях дискретної математики (теорії графів, мереж), розпізнавання образів (класифікація, кластерний аналіз), лінгвістики, цифрової обробки сигналів, вейвлет і фрактального аналізу.

Спеціалізованих програм, які допомагають збирати та сортувати матеріали з відкритих електронних інформаційних ресурсів, зокрема з електронних ЗМІ, на ринку програмних продуктів є досить багато, але всі вони, як правило, здійснюють зберігання середніх або великих об’ємів інформації, мають прості пошукові можливості та/або тематичні рубрикатори, не пропонуючи механізмів якісного аналізу. Деякі програми вміють здійснювати “інтелектуальний” пошук у масиві даних, відбираючи документи за набором ключових слів, частотою їх використання та відносним розташуванням, реалізовуючи це з урахуванням морфології. Такі програми вже здатні здійснювати простий контент-аналіз та семантико-статистичну обробку.

Як правило, інформаційні масиви перетворюються зазначеними вище системами в сховища даних або корпоративні портали знань – інтегровані інформаційні репозиторії, доступні для оперативного узагальнення й аналізу. Для підвищення їх функціональності вводяться додаткові програмні елементи машинного навчання, що забезпечують адаптацію критеріїв групування документів.

За рахунок попереднього оброблення інформації, що проводиться на етапі формування сховищ даних, значно підвищується ефективність таких процесів, як інтелектуальний аналіз даних, глибинний аналіз текстів та виявлення нових знань у них.

Для спрощення пошуку користувачем спостерігається тенденція застосування елементів нечіткої логіки запитів (нечіткого пошуку), побудови функціональних інформаційних портретів, візуалізації семантичних зв’язків. Так само ці можливості

безпосередньо пов'язані з дослідженнями за напрямом розпізнавання образів, пошуку мультимедійних даних, аналізу можливостей щодо мовного введення інформації.

Основним стримувальним фактором у завданні виявлення та оцінювання рівня деструктивного ІПсВ ОВУ в ході використання широкого спектра пошукових систем, які легко справляються з "простим" повнотекстовим пошуком, є ускладнення процесу прийняття рішень під час спроби аналізу великих об'ємів неструктурованих або слабо структурованих даних.

Використання численних систем моніторингу та аналізу текстових даних, що вільно розповсюджуються, не завжди доцільне через часткову реалізацію ними необхідних функціональних можливостей щодо інтелектуального аналізу даних і їх основної спрямованості на застосування у сфері бізнес-маркетингу. Тому для виявлення та оцінювання деструктивного ІПсВ ОВУ потрібне застосування одразу декількох таких продуктів для задоволення потреб операторів / аналітиків. Також слід зазначити, що подібні продукти переважно розповсюджуються із закритим вихідним кодом та не дозволяють дослідити закладені в їх основу алгоритми.

Комерційні продукти провідних виробників забезпечують досить широкий функціонал для досліджень, але зазвичай побудовані за схемою надання доступу до власної аналітичної платформи, даних (серверів виробників) та не дозволяють завантажувати останні на власні ресурси для подальшого ретроспективного аналізу, оцінювання та прогнозування. Основним спрямуванням також є бізнес-аналітика. Доступ до ресурсів проводиться на основі передплачених тарифних планів високої вартості. Також використання аналітичної платформи зазначених продуктів для пошуку необхідної інформації, її оброблення й формування звітно-аналітичних документів спеціальними органами та службами може слугувати додатковою розвідувальною ознакою щодо визначення їх інтересів і напрямів діяльності.

Використання відомих різноманітних модулів, що реалізують окремі функції моніторингу, веб-сервісів та інших систем вважається доцільним під час виконання окремих специфічних завдань (наприклад, аналізу активності розповсюдження інформації, залученості аудиторії, визначення географічної інформації акаунтів користувачів соціальних мереж (СМ) тощо) як додаткових інструментів аналітика. Виходячи із зазначеного вище, актуальним є завдання автоматизації моніторингу електронних ЗМІ за рахунок створення спеціалізованого ПЗ (СПЗ) в удосконаленій автоматизованій системі (АС).

Основною метою створення удосконаленої АС є підвищення оперативності інформаційно-аналітичної роботи ОВУ щодо пошуку й аналізу документів, отриманих із відкритих джерел інформації.

Удосконалена АС повинна забезпечувати періодичний збір та тематичний пошук документів із відкритих джерел інформації електронних ЗМІ, їх лінгвістичну обробку, ведення бази даних (БД) отриманих документів, надання програмного інструментарію для здійснення контент-аналізу користувачами.

З урахуванням цих особливостей розроблюване СПЗ має забезпечувати реалізацію таких основних функцій:

цілеспрямований пошук потрібної інформації та відбір інформаційного матеріалу з відкритих електронних ЗМІ за вимогами оператора;

надання оператору зручного інструментарію для проведення аналізу інформаційних повідомлень (ІП);

оцінювання рівня деструктивного ІПсВ;

збереження ІП та результатів їх аналізу в БД.

Удосконалена АС повинна забезпечувати можливість:

контекстного пошуку в масиві вихідних ІП із можливістю використання логічних відношень (І, ЧИ, НІ) та відстані між словами;

пошуку ІП за різними параметрами: датою публікації; інформаційними об'єктами та їх списками; джерелами електронних ЗМІ / СМ / RSS-каналів; авторами; інформаційними приводами (тематичними рубриками); оцінкою характеру згадування у висвітленні теми (об'єкта);

формування електронного оперативного дайджесту основних подій у ЗМІ: оперативної інформації про основні події у світі щодо України, у державі в цілому та в зоні проведення операції Об'єднаних сил зокрема (новини з інформаційних стрічок агентств, окремі стрічки основних подій, що мають негативне забарвлення);

формування оперативного дайджесту за відповідними ключовими темами (хештегами), наприклад: Президент України (рейтинг, позитив, негатив, цитування); Міністр оборони України; Міністерство оборони України; керівники Міністерства оборони України; сучасний стан ЗС України; активні бойові дії; дискредитація ЗС України; протиправні та злочинні дії військовослужбовців; проблеми в армії, мобілізація; дислокація російсько-терористичних військ; докази присутності кадрових військовослужбовців, озброєння та військової техніки РФ в Україні; факти порушення Мінських угод; інформація щодо ватажків терористів тощо.

Усі ІП, отримані оператором (користувачем), мають проходити лінгвістичну обробку, яка включає:

виділення інформаційних об'єктів у дайджесті та повнотекстних публікаціях;

тематичну класифікацію текстів;

виявлення груп інформаційних подій та кластеризацію інформаційних матеріалів;

визначення характеру згадування об'єктів (нейтральне, позитив, негатив);

можливість фільтрації публікацій за приналежністю та рівнем ЗМІ (закордонні (російські), українські, регіональні, місцеві).

Для кожного інформаційного матеріалу повинні бути доступні такі відомості:

заголовок (назва);

джерело (назва електронного ЗМІ / групи СМ / RSS-канал);

дата публікації матеріалу;

автор (якщо зазначено).

Після того, як матеріал зібрано, актуальним стає завдання його якісного аналізу. Аналіз інформації покладається на оператора, який, на відміну від комп'ютерної програми, здатен накопичувати досвід та має інтуїцію. Хоча швидкість оцінювання при цьому відносно мала, спостерігається суттєвий виграш у якості. Необхідність покладання аналізу інформації на оператора обумовлена також тим, що дані, отримані з відкритих джерел інформації, можуть містити дезінформацію. У відкритих електронних ЗМІ часто розміщують інформацію, орієнтовану на цілеспрямоване формування певних образів. Потрібен аналіз, який дозволить досягти такого рівня розуміння повідомлення, за якого можливо встановити мету ІП, що не можливо з використанням автоматичних систем. Крім того, автоматична система неминуче буде враховувати інформацію, яка має заздалегідь

фейковий характер, але з програмного погляду ніяк не відрізняється від справжньої. Враховуючи значний обсяг даних, що поширюються у відкритих джерелах, можна стверджувати, що додатково виникає завдання оцінювання релевантності джерела інформації, під якою розуміється встановлювана в ході інформаційного пошуку відповідність змісту контенту інформаційному запиту.

З урахуванням зазначеного вище, розроблюване СПЗ має максимально полегшити роботу оператора: по-перше, забезпечити його обмеженою вибіркою документів, відсіявши за встановленими фільтрами зайве; по-друге, надати зручний інструментарій для проведення оцінювання.

Для реалізації перерахованих можливостей запропоновано функціональну схему удосконаленої АС (рис. 1).

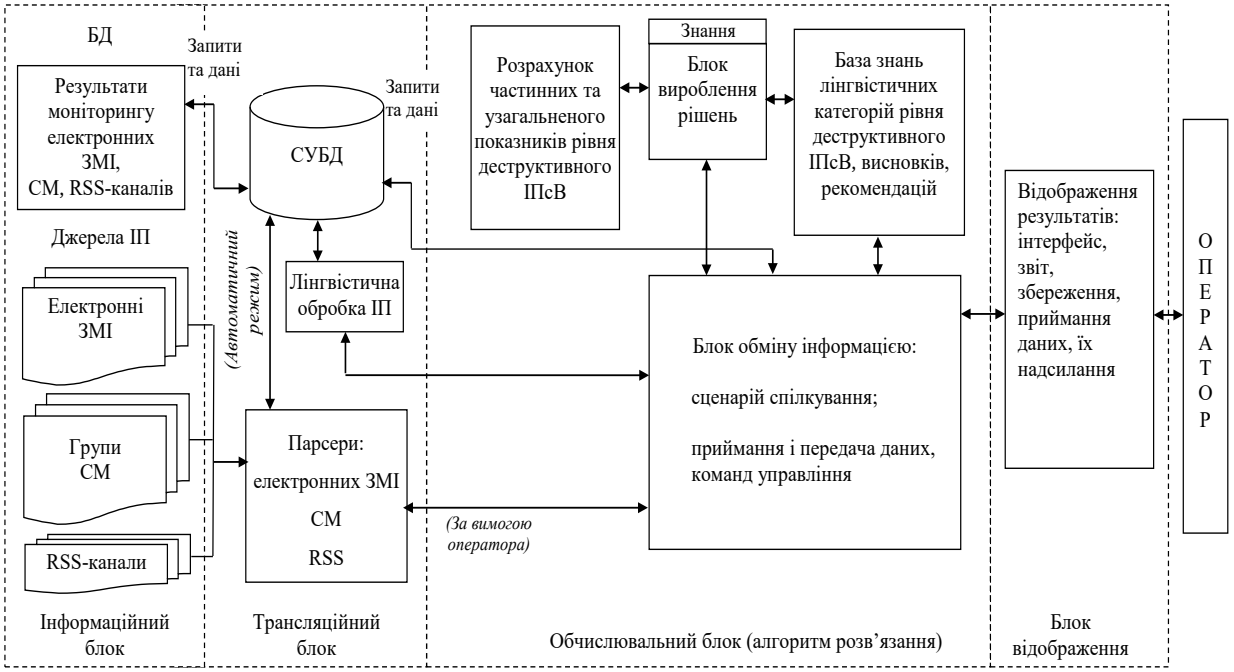


Рис. 1. Функціональна схема удосконаленої АС виявлення та оцінювання деструктивного ІПсВ в електронних ЗМІ

Відповідно до схеми доцільно, щоб АС складалася з трьох основних блоків: інформаційного, трансляційного, обчислювального.

Інформаційний блок включає БД результатів моніторингу електронних ЗМІ, СМ, RSS-каналів та визначений перелік відкритих джерел.

Трансляційний блок містить у собі систему управління базами даних (СУБД), блок парсерів відкритих джерел інформації (програмні модулі, що реалізують окремий функціонал відповідно до структури HTML-коду веб-ресурсу, СМ, параметризованих запитів-відповідей RSS-каналів) та блок лінгвістичної обробки ІП.

Обчислювальний блок містить базу знань (БЗ) лінгвістичних категорій рівня деструктивного ІПсВ, блок розрахунку частинних та узагальненого показників рівня деструктивного ІПсВ, блок вироблення рішень та обміну інформацією. За допомогою блоку вироблення рішень на підставі фактів БЗ формуються вихідні рішення і через блок обміну інформацією надаються оператору для вироблення остаточного рішення. Додатково він має можливість візуалізації проміжних результатів розрахунків у вигляді

таблиць, графіків та звітних матеріалів. Прикінцевий блок – блок відображення результату, що реалізує подання даних обчислень оператору.

Висновки. Завдання виявлення та оцінювання деструктивного ІПсВ в електронних ЗМІ зумовило необхідність розроблення удосконаленої схеми АС та СПЗ, яке окрім функцій, властивих аналогам, визначатиме факти наявності або відсутності в контенті ознак деструктивного впливу. Відповідна АС дозволяє підвищувати оперативність інформаційно-аналітичної роботи ОВУ. У статті обґрунтовано вимоги до АС та її функціональних спроможностей. Науковою новизною отриманих результатів є удосконалення архітектури АС виявлення та оцінювання деструктивного ІПсВ в електронних ЗМІ для підвищення якості аналізу ІП шляхом поділу функцій їх збору та обробки на інформаційний, трансляційний та обчислювальний блоки.

Перспективним напрямком подальших досліджень є створення розподіленої клієнт-серверної архітектури АС, що реалізує функції системи підтримки прийняття рішень виявлення та оцінювання деструктивного ІПсВ в електронних ЗМІ.

СПИСОК ЛІТЕРАТУРИ

1. Жарков Я. М. Інформаційно-психологічна боротьба у воєнній сфері : навч. посіб. Київ : вид.-поліграф. центр “Київський університет”, 2014. 423 с.

2. Додонов А. Г., Ландэ Д. В., Прищепа В. В., Путятин В. Г. Конкурентная разведка в компьютерных сетях. Киев : ИПРИ НАН Украины, 2013. С. 20–45.

3. Ланде Д. В., Кондратенко Я. А. Особливості побудови систем розподіленого контент-моніторингу глобальних інформаційних мережах // Information Technology and Security. 2017. Vol. 5. Iss. 1 (8). P. 5–11.

4. Барсегян А. А., Куприянов М. С., Степаненко В. В., Холод И. И. Технологии анализа данных: Data Mining, Visual Mining, Text Mining, IOLAP. 2-е изд., перераб. и. доп. Санкт-Петербург : БХВ, 2007. 384 с.

5. Liu H., Gegov A., Cocea M. Rule Based Systems for Big Data. A Machine Learning Approach. Heidelberg, Switzerland : Springer, 2016. Studies in Big Data. Vol. 13. 121 p.

6. Липинский Ю. В. Средства информационного поиска и навигации в больших массивах неструктурированной информации. URL: http://masters.donntu.org/2009/fvti/larionova/library/article23.htm (дата обращения: 20.06.2019).

7. Разведка по открытым источникам для малого бизнеса. URL: http://www.osint.ru/open-source-intelligence-annot.htm (дата обращения: 20.06.2019).

8. Аликберов А. Несколько слов о том, как работают роботы поисковых машин. URL: http://citforum.ru/internet/search/art_1.shtml (дата обращения: 20.06.2019).

9. Тихонов В. Поисковые системы в сети Интернет. URL: http://citforum.ck.ua/internet/search/searchsystems.shtml (дата обращения: 20.06.2019).

10. Храмцов П. Поиск и навигация в Internet. URL: http://masters.donntu.org/2005/fvti/shadiaburuck/library/xramzov.htm (дата обращения: 20.06.2019).

11. Додонов А. Г., Ландэ Д. В., Путятин В. Г. Современные поисковые технологии – проблемы и некоторые пути их решения // Реєстрація, зберігання і обробка даних. 2010. Т. 12, № 3. С. 36–55.

12. Аналитическая система “Галактика ZOOM”. URL: http://club.cnews.ru/blogs/entry/galaktika_zoom_opyt_uspeshnyh__99d0a (дата обращения: 20.06.2019).
13. Мифы и реальности Internet – известные и скрытые возможности сети. URL: http://www.dist-cons.ru/modules/internet/main.htm (дата обращения: 20.06.2019).
14. 15 инструментов мониторинга СМИ и социальных медиа. URL: http://mediabitch.ru/15-instrumentov-monitoringa/ (дата обращения: 20.06.2019).
15. Архипов О. Є, Петренко М. А. Застосування онтологічних ієрархій у задачах визначення цінності інформації. Захист інформації. 2012. № 1. С. 42–47.

Подано 24.09.2019

А. А. Завада, М. М. Павленко, Е. М. Наумчак, С. А. Ратушний

УСОВЕРШЕНСТВОВАННАЯ ФУНКЦИОНАЛЬНАЯ СХЕМА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ВЫЯВЛЕНИЯ И ОЦЕНКИ ДЕСТРУКТИВНОГО ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ В ЭЛЕКТРОННЫХ СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

В статье проведен анализ существующего специализированного программного обеспечения мониторинга информационного пространства (контент-мониторинга), предназначенного для выявления информационных угроз и деструктивных информационно-психологических воздействий, которые распространяет противник. Исследованы основные функции систем контент-мониторинга и рассмотрены проблемные вопросы, возникающие в ходе работы с ними. Проанализированы технические концепции, используемые для решения проблем обработки сверхбольших объемов данных, поиска и навигации в динамических информационных потоках. Также выявлены основные недостатки в использовании существующих программных средств мониторинга открытых электронных информационных ресурсов, не позволяющие работать со сверхбольшими объемами неструктурированных данных. Основными из них являются работа с малыми, средними, большими объемами информации, простота поисковых возможностей, отсутствие механизмов анализа. Определена цель разрабатываемого программного продукта, которая заключается в повышении оперативности информационно-аналитической работы органов военного управления по поиску и анализу документов, полученных из открытых источников информации, представлено его общую структуру и очерчены основные функции. Предложен подход к созданию специализированного программного обеспечения выявления и оценки деструктивного информационно-психологического воздействия в электронных средствах массовой информации органам военного управления, который должен облегчить работу оператора: обеспечить его ограниченной выборкой документов, отсеяв по установленным фильтрам лишнее; предоставить удобный инструментарий для проведения оценки. Предложена усовершенствованная функциональная схема автоматизированной системы, которая состоит из трех основных блоков: информационного, трансляционного, вычислительного..

Ключевые слова: *автоматизированная система; электронные средства массовой информации; мониторинг; деструктивное информационно-психологическое воздействие; органы военного управления; специализированное программное обеспечение.*

A. A. Zavada, M. M. Pavlenko, O. M. Naumchak, S. A. Ratushnyi

IMPROVED BLOCK DIAGRAM OF THE AUTOMATED SYSTEM OF THE DETECTION AND EVALUATION OF DESTRUCTIVE INFORMATION AND PSYCHOLOGICAL INFLUENCE IN ELECTRONIC MEDIA

In the work the existing specialized software for information space monitoring (content monitoring), which is designed to identify information threats and destructive information and psychological influences that are spread by the enemy was analyzed. The main functions of content monitoring systems are presented and problems that arise during their work are considered. The technical concepts used to solve the problems of big-data processing, searching and navigating dynamic information flows were analyzed. There are also major disadvantages to using existing open source electronic monitoring tools that do not allow the processing of the unstructured big-data. These include working with small, medium, large data, ease of search capabilities, lack of quality of analysis tools and business orientation. The main purpose of the developed software product is determined, which is to increase the efficiency of information and analytical work of the military authorities in search and analysis of documents obtained from open sources of information, its general structure and the main functions are defined. An approach to the creation of specialized software for detecting and evaluating the destructive information and psychological influence in electronic media for military authorities is proposed, which should make the operator's work as easy as possible: to provide him with a limited selection of documents, eliminating unnecessary filtering; provide convenient tools for evaluating. Functional diagram of the software is proposed, which consists of three main blocks: information, broadcast, computing.

Keywords: *automated system; electronic mass media; monitoring; information and psychological influence; military authorities; specialized software.*

ISSN 2076-1546

УДК 621.396 DOI: 10.46972/2076-1546.2019.17.02

М. В. Бугайов, Б. В. Молодецький, І. О. Михайлюк, В. В. Гордійчук

МЕТОД ОЦІНЮВАННЯ ПАРАМЕТРІВ СИГНАЛІВ РАДІОСТАНЦІЙ ЗІ ШВИДКОЮ ПСЕВДОВИПАДКОВОЮ ПЕРЕБУДОВОЮ РОБОЧОЇ ЧАСТОТИ

Сучасні засоби радіозв'язку спеціального призначення використовують режим надкороткої пакетної передачі зі швидкою псевдовипадковою перебудовою робочої частоти та некогерентною частотною маніпуляцією. Ідентифікацію таких радіостанцій запропоновано здійснювати шляхом оцінювання швидкостей перебудови частоти та передавання інформації, кількості частотних каналів і кроку сітки частот прийнятих радіосигналів, а також порівняння отриманих значень із відповідними характеристиками відомих радіостанцій зі швидкою псевдовипадковою перебудовою робочої частоти. Часові межі та тривалість частотних елементів розраховують за комплексною обвідною прийнятого сигналу. Для цього розроблено відповідний метод, що полягає у фільтрації обвідної за допомогою вікна з ковзним середнім для подавлення шумової складової та порогового оброблення. Частоти частотних елементів визначають за незгладженими періодограмними оцінками, а для підвищення точності оцінювання частоти використовують експоненціальну екстраполяцію дискретного спектра потужності. Показано, що для однозначного визначення кроку сітки частот та рознесення частот частотної маніпуляції необхідно проаналізувати кількість частотних елементів, що не менше кількості частотних каналів. Шляхом аналізу гістограми різниць відсортованого за зростанням вектора частот частотних елементів визначають крок сітки частот, рознесення частот та кратність частотної маніпуляції. Наближену оцінку кількості частотних каналів обчислюють як відношення розмаху вектора частот частотних елементів до кроку його сітки. Швидкість передавання інформації можна встановити лише після демодуляції сигналу та аналізу бітових потоків, у результаті якого можна визначити структуру кадрів і кількість службових та інформаційних бітів. Запропонований метод забезпечує оцінювання значень параметрів сигналів із відносною помилкою, що не перевищує 0,3%, у разі відношення сигнал-шум вище 5 дБ.

Ключові слова: *псевдовипадкова перебудова робочої частоти; ідентифікація; частотний канал; частотний елемент; інформаційний символ; частотна маніпуляція.*

Постановка проблеми у загальному вигляді. Для забезпечення завадозахищеності та прихованості сучасних засобів радіозв'язку спеціального призначення використовують режим надкороткої пакетної передачі з псевдовипадковою перебудовою робочої частоти (ППРЧ), що використовує короткочасну передачу інформації в ефір на різних частотах [1–2]. Такі цифрові радіостанції іноді працюють у режимі швидкої ППРЧ (швидкість перебудови робочої частоти більша за символьну швидкість та перевищує 1000 змін за секунду) і використовують значну кількість частотних каналів (кілька тисяч) із частотним рознесенням між сусідніми каналами, що значно менше ширини спектра частотного елемента. Основним видом модуляції в таких радіостанціях є некогерентна частотна маніпуляція (ЧМн). Крім того, у переважній більшості практично важливих випадків

прийом радіосигналів проводиться на фоні шумів, а самі сигнали поширюються через канал із завмираннями. Вказані особливості прийнятих сигналів даних радіостанцій призводять до складнощів їх ідентифікації, що зумовлює необхідність розроблення відповідних методів оцінювання параметрів сигналів зі швидкою ППРЧ.

Аналіз останніх досліджень та публікацій. Питання виявлення та оцінювання параметрів сигналів із ППРЧ розглядалися в численних вітчизняних та зарубіжних публікаціях. Зокрема, у [3] запропоновано алгоритм виявлення радіосигналів із ППРЧ на основі аналізу значень асиметрії та ексцесу спектральних оцінок. Проте даний алгоритм не забезпечує отримання оцінок параметрів сигналу. У [4] для виявлення та оцінювання частоти сигналів із ППРЧ запропоновано використовувати багатоканальний приймач на основі широкосмугового модуляційного конвертора, а в [5] наведено частотно-часовий алгоритм оцінювання параметрів ППРЧ. Точність оцінювання частотно-часових параметрів для запропонованих методів є недостатньою для ідентифікації радіостанцій, що є досить важливим для систем радіомоніторингу. У [6] розглянуто алгоритм для розпізнавання факту наявності в смузі частот аналізу сигналів із ППРЧ, що вимагає незначних обчислювальних затрат. Проте він не може бути застосований для систем зі швидкою ППРЧ. Запропонований у [7] підхід також не забезпечує необхідної точності визначення частотних параметрів сигналу з ППРЧ.

Особливості розглянутих методів та алгоритмів не дозволяють їх використовувати для ідентифікації радіостанцій, які працюють у режимі надкороткої пакетної передачі зі швидкою ППРЧ.

Формулювання завдання дослідження. Завданням дослідження є розроблення методу оцінювання параметрів сигналів радіостанцій зі швидкою ППРЧ та некогерентною частотною маніпуляцією в умовах їх прийому на фоні шумів та в каналі із завмираннями.

Виклад основного матеріалу

1. Модель прийнятого радіосигналу

Для швидкої ППРЧ розширення спектра досягається за рахунок рознесення символів тривалістю T_s на незалежні частотні елементи (субсимволи), кожен з яких передається почергово на своїй частоті. Часовий інтервал між переключеннями частот (тривалість частотного елемент T_h) характеризує час роботи на одній частоті [1]. При цьому $T_h = T_s/L$, де L − кількість частотних елементів, на які розбивається інформаційний символ. Основним видом інформаційної модуляції при передачі даних у системах зі швидкою ППРЧ є M-на некогерентна ЧМн, $M = 2^l$.

На рис. 1 наведено фрагмент частотно-часової матриці сигналу зі швидкою ППРЧ та двійковою ЧМн. Один інформаційний символ передається протягом двох частотних елементів. У межах тривалості частотного елемента T_h сигнал передається на частоті f_{ri}. Крок сітки частот незмінний і становить Δf, а рознесення частот ЧМн − ΔF.

Через особливості передавача радіостанцій значення амплітуд частотних елементів, які передаються на різних робочих частотах, є різними, а обвідна частотного елемента через специфіку його формування є не постійною, а складається з ділянки переходу між сусідніми субсимволами тривалістю T_{tr} та ділянки тривалістю T_{act}, на якій частотний елемент має прямокутну обвідну [1].

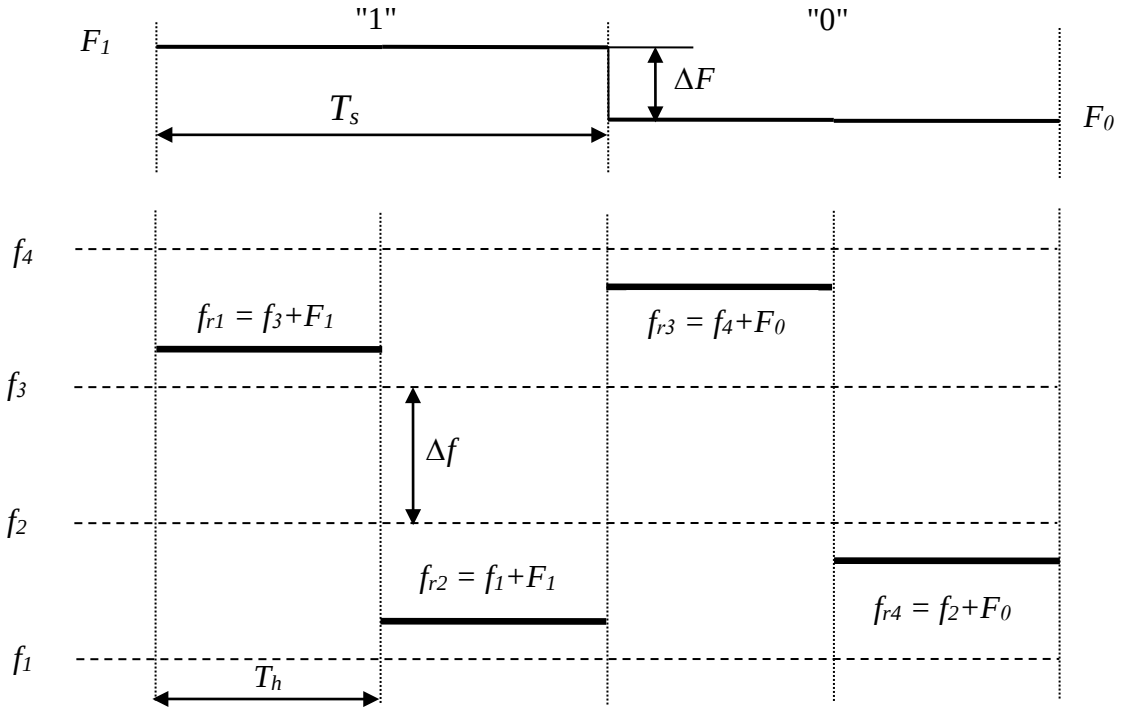


Рис. 1. Фрагмент частотно-часової матриці сигналу зі швидкою ППРЧ

На рис. 2 наведено 12 частотних елементів у часовій області, а в його правому верхньому кутку у збільшеному вигляді показано частотний елемент та його складові. Тривалість частотного елемента становить $T_h = T_{act}+T_{tr}$. Тривалість перехідної ділянки – $T_{tr} = \delta T_h$, де $\delta \approx 0{,}1...0{,}2$.

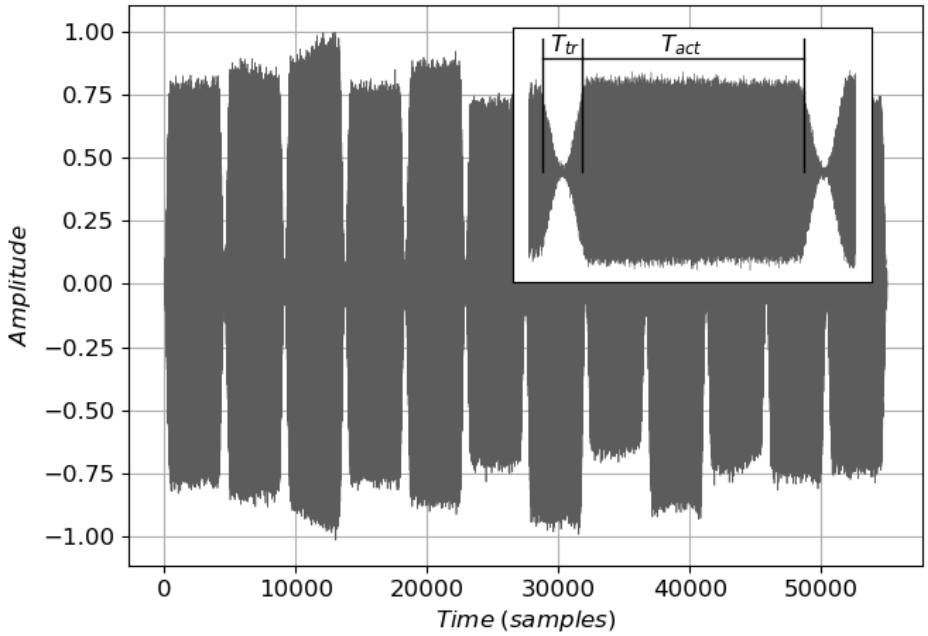


Рис. 2. Обвідна та часові інтервали складових частотного елемента

У припущенні, що в прийнятій реалізації сигналу міститься лише один сигнал зі швидкою ППРЧ та ЧМн, узагальнену модель прийнятого радіосигналу на фоні білого гаусівського шуму з нульовим середнім $\xi(t)$ можна записати у такому вигляді:

$$x(t)=\begin{cases} U(t)\,sin^2\left(\dfrac{\delta t}{2T_h}\right)+\xi(t), & iT_h \le t \le (i+1)\dfrac{\delta}{2}T_h; \\ U(t)+\xi(t), & (i+1)\dfrac{\delta}{2}T_h < t < (i+1)\left(1-\dfrac{\delta}{2}\right)T_h; \\ U(t)\,cos^2\left(\left(1-\dfrac{\delta}{2}\right)\dfrac{t}{T_h}\right)+\xi(t), & (i+1)\left(1-\dfrac{\delta}{2}\right)T \le t \le (i+1)T_h; \end{cases} \quad (1)$$

$$U(t)=A_i\rho(t)\cos\left\{2\pi\left(f_0+f_i+F_j\right)t\right\},\ i\in Z^{\geq},\ j=\lfloor i/L \rfloor,$$

де A_i – значення амплітуди i-го частотного елемента, В;

$\rho(t)$ – множник, що враховує завмирання сигналу в каналі поширення;

f_0 – зміщення частоти від початку смуги аналізу до першого частотного елемента, Гц;

$f_i = n_h \Delta f$ – частота i-го частотного елемента в Гц, де $n_h = 1..N_h$ – номер частотного каналу, N_h – кількість частотних каналів;

$F_j = m\Delta F$ – надбавка частоти за рахунок маніпуляції в Гц, де $m = 1..M$ – значення інформаційного символа;

$\lfloor\ \rfloor$ – операція округлення до цілого в меншу сторону.

Якщо розподіл значень робочих частот ППРЧ f_i є рівномірним, то можна припустити, що значення амплітуд частотних елементів A_i також розподілені рівномірно в деякому діапазоні $[A_{\min}, A_{\max}]$.

У системах зі швидкою ППРЧ, як правило, не проявляються частотно-селективні завмирання, тому що швидкість зміни робочої частоти перевищує швидкість передачі інформаційних символів. Тому такий канал радіозв'язку можна охарактеризувати як канал з повільними завмираннями (дрібномасштабне завмирання Релея), що проявляється в зменшенні значення відношення сигнал-шум (ВСШ) [8]. У виразі (1) множник $\rho(t)$ описує випадкову величину, розподілену за законом Релея. Із загасанням Релея пов'язані найбільші завмирання, що припадають на середню потужність прийнятого сигналу.

2. Опис методу оцінювання параметрів сигналу

Під час оброблення сигналів зі швидкою ППРЧ і ЧМн оцінюванню підлягають такі параметри: швидкість перебудови частоти, символьна швидкість, швидкість передавання даних, кількість частотних каналів N_h і крок сітки частот Δf.

Оскільки для радіостанцій зі швидкою ППРЧ крок сітки частот Δf менший ширини спектра частотного елемента $1/T_h$, то використання непараметричних методів спектрального аналізу на основі швидкого перетворення Фур'є (ШПФ) не забезпечить розділення сусідніх частотних каналів. Застосування параметричних методів спектрального оцінювання з високою роздільною здатністю за частотою (MUSIC) пов'язане з необхідністю попереднього оброблення прийнятої реалізації для визначення кількості вузькосмугових складових. Крім того, обчислювальна складність таких методів пропорційна третьому степеню довжини вікна. Проте, якщо відомо, що в заданих частотно-часових межах міститься лише одна вузькосмугова складова, то застосування

параметричних методів є недоцільним, оскільки система радіомоніторингу повинна працювати в реальному масштабі часу. Тому оцінимо часові межі кожного частотного елемента, у яких будемо визначати його частоту.

Для обчислення часових меж частотних елементів розрахуємо обвідну дискретизованої з частотою F_s, прийнятої реалізації процесу $x[n]$ відповідно до такого виразу:

$$E[n] = \sqrt{x^2[n] + x_Q^2[n]}, \tag{2}$$

де $x_Q[n]$ − квадратурна складова, отримана в результаті перетворення Гільберта.

Відповідно до рис. 2 необхідно встановити деякий пороговий рівень і точки його перетину з обвідною сигналу, що визначатимуть межі частотних елементів. Через влив завмирань та адитивного шуму обвідна сигналу буде сильно порізаною, тому для її згладжування використаємо вікно ковзного середнього, довжиною P. Перед цим обвідну сигналу нормуємо до її максимального значення на інтервалі аналізу. Значення порога γ визначимо для випадку, коли в прийнятій реалізації міститься лише шум. У такому разі значення відліків обвідної $E[n]$ підпорядковані розподілу Релея, а значення згладженої вікном ковзного середнього, довжиною P, обвідної $E[n]$ для $P \geq 30$ відповідно до центральної граничної теореми будуть розподілені нормально [9]. У ході експериментальних досліджень було встановлено, що вибіркове середнє для $E_P[n]$ незалежно від значення P становить близько 0,216. Вибіркове середньоквадратичне відхилення (СКВ) у разі збільшення P удвічі зменшується в середньому у $\sqrt{2}$ разів. Тоді значення порога можна записати в такому вигляді:

$$\gamma \approx 0,216 - 0,0245\beta\sqrt{\frac{40}{P}}, \tag{3}$$

де β − значення квантиля стандартного нормального розподілу. За $\beta = 3$ ймовірність того, що значення шумового відліку буде нижче значення порога, становитиме 0,00135, а за $\beta = 4$− лише 0,00003. Коефіцієнт перед β (0,0245) відповідає значенню СКВ для $P = 40$.

У разі $P < 30$ розраховане за виразом (3) значення порога буде дещо заниженим через відхилення розподілу значень $E_P[n]$ від нормального в бік розподілу χ^2, у якого правий хвіст є більш тяжким.

На рис. 3 наведено етапи порогового оброблення прийнятої реалізації для таких значень деяких параметрів моделі (1): тривалість частотного елемента $T_h = 40$ мкс, тривалість перехідної ділянки $T_{tr} = 0,2T_h = 8$ мкс, $A_{\min}/A_{\max} = 0,7$. Частота дискретизації в цьому разі становила $F_s = 80$ МГц. Значення порога було розраховано за виразом (3) для $\beta = 4$ і $P = 200$. На рис. 3а показано обвідну (Envelope), обвідну після фільтра ковзного середнього (Filtered Envelope) та поріг (Threshold) для випадку, коли в прийнятій реалізації міститься один шум. На рис. 3б відображено випадок порогового оброблення, коли в прийнятій реалізації міститься лише сигнал, а на рис. 3 в, 3 г − сигнал із

завмиранням Релея у разі ВСШ 80 дБ і 0 дБ відповідно. У правому верхньому куті рис. 3 б, 3 в наведено у збільшеному вигляді ділянку переходу між першим та другим частотними елементами. Межі частотних елементів визначають як точки перетину ділянки наростання згладженої обвідної з порогом.

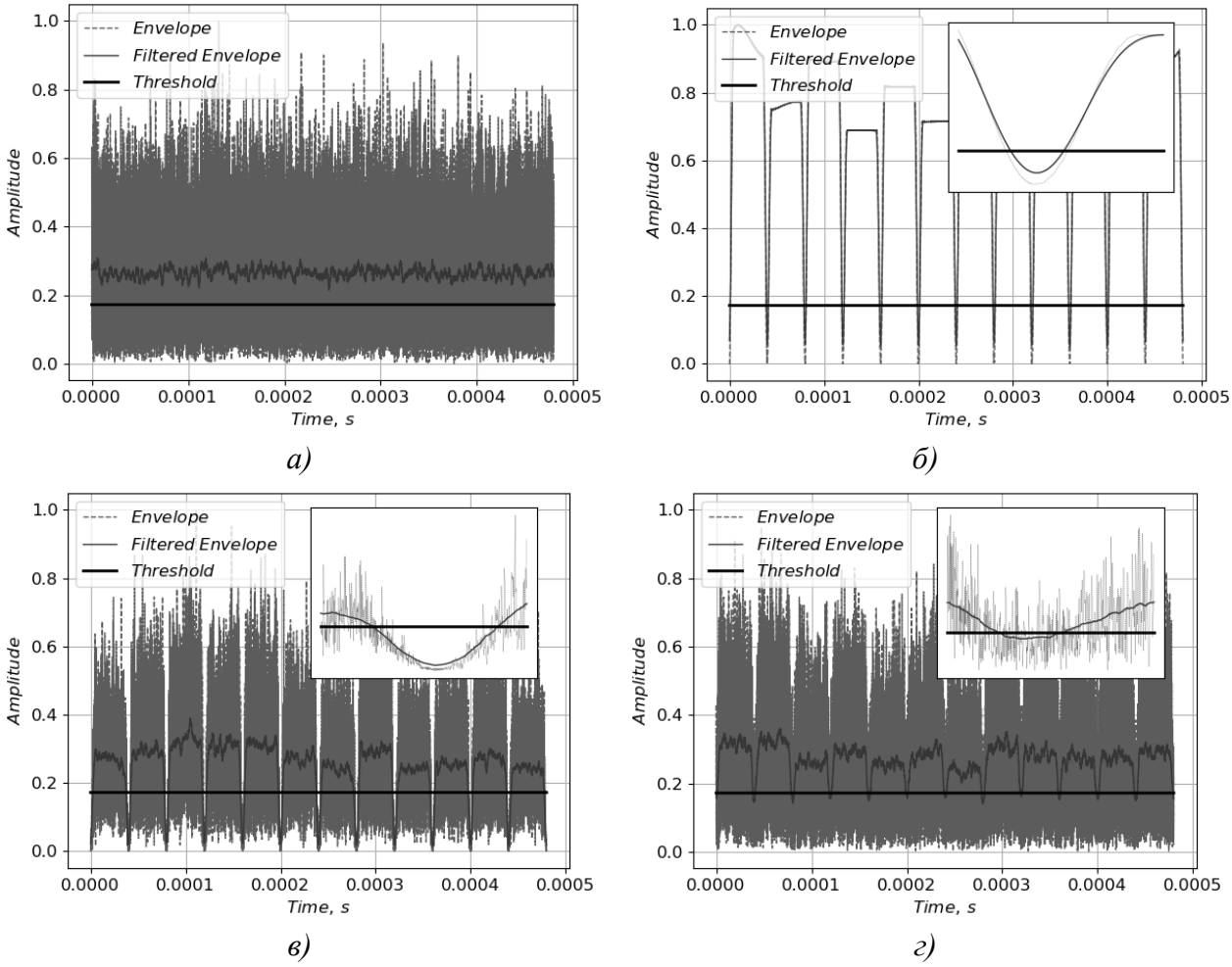


Рис. 3. Порогове оброблення комплексної обвідної для визначення часових меж частотних елементів

Якщо відомо, що ВСШ є високим, то значення довжини вікна згладжування P можна обирати в межах 20−40. Здатність запропонованого підходу до визначення часових меж частотних елементів залежить від кількості відліків прийнятої реалізації $x[n]$, які містяться в одному частотному елементові: у разі збільшення частоти дискретизації для розрізнення окремих частотних елементів необхідне менше значення ВСШ. Запропонований підхід до встановлення часових меж частотних елементів не потребує жодної апріорної інформації про сигнал.

Для визначення частот частотних елементів f_{ri} будемо використовувати незгладжені періодограмні оцінки. Значення відліків спектральної щільності потужності (СЩП) розрахуємо відповідно до такого виразу:

$$X_w[k] = \left| \sum_{n=1}^{N} x[n] w[n] \exp\left(-j2\pi k \frac{n}{N} \right) \right|^2, \; 0 \le k \le N-1, \tag{4}$$

де $w[n]$ − відліки віконної функції довжиною N.

Дискретний спектр (4) розраховуємо для частот kF_s/N. Тоді максимальна помилка оцінювання частоти буде для випадку розташування частоти гармонічного сигналу посередині між двома дискретними частотами і становитиме $kF_s/(2N)$.

Для підвищення точності визначення частоти за фіксованої довжини вікна аналізу ШПФ будемо використовувати експоненціальну екстраполяцію дискретного спектра потужності. Тоді значення частоти сигналу може бути обчислене за таким виразом [10]:

$$f_m = \frac{F_s}{N}\left(k_m + \frac{\ln\left(\frac{X_w[k_m+1]}{X_w[k_m-1]}\right)}{2\ln\left(\frac{X_w[k_m]^2}{X_w[k_m+1]X_w[k_m-1]}\right)}\right),\ 0 \le k \le N-1, \qquad (5)$$

де k_m – номер максимального відліку СЩП;

$X_w[k_m]$, $X_w[k_m - 1]$, $X_w[k_m + 1]$ – значення максимального та двох сусідніх відліків СЩП.

Необхідною умовою застосування даного підходу є те, що мінімальна ширина піка спектра гармонічного сигналу повинна становити 3 частотні відліки. Для цього застосовують попереднє оброблення сигналу експоненціальним вікном:

$$w[n] = \exp\left(-\frac{1}{2}\left(\alpha\frac{n-0,5N}{N-1}\right)^2\right),\ n \in [0, N-1], \qquad (6)$$

де $\alpha = 3..8$ – параметр вікна, у разі збільшення значення якого помилка оцінювання частоти зменшується.

Для визначення кроку сітки частот Δf та рознесення частот ЧМн ΔF необхідно проаналізувати не менше ніж N_h частотних елементів. Якщо ж кількість прийнятих частотних елементів становить $N_r < N_h$, то однозначно встановити значення Δf і ΔF досить складно.

Розглянемо випадок ЧМн-2. Якщо в прийнятій реалізації міститься $N_r = N_h$ унікальних частотних елементів, які утворюють масив $\mathbf{f_r} = (f_{r1}, f_{r2}, f_{r3}, \ldots, f_{rNh})$, то для визначення параметрів Δf і ΔF відсортуємо $\mathbf{f_r}$ за зростанням і розрахуємо значення різниць *diff* (f_{ri}) між кожним наступним і попереднім елементом даного масиву. У результаті виконання вказаних операцій отримаємо три набори чисел: $\Delta f - \Delta F$, Δf і $\Delta f + \Delta F$.

На рис. 4 наведено гістограму значень *diff* (f_{ri}) для $N_r = N_h = 3120$, Δf = 12,5 кГц, ΔF = 8,33 кГц, кожен інформаційний символ розбивається на $L = 3$ частотні елементи. Через те, що сигнал приймається на фоні адитивного шуму і завмирань Релея, оцінки значень *diff* (f_{ri}) будуть отримані з похибками і кожне значення зосереджуватиметься в деякій області (рис. 4). Тому для отримання оцінок Δf і ΔF на гістограмі визначено поріг (3...5). У межах значень, що перевищують даний поріг, розраховують середні значення для *diff* (f_{ri}), які і приймаються за значення шуканих частот. У загальному випадку кількість мод у гістограмі становить $2M - 1$, а їх очікувані значення – $\Delta f \pm m\Delta F$, m=0..$M - 1$. Отже, за формою гістограми можна оцінити кратність ЧМн.

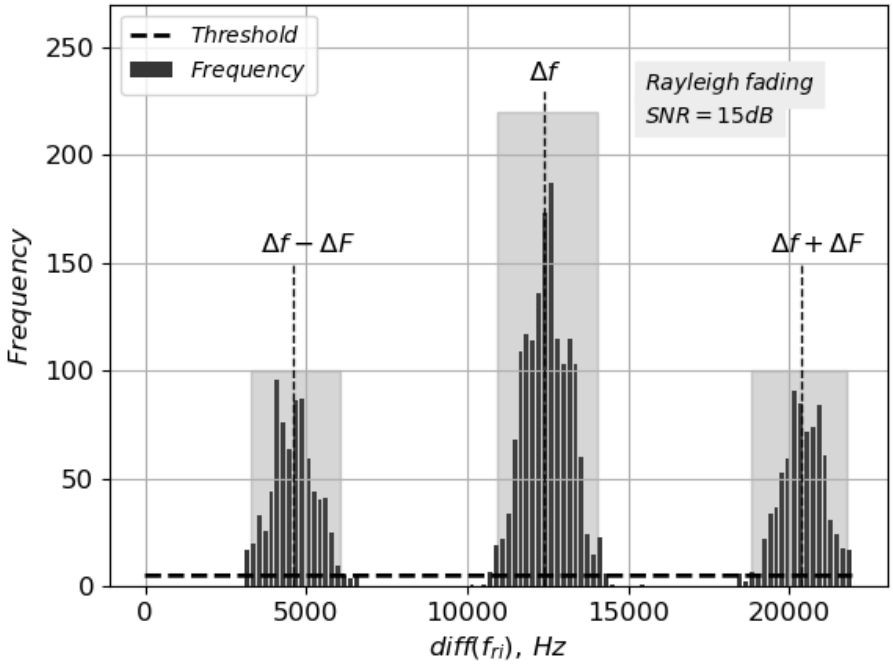
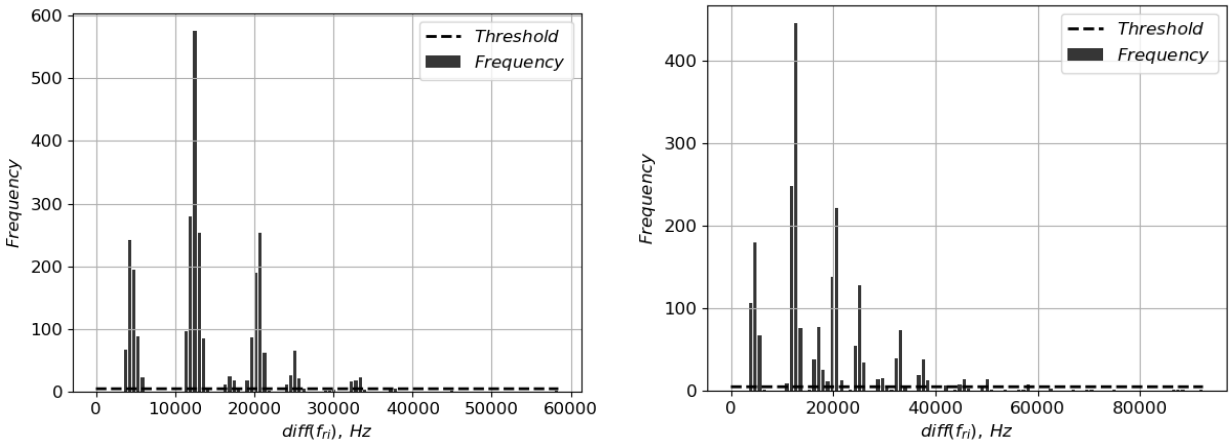


Рис. 4. Гістограма значень параметрів $\Delta f - \Delta F$, Δf і $\Delta f + \Delta F$ для $N_r = N_h$

Якщо кількість прийнятих частотних елементів $N_r > N_h$, то форма гістограми буде аналогічною до випадку $N_r = N_h$. Якщо $N_r < N_h$, то кількість різних значень $diff\,(f_{ri})$ буде більшою, ніж для попередніх випадків. На рис. 5а наведено гістограму для $diff\,(f_{ri})$, коли прийнято 90% частотних каналів, а на рис. 5б − 70%. Очевидно, що в разі малих співвідношень N_r / N_h однозначно оцінити параметри Δf, ΔF та M досить складно.



а) *б)*

Рис. 5. Гістограма значень різниць відсортованого вектора прийнятих частот для N_r / N_h = 0,9 (а) та N_r / N_h = 0,7 (б)

Наближену оцінку кількості частотних каналів можна отримати за таким виразом:

$$N_h \approx \frac{\max(\mathbf{f_r}) - \min(\mathbf{f_r})}{\Delta f}. \qquad (7)$$

Передавання символів у разі ЧМн здійснюється, як правило, на ортогональних частотах, тому наближено можна вважати, що символьна швидкість становить $R_s \approx \Delta F$,

тобто тривалість символа $T_s \approx 1/\Delta F$. Кількість частотних елементів L, на які розбивається інформаційний символ, можна оцінити за таким виразом:

$$L = \lfloor T_s / T_h \rceil = \lfloor 1_s / (T_h \Delta F) \rceil, \tag{8}$$

де $\lfloor . \rceil$ – знак округлення до найближчого цілого.

Тоді після уточнення оцінка символьної швидкості становитиме

$$R_s = 1/(T_h L). \tag{9}$$

Швидкість передавання даних (інформаційних та службових бітів) можна оцінити, враховуючи кратність модуляції M та уточнене значення тривалості символа LT_h:

$$R_d = \log_2 M/(LT_h). \tag{10}$$

Швидкість передавання інформації R_I можна встановити лише після демодуляції сигналу та аналізу бітових потоків, у результаті якого можна визначити структуру кадрів і кількість службових та інформаційних бітів. Тому за розрахованим значенням R_d можна лише наближено оцінити R_I і порівняти її з відповідним значенням для відомих радіостанцій.

Отже, метод оцінювання параметрів сигналу зі швидкою ППРЧ полягає в послідовному виконанні таких операцій: визначення часових меж частотних елементів, оцінювання значень вектора частот $\mathbf{f_r}$ і тривалості частотного елемента T_h, розрахунок параметрів і характеристик радіопередачі (Δf, ΔF, M, N_h, R_s) . Якщо у прийнятій реалізації містяться вузькосмугові або імпульсні перешкоди, то їх доцільно попередньо видалити із використанням методу, описаного в [7].

3. Дослідження розробленого методу та обговорення результатів

Дослідження розробленого методу проведемо шляхом математичного моделювання процесу визначення параметрів і характеристик радіосигналів та статистичного оброблення результатів вимірювань. Параметри радіосигналу зі швидкою ППРЧ наведено у табл. 1. Значення ВСШ змінювалося при цьому в діапазоні від 5 до 30 дБ з кроком 5 дБ. Дослідженню підлягали значення відносних помилок визначення тривалості частотного елемента, кроку сітки частот, кількості частотних каналів та швидкості передачі даних.

Таблиця 1

Значення параметрів радіосигналу в ході моделювання

Параметр	T_h, мкс	Δf, кГц	ΔF, кГц	δ	M	L	N_h	F_s, МГц	$\frac{A_{min}}{A_{max}}$
Значення	40	12,5	8,33	0,2	2	3	3120	80	0,7

Відносну похибку вимірювання тривалості частотного елемента визначатимемо за таким виразом:

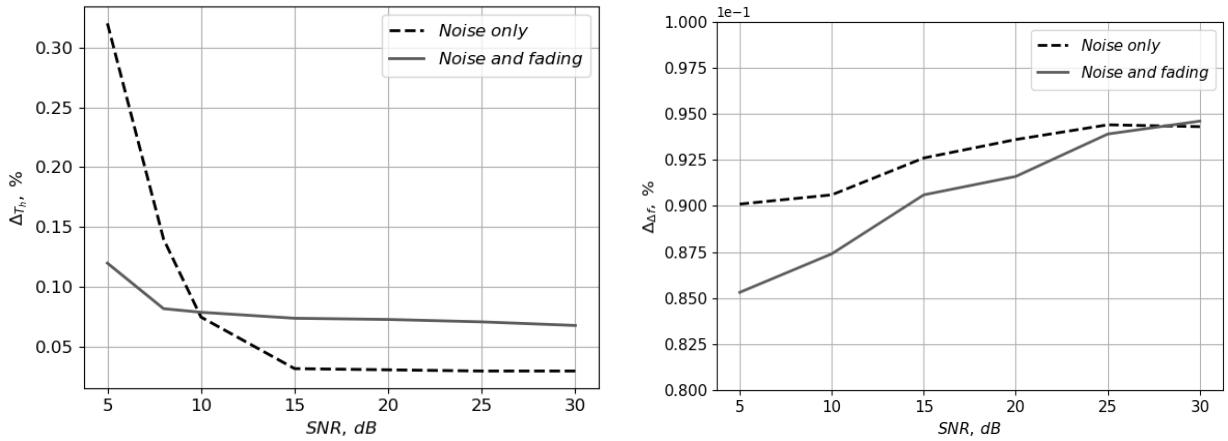
$$\Delta_{T_h} = \frac{1}{T_h N_T} \sum_{i=1}^{N_T} \left| T_h - \hat{T}_{hi} \right| \cdot 100\%, \tag{11}$$

де N_T − кількість частотних елементів, за якими проводилося вимірювання;

$\hat{T}_{hi}$ − оцінка значення тривалості *i*-го частотного елемента.

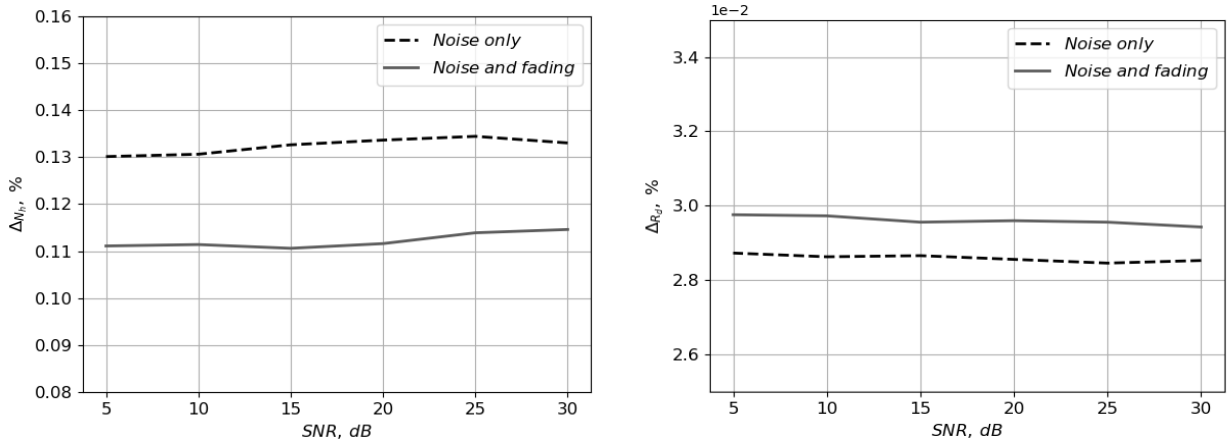
Аналогічно розраховуються значення відносних помилок для інших параметрів.

На рис. 6а наведено залежність значення відносної помилки вимірювання тривалості частотного елемента від ВСШ для випадків оброблення сигналу на фоні шуму (пунктирна лінія) та на фоні шуму із завмираннями Релея (суцільна лінія). Втрати за рахунок завмирання Релея становлять близько 5 дБ (в еквіваленті ВСШ). За значень ВСШ менше 10 дБ похибка оцінювання T_h є меншою для каналів із завмираннями, а більше 10 дБ – навпаки. Це пояснюється особливостями підходу до визначення даного параметра. Варто зауважити, що значення тривалості частотного елемента можна оцінити також для випадків $N_r < N_h$. На рис. 6б показано залежність відносної помилки оцінювання кроку сітки частот від ВСШ. Незначне зменшення цієї помилки в разі зменшення ВСШ можна пояснити тим, що за вищого рівня шуму помилки вимірювання значення частоти окремих частотних елементів через обмежену роздільну здатність ШПФ стають менш корельованими, а в разі їх усереднення помилка оцінювання кроку сітки частот дещо знижується.



а) *б)*

Рис. 6. Залежність відносної помилки вимірювання тривалості частотного елемента (а) та кроку сітки частот (б) від ВСШ



а) *б)*

Рис. 7. Залежність відносної помилки визначення кількості частотних каналів (а) та швидкості передачі даних (б) від ВСШ

На рис. 7а наведено залежність відносної помилки оцінювання кількості частотних каналів, а на рис. 7б – швидкості передавання даних від ВСШ. З наведених графіків видно, що точність визначення вказаних параметрів практично не залежить від значення ВСШ. Це пов'язано з тим, що вони розраховуються (вирази (7), (10)) на основі оцінок виміряних параметрів, помилки оцінювання яких не перевищують 0,3%.

Аналіз рис. 6–7 показує, що в діапазоні значень ВСШ 5−30 дБ відносні помилки оцінювання значень параметрів сигналів не перевищують 0,3%, що дозволить проводити ідентифікацію радіостанцій зі швидкою ППРЧ та ЧМн. Оцінювання параметрів у разі нижчих значень ВСШ за рахунок застосування довгих вікон ШПФ є досить проблематичним, оскільки сусідні частотні елементи не будуть розділятися.

Висновки. Наукова новизна запропонованого методу полягає в розроблених підходах до визначення часових меж частотних елементів на основі порогового оброблення комплексної обвідної та оцінювання кроку сітки частот, рознесення частот і кратності ЧМн на основі аналізу гістограми різниць відсортованого масиву частот частотних елементів. Запропонований метод забезпечує оцінювання значень параметрів сигналів із відносною помилкою, що не перевищує 0,3%, за значень ВСШ не нижче 5 дБ. Достовірність отриманих наукових результатів підтверджується результатами математичного моделювання. Отримані результати можуть бути використані для розроблення алгоритмів демодуляції радіосигналів зі швидкою ППРЧ.

Перспективи подальших досліджень пов'язані з розробленням методів ідентифікації та демодуляції радіосигналів зі швидкою ППРЧ та іншими видами смугової модуляції.

СПИСОК ЛІТЕРАТУРИ

1. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты : Монография. Санкт-Петербург : Свое издательство, 2013. 166 с.

2. Кувшинов О. В., Гурський Т. Г., Гриценок К. М., Шишацький А. В. Аналіз режимів роботи та перспектив бойового застосування сучасних військових УКХ радіостанцій іноземного виробництва // Зб. наук. праць. Київ : ВІТІ, 2018. № 1. С. 43−50.

3. Hamed H. F., Abdullah A. K., Al-waisaw S. Frequency Hopping Spread Spectrum Recognition Based on Discrete Fourier Transform and Skewness and Kurtosis // International Journal of Applied Engineering Research, 2018. Vol. 13, N. 9. P. 7081–7085.

4. Lei Z., Yang P., Zheng L. Detection and Frequency Estimation of Frequency Hopping Spread Spectrum Signals Based on Channelized Modulated Wideband Converters // Electronics, 2018. N 7 (170). P. 1–18. DOI:10.3390/electronics7090170.

5. Wan J., Zhang D., Xu W., Guo Q. Parameter Estimation of Multi Frequency Hopping Signals Based on Space-Time-Frequency Distribution // Symmetry. 2019. N 11 (648). P. 1–18. Doi:10.3390/sym11050648.

6. Горшков Д. В., Мещеряков Ю. Ю., Токарев А. Б. Экспресс-тест наличия в диапазоне частот сигналов с ППРЧ при панорамной обработке данных системой радиомониторинга // Вестник Воронежского ин-та. 2018. № 2. С. 124−132.

7. Бугайов М. В. Частотно-часовий матричний метод виявлення радіосигналів зі стрибкоподібною зміною робочої частоти в складній сигнальній обстановці // Вчені записки Таврійського нац.. ун-ту ім. В. І. Вернадського. Серія: Технічні науки. Херсон : Вид. дім "Гельветика", 2019. Т. 30 (69), № 3, Ч. 1. С. 61−65.
8. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е испр. ; пер. с англ. Москва : Изд. дом «Вильямс», 2007. 1104 с.
9. Горбань І. І. Теорія ймовірностей і математична статистика для наукових працівників та інженерів. Київ : НАНУ, 2003. 244 с.
10. Gasior M., Gonzalez J. L. Improving FFT frequency measurement resolution by parabolic and gaussian interpolation // AB-Note-2004-021 BDI. Geneva, 2004. P. 1–18.

Подано 17.10.2019

Н. В. Бугаёв, Б. В. Молодецкий, И. О. Михайлюк, В. В. Гордейчук

МЕТОД ОЦЕНИВАНИЯ ПАРАМЕТРОВ СИГНАЛОВ РАДИОСТАНЦИЙ С БЫСТРОЙ ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТЫ

Современные средства радиосвязи специального назначения используют режим сверхкороткой пакетной передачи с быстрой псевдослучайной перестройкой рабочей частоты и частотной манипуляцией. Идентификацию таких радиостанций предложено осуществлять путем оценки скорости перестройки частоты и передачи информации, количества частотных каналов и шага сетки частот принятых радиосигналов и сравнения полученных значений с соответствующими характеристиками известных радиостанций с быстрой псевдослучайной перестройкой рабочей частоты. Временные границы и продолжительность частотных элементов рассчитывают по комплексной огибающей принимаемого сигнала. Для этого разработан соответствующий метод, заключающийся в фильтрации огибающей с помощью окна со скользящим средним для подавления шумовой составляющей и пороговой обработки. Частоты частотных элементов определяются по несглаженным периодограммным оценкам, а для повышения точности определения частоты использована экспоненциальная экстраполяция дискретного спектра мощности. Показано, что для однозначного определения шага сетки частот и разноса частот частотной манипуляции необходимо проанализировать количество частотных элементов, не меньше количества частотных каналов. Путем анализа гистограммы разностей отсортированного по возрастанию вектора частот частотных элементов определяют шаг сетки частот, разнос частот и кратность частотной манипуляции. Приближенную оценку количества частотных каналов вычисляют как отношение размаха вектора частот частотных элементов к шагу сетки частот. Скорость передачи информации можно установить только после демодуляции сигнала и анализа битных потоков, в результате которого можно определить структуру кадров и количество служебных и информационных битов. Предложенный метод обеспечивает оценки значений параметров сигналов с относительной ошибкой, не превышающей 0,3%, при значениях отношения сигнал-шум выше 5 дБ.

***Ключевые слова**: псевдослучайная перестройка рабочей частоты, идентификация, частотный канал, частотный элемент, информационный символ, частотная манипуляция.*

M. V. Buhaiov, B. V. Molodetsky, I. O. Mykhailiuk, V. V. Hordiichuk

METHOD OF SIGNAL PARAMETERS ESTIMATION OF RADIOSTATIONS WITH FAST FREQUENCY HOPPING SPREAD SPECTRUM

Modern special-purpose radios utilize ultra-short burst mode with frequency hopping spread spectrum. Such digital radios operate, as a rule, in the fast frequency hopping spread spectrum mode and use a considerable number of frequency channels with frequency separation between adjacent channels, which is significantly less than the spectrum width of the frequency element. The main modulation in such radios is frequency manipulation. The identification of signals with fast frequency hopping spread spectrum and frequency manipulation is performed by estimating the speed of frequency tuning, the speed of information transmission, the number of frequency channels and the step of the frequency grid and comparing the obtained values with the corresponding characteristics of known radio stations with fast frequency hopping spread spectrum. The time limits and the duration of the frequency elements are calculated by the envelope of the received signal. For this purpose, a suitable method has been developed, which consists in filtering the envelope by means of a moving average window for suppression of the noise component and threshold processing. The threshold value is selected by the given probability of its exceeding by noise sample. The proposed approach to determining the time limits of frequency elements does not require any a priori signal information. To determine the frequencies of the frequency elements periodogram estimates are used. An exponential extrapolation of the discrete power spectrum was used to increase the frequency resolution at a fixed window length of the fast Fourier transform. It is shown that in order to uniquely determine the step of the frequency grid and the diversity of frequency manipulation frequencies, it is necessary to analyze the number of frequency elements not less than the number of frequency channels. By analyzing the histogram of the differences of sorted frequency vector of the frequency elements, determine the frequency grid, frequency diversity and the multiplicity of frequency manipulation. An approximate estimate of the number of frequency channels is calculated as the ratio of the magnitude of the frequency vector of the frequency elements to the step of the frequency grid. As a rule, symbol transmission at frequency manipulation is carried out at orthogonal frequencies, so it can be roughly assumed that the symbolic speed is equal to the frequency diversity of the frequency manipulation. The baud rate can be set only after signal demodulation and bit stream analysis, which can determine the frame structure and the number of service and information bits. The proposed method provides the estimation of the values of the parameters necessary for the identification of radio stations of signal parameters with a relative error not exceeding 0.3%, with values of signal to noise ratio not lower than 5 dB.

Keywords: *frequency hopping spread spectrum, identification, frequency channel, frequency element, information symbol, frequency manipulation.*

УДК 004.932 DOI: 10.46972/2076-1546.2019.17.03

С. І. Березіна, Ю. О. Гордієнко, О. І. Солонець

АНАЛІЗ ШЛЯХІВ ВИРІШЕННЯ ПРОБЛЕМИ СЕГМЕНТАЦІЇ ВИСОКОТЕКСТУРОВАНИХ ОБ'ЄКТІВ

Підвищення оперативності та достовірності обробки даних аерокосмічного знімання безпосередньо пов'язане з вирішенням завдання автоматизації процесу дешифрування, що досягається мінімізацією зон пошуку, виявленням замаскованих об'єктів та визначенням динаміки змін у районах спостереження. Першочерговим етапом, що визначає якість автоматизованої обробки та результату дешифрування в цілому, є тематичне сегментування зображення, у процесі якого необхідно враховувати наявність значної кількості текстурованих об'єктів. У статті проаналізовано шляхи вирішення проблеми сегментації високотекстурованих об'єктів, які мають великий діапазон зміни можливих значень кольору. Дослідження проводилися щодо виокремлення лісових масивів і поодиноких насаджень від луки, степу тощо, які мають аналогічні колірні характеристики, але відрізняються текстурою, а також житлових масивів від лісових, яким притаманні однакові розміри зерна текстури та різні колірні характеристики. Досліджено: метод опису текстури, який ґрунтується на обчисленні кількості перепадів яскравості на одиницю площі зображення; метод опису й виміру текстури, що характеризується довжиною серії; методи опису текстури, що базуються на обчисленні їх фрактальної розмірності. Для можливості опису текстури різними методами, у першу чергу, встановлено апертуру вікна аналізу, яка забезпечує відокремлення різних класів об'єктів. Проаналізовані методи опису текстури показали в будь-якому випадку наявність зон помилкової ідентифікації на результуючих зображеннях. Визначено, що найкращий результат отримано в разі використання методу опису й виміру текстури, який ґрунтується на обчисленні кількості перепадів яскравості на одиницю площі зображення, та методу опису текстури на основі обчислення її фрактальної розмірності за методом знаходження площі піраміди покриття фрагмента зображення. Для отримання більш точної сегментної карти зображення, яке містить високотекстуровані фрагменти, запропоновано комплексування двох зазначених методів.

Ключові слова: *сегментування зображення; дешифрування зображення; кластеризація колірного простору; текстурні ознаки; контуропідкреслювальні фільтри; поле фрактальної розмірності.*

Постановка проблеми в загальному вигляді. Для ведення бойових дій у сучасних умовах потрібна висока інформативність розвідувальних даних, яка забезпечується формуванням цифрових зображень з високою просторовою розрізненністю. Це призводить до значного зростання обсягу оброблюваної інформації. Автоматизація процесу дешифрування знімків дозволяє підвищити оперативність та достовірність за рахунок мінімізації зон пошуку, виявлення замаскованих об'єктів та визначення динаміки на знімках. Першочерговим етапом, що визначає якість автоматизованої обробки та

результату дешифрування в цілому, є тематичне сегментування зображення. Для створення автоматизованої системи розпізнавання необхідно враховувати наявність на космічних та аерознімках великої кількості текстурованих об'єктів, які є найбільш складними для процесу побудови сегментної карти. Тому актуальним стає завдання розв'язання проблеми сегментації високотекстурованих об'єктів.

Аналіз останніх досліджень і публікацій. Існує багато методів сегментування зображення, які ґрунтуються на базових властивостях сигналу: яскравості, однорідності та розривності, – що орієнтовані на різні властивості розбиття. Згідно з класифікацією Скарбека й Кошана, усі ці методи розділені на такі групи [1, 2]:

1) методи на основі властивостей пікселя: кластеризація в кольоровому просторі; порогова обробка гістограми; нечітка кластеризація в кольоровому просторі;

2) методи на основі властивостей області: вирощування регіонів; дроблення-злиття ділянок;

3) методи на основі виділення меж: глобальні, локальні.

Методи на основі властивостей пікселя ґрунтуються на тому, що кожен піксель зображення однозначно характеризується просторовими координатами і значенням складових кольору $F_{RGB}(x,y,r,g,b)$ у колірному просторі RGB та $F_{HSV}(x,y,h,s,v)$ у колірному просторі HSV:

$$F_{HSV}(x,y,h,s,v) = \Phi\left(F_{RGB}(x,y,r,g,b)\right),$$

де $\Phi\left(F_{RGB}(x,y,r,g,b)\right)$ – функція перерахунку з колірної моделі RGB у колірну модель HSV.

Уході проведення сегментації правило прийняття рішення про віднесення пікселя до певного класу для колірного простору RGB буде виглядати таким чином [3]:

$$\begin{cases} \left(|r_0 - r| < \delta r \wedge |g_0 - g| < \delta g \ \wedge |b_0 - b| < \delta b\right) \Rightarrow F(x,y,r,g,b) \in A_0; \\ \left(|r_0 - r| > \delta r \vee \ |g_0 - g| > \delta g \vee |b_0 - b| > \delta b\right) \ \Rightarrow F(x,y,r,g,b) \in A_1, \end{cases} \quad (1)$$

де A_0 – піксель зображення належить об'єкту певного класу;

A_1 – піксель зображення не належить до цього класу об'єкта;

r_0, g_0, b_0 – математичні сподівання значення інтенсивності червоного, синього і зеленого кольорів еталонного зображення об'єкта;

$\delta r, \delta g, \delta b$ – допустимі відхилення від еталонного значення.

У разі використання колірного простору HSV правило набирає такого вигляду [3]:

$$\begin{cases} \left(|h_0 - h| < \delta h \wedge |s_0 - s| < \delta s \ \wedge |v_0 - v| < \delta v\right) \Rightarrow F(x,y,h,s,v) \in A_0; \\ \left(|h_0 - h| > \delta h \vee \ |s_0 - s| > \delta s \vee |v_0 - v| > \delta v\right) \ \Rightarrow F(x,y,h,s,v) \in A_1, \end{cases} \quad (2)$$

де h_0, s_0, v_0 – математичні сподівання значень тону, насиченості та яскравості еталонного зображення;

δh, δs, δv – допустимі відхилення від еталонного значення.

Тоді результатом кластеризації буде квантування кольору для зображення [4].

Труднощі використання методів сегментації даної групи пов'язані з виділенням текстурованих об'єктів, які мають великий діапазон можливих значень кольору. Для знімків земної поверхні це виокремлення лісових масивів і поодиноких насаджень від луки, степу тощо, які мають аналогічні колірні характеристики, але відрізняються текстурою. На рис. 1–2 наведено знімки, на яких проводилися дослідження (рис. 1) та гістограми розподілу колірних характеристик (рис. 2). Результат кластеризації за правилами (1), (2) наведено на рис. 3.

Рис. 1. Знімки, на яких проводились дослідження

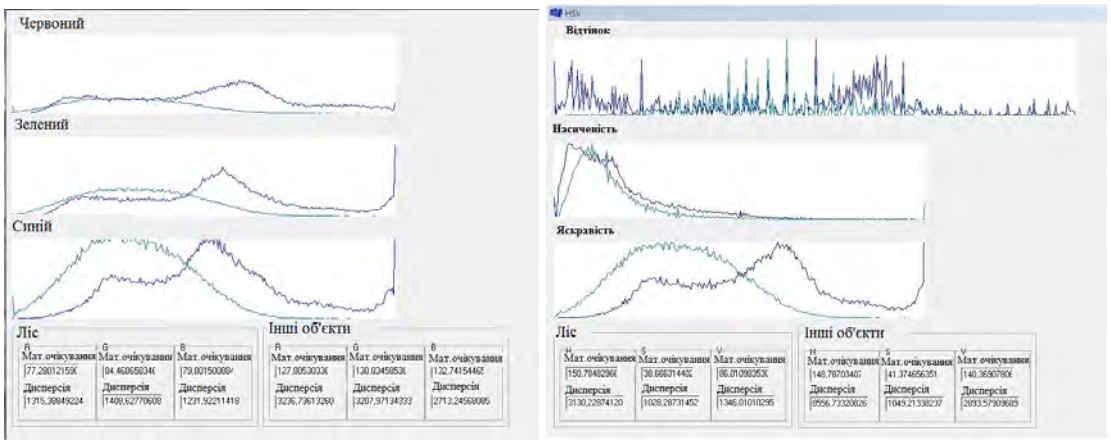
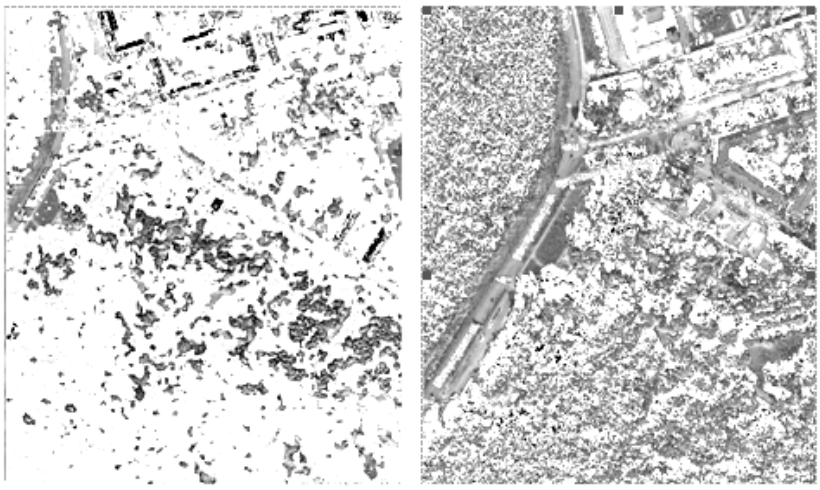


Рис. 2. Гістограми розподілу характеристик кольору (RGB) та (HSV)



а) *б)*

Рис. 3. Результат виділення лісових масивів на підставі колірних характеристик: а) використання усього діапазону можливих значень; б) звужений діапазон допустимих значень

Проаналізувавши отримані результати, можна зробити висновок, що діапазон можливих колірних значень пікселів лісових масивів, які належать зображенню, варіюється в широких межах, а отже, використання дешифрувальних ознак, що ґрунтуються на колірних характеристиках досліджуваної зони, не дає прийнятних результатів у разі дешифрування (рис. 3а). Зменшення діапазону допустимих значень дозволяє ліквідувати велику частину помилок першого роду, але пропорційно збільшує кількість помилок другого роду (рис. 3б).

Методи на основі властивостей області враховують просторове розташування точок напряму [5]–[7] для текстурованих об'єктів, але в такому разі не виконуються вимоги до результату сегментації невеликої кількості дрібних «дірок» усередині регіону та до гладкості меж регіонів.

Методи, що ґрунтуються на операторах виділення меж [6], [8], формулюють завдання сегментації як задачу пошуку меж регіонів. Для визначення точки перепаду яскравості застосовується апарат диференціальної геометрії. За наявності зображень текстурованих об'єктів на знімках визначається велика кількість точок, позначених як точки перепаду яскравості, що призводить до значного ускладнення алгоритму визначення меж об'єкта.

Формулювання завдання дослідження. Завданням дослідження є вибір методів автоматичної сегментації зображення для отримання найбільш точної сегментної карти високотекстурованих об'єктів.

Виклад основного матеріалу. Поняття текстури трактується як характер розподілу спектральної яскравості за полем зображення об'єкта, обумовлений взаємним закономірним розташуванням неоднорідних за спектральною яскравістю елементів, що складають об'єкт. Текстура відображає внутрішню будову об'єкта, тобто взаємне положення елементів, що його складають або утворюють поверхню, і їх яскравість. Текстура може передавати впорядковану зміну тону у вигляді геометрично правильних або майже правильних рисунків. Подібну текстуру мають, наприклад, цегляна кладка, кахельне облицювання, спеціально розфарбовані поверхні: шахівниця, пішохідний перехід тощо. Інший тип – стохастична текстура. Вона властива природним об'єктам і, як правило, є наслідком шорсткості спостережуваних об'єктів [9].

Текстурні ознаки за своєю природою залежать від розміру ділянки, на якій вони визначаються. Оскільки текстура – просторова властивість, виміри її ознак повинні бути обмежені областями, що мають відносну однорідність. Тому перш ніж робити спроби виміряти текстуру, необхідно встановити межі області однорідної текстури шляхом спостереження або за допомогою одного з методів автоматичної сегментації зображення.

1. Метод для опису і виміру текстури, який ґрунтується на обчисленні кількості перепадів яскравості на одиницю площі зображення. Розенфельд і Трої запропонували як текстурну ознаку використати кількість перепадів яскравості в околі точки [10]. Спочатку за допомогою деякої системи виявлення перепадів створюється такий контурний препарат $E(j,k)$, що $E(j,k)=1$ для виявленої точки перепаду, інакше $E(j,k)=0$. Зазвичай поріг виявлення встановлюється нижче, ніж у разі виділення граничних точок областей постійної яскравості. Потім формується текстурна ознака:

$$T(j,k)=\left[\frac{1}{(2W+1)^2}\right]\sum_{m=j-W}^{j+W}\sum_{n=k-W}^{k+W}E(m,n),$$

де $2W+1$ – апертура вікна;

$E(m,n)$ – контурний препарат.

Точність обчислення кількості перепадів, а отже, ідентифікація лісових масивів на знімку залежить від обраного контуропідкреслювального фільтра. Найбільш чутливим до перепадів яскравості й таким, що дає необхідну тонку межу, є фільтр Уолліса, який запропонував нелінійний метод виявлення перепадів яскравості на основі гомоморфної обробки зображення [11]. Основна перевага цього детектора перепадів, крім простоти обчислень, полягає в тому, що він не чутливий до мультиплікативних змін рівня яскравості. Результат обробки наведено на рис. 4.

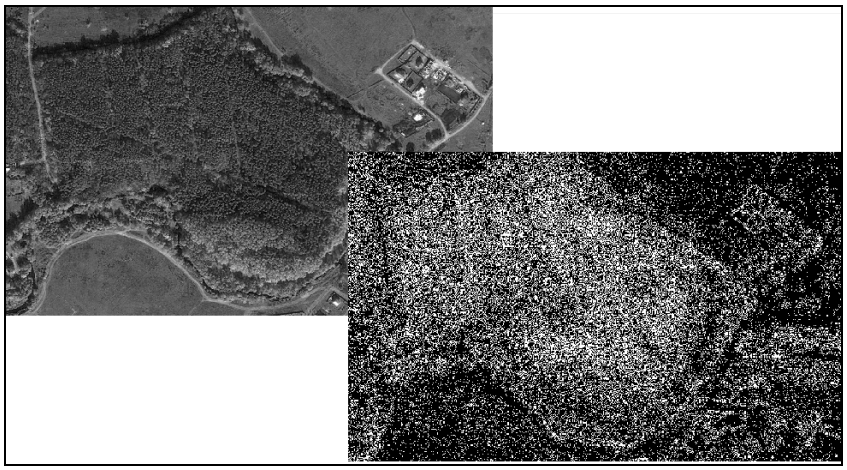


Рис. 4. Результат виявлення перепадів яскравості фільтром Уолліса

У ході реалізації методу на основі обчислення кількості перепадів яскравості на одиницю площі зображення початковий знімок переводився в монохромний. Для компенсації похибки, пов'язаної з умовами освітленості в момент знімання, у результаті проведеного аналізу було прийнято рішення використати 16 градацій яскравості. Перетворення проводилися методом нелінійного підвищення контрасту. У результаті визначення оптимального розміру сканувального вікна був отриманий графік залежності кількості перепадів яскравості від розмірів вікна (рис. 5). Згідно з даними було встановлено, що зона насичення спостерігається у вікні розміром 10 х 10. Результат кластеризації на основі розглянутої текстурної ознаки наведено на рис. 6.

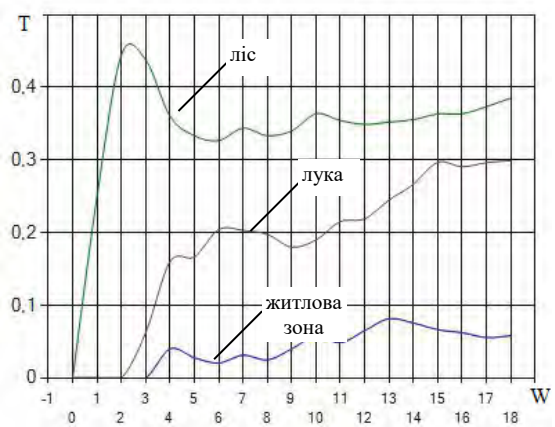
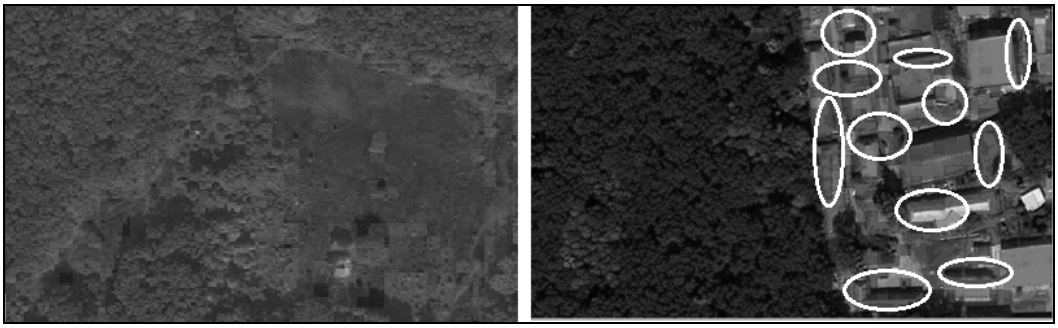


Рис. 5. Залежність кількості перепадів яскравості від розміру вікна



а) *б)*

Рис. 6. Результат визначення на знімку: а) лісу та луки; б) лісу та житлової зони

Результат кластеризації на основі підрахунку кількості перепадів яскравості (рис. 6) дав досить стійке розпізнавання класів «лука» – «ліс», проте суттєві помилки спостерігалися в ході розпізнаванні класів «ліс» – «житлова зона». Білим кольором відзначено зони помилкового виявлення. Отже, розглянутий метод не дозволяє однозначно ідентифікувати зони лісу та лісових насаджень.

2. Метод опису і виміру текстури, що характеризується довжиною серії. Галлоуей запропонував метод виміру текстури, у якому замість гістограм яскравості використовуються гістограми довжин серій [11]. Довжина серії визначається звичайним способом як кількість наступних один за одним у певному напрямі елементів зображення з однаковою яскравістю. У разі грубої текстури виходять довгі серії, а за дрібної – короткі. Для компенсації похибки, пов'язаної з умовами освітленості в момент знімання, у результаті проведеного аналізу було прийнято рішення використати 4 градації яскравості. Побудовану гістограму довжин серій наведено на рис. 7.

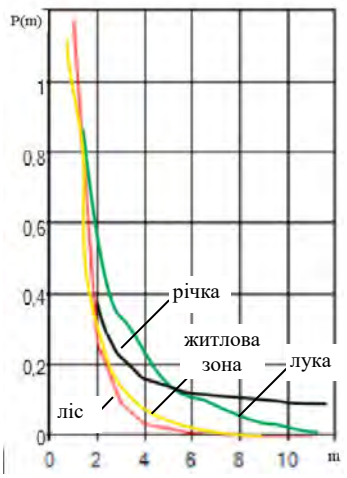


Рис. 7. Гістограма довжин серій

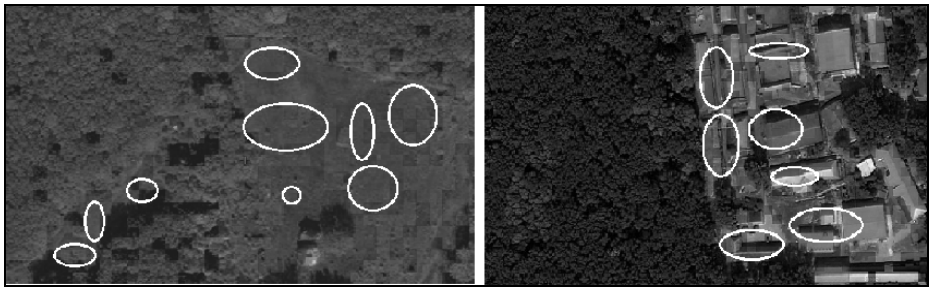
Процес кластеризації проводився на основі розрахунку показника зворотного моменту:

$$\Lambda = \frac{\sum_{n=1}^{N} \frac{m_n}{n^2}}{\sum_{n=1}^{N} m_n},$$

де N – кількість можливих довжин серій;

m_n – кількість серій довжини n.

На результуючих зображеннях так само присутні зони помилкової ідентифікації «ліс» – «лука» та «ліс» – «житлова зона» (рис. 8).

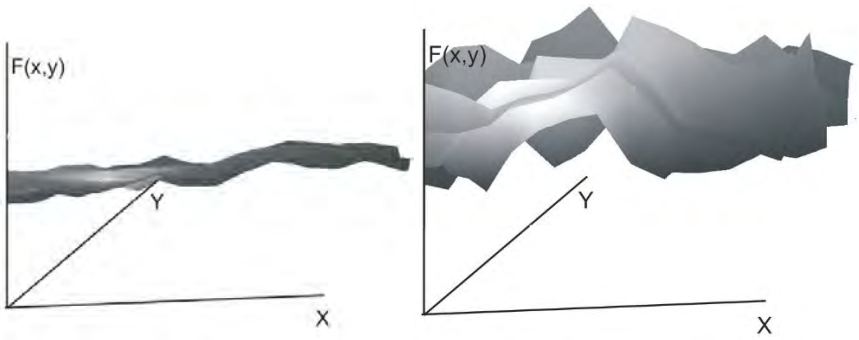


а) *б*

Рис. 8. Результат обробки зображення методом на основі обчислення довжин серій: а) «ліс» – «лука»; б) «ліс» – «житлова зона»

Аналіз отриманих результатів показав, що в разі використання розглянутих методів ідентифікації лісових масивів присутні зони помилкового виявлення.

3. Методи опису текстури на основі обчислення її фрактальної розмірності. Для використання зазначених методів виходять з того, що фрактальна розмірність є дробовою величиною, яка характеризує форму поверхні об'єкта і є показником міри заповнення простору фрактальною структурою. Для фрагмента зображення це неоднорідність заповнення колірного простору (рис. 9). Якщо розглядати ці об'єкти в різному масштабі, то постійно виявляються одні й ті ж фундаментальні елементи, які визначають дробову або фрактальну розмірність структури [12].



а) *б)*

Рис. 9. Заповнення колірного простору фрагментами зображення: а) дороги; б) лісу

За визначенням Б. Мандельброта, об'єкт фрактальний, якщо його розмірність за Хаусдорфом – Безиковичем, тобто фрактальна розмірність, перевищує топологічну та є нецілим числом [12]. Комп'ютерні алгоритми обчислення фрактальної розмірності d зазвичай використовують співвідношення [13]

$$lg\, N(\varepsilon) = lg\, c - d\, lg \frac{1}{\varepsilon} \qquad (3)$$

де c – константа;

ε – апертура вікна.

Існує багато методів визначення $N(\varepsilon)$, застосування яких обумовлюється специфікою поставленого завдання, але усі вони включають підрахунок об'єму або площі фрактальної форми і того, як вона змінюється в масштабах, якщо цей об'єм або форма збільшуються. Як слідує з (3), графік залежності $lg\,N(\varepsilon)$ від $lg\frac{1}{\varepsilon}$ – пряма з кутовим коефіцієнтом *d*. Для визначення невідомих параметрів *c* та *d* (хоча значення *c* зазвичай не становить інтересу) необхідно оцінити $N(\varepsilon)$ для двох розмірів – ε_1 та ε_2:

$$\begin{cases} lg\,N(\varepsilon_1) = lg\,c - d\,lg\frac{1}{\varepsilon_1}; \\ lg\,N(\varepsilon_2) = lg\,c - d\,lg\frac{1}{\varepsilon_2}. \end{cases}$$

Оскільки текстура не є фракталом, величини $N(\varepsilon)$ можуть бути знайдені лише приблизно, розрахунок проводиться для більшої кількості значень ε. Для пошуку значення фрактальної розмірності *d* зазвичай використовують метод найменших квадратів, що забезпечує мінімум суми квадратів відхилень (рис. 10).

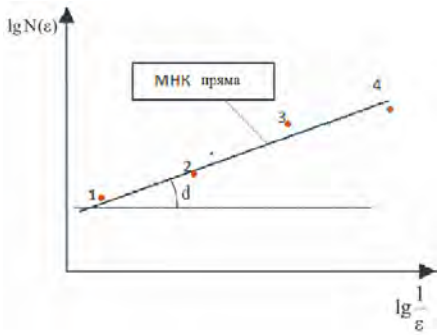
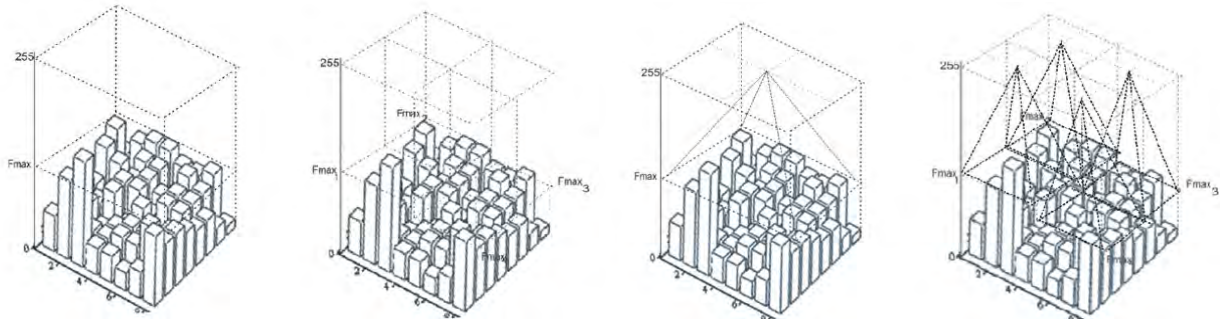


Рис. 10. Визначення фрактальної розмірності за масивом значень

Отже, для підрахунку розмірності необхідно точно задати деякий набір операцій виміру та інтерпретації розмірності. У ході досліджень проводився аналіз методу підрахунку кубів (рис. 11а) та методу знаходження площі піраміди (рис. 11б).



а) *б)*

Рис. 11. Покриття фрагмента зображення за методами: а) підрахунку кубів; б) знаходження площі піраміди

Суть методу підрахунку кубів полягає в тому, що початкове зображення обробляється сканувальним вікном з апертурою, кратною 8. При кожному положенні вікна знаходиться максимальне значення яскравості та визначається дефіцит куба до значення 255 за координатою *z* (яскравість). Потім розмір апертури зменшується в 2 (4) рази, а розрахунки повторюються. На підставі отриманих значень розраховуються $lg\,N(\varepsilon)$ та $lg\frac{1}{\varepsilon}$ (ε – розміри куба, $N(\varepsilon)$ – дефіцит яскравості).

Нахил графіка залежності $lg\,N(\varepsilon)$ від $lg\frac{1}{\varepsilon}$ дає безпосередньо фрактальну розмірність *D*. Для визначення оптимальних розмірів вікна було побудовано графік залежності $lg\,N(\varepsilon)$ від розмірів сканувального вікна (рис. 12).

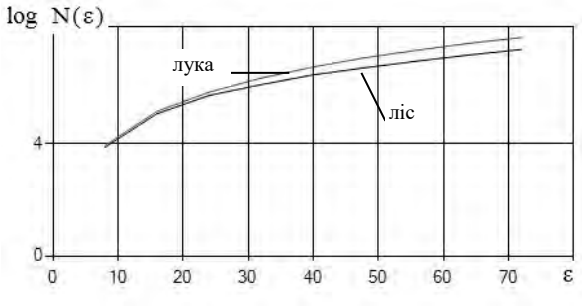


Рис. 12. Графік залежності $lg\,N(\varepsilon)$ від розмірів сканувального вікна

Згідно з графіком (рис. 12) визначено розміри сканувального вікна, за яких об'єкти «лука» – «ліс» різняться та становлять 16 х 16, 24 х 24, 32 х 32. Статистичний аналіз фрактальної розмірності, розрахованої за методом кубів за розміру сканувального вікна 16 х 16, підтвердив можливість її використання для розрізнення класу об'єктів лісових масивів від луки (рис. 13).

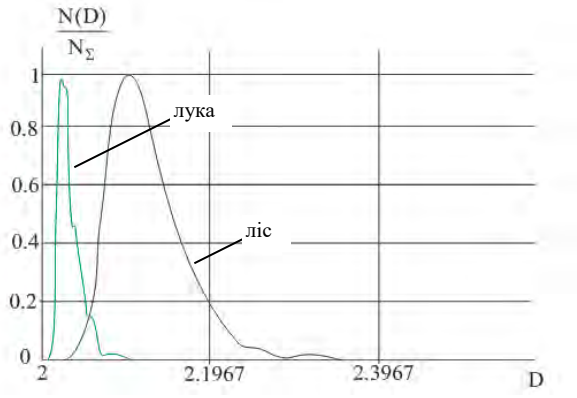


Рис. 13. Графік розкиду значень фрактальної розмірності двох об'єктів («лука» – «ліс»)

Згідно з рис. 13 на знімках ділянки луки та лісу є значення, які знаходяться в зоні невизначеності (2,0277–2,1025). Отже, у результаті розпізнавання виникатимуть незначні помилки 1-го і 2-го роду. Результат обробки зображення наведено на рис. 14, аналіз якого показує, що зони помилкової ідентифікації мають меншу площу, ніж у розглянутих вище методах, однак наявні помилки, пов'язані з ідентифікацією будівель.

Рис. 14. Результат сегментації зображення за методом підрахунку кубів

У разі використання методу піраміди для визначення фрактальної розмірності знаходять значення інтенсивності центрального пікселя в сканувальному вікні та будують піраміду висотою, що дорівнює значенню інтенсивності кольору центрального пікселя, у її основі лежить квадрат, сторона якого дорівнює стороні сканувального вікна. Обчислюють площу бічних площин піраміди, далі повторюють зазначені дії для вікна, поступово зменшуючи його розмір удвічі. Будують графік логарифмічної залежності площі піраміди від розмірів вікна, апроксимують даний графік методом найменших квадратів та визначають кут нахилу даної прямої до площини. Значення фрактальної розмірності зображення розраховують за (3).

Статистичний аналіз фрактальної розмірності, розрахованої за методом піраміди за розмірів сканувального вікна 16 х 16, підтвердив можливість її використання для розділення класу об'єктів лісових масивів від луки (рис. 15).

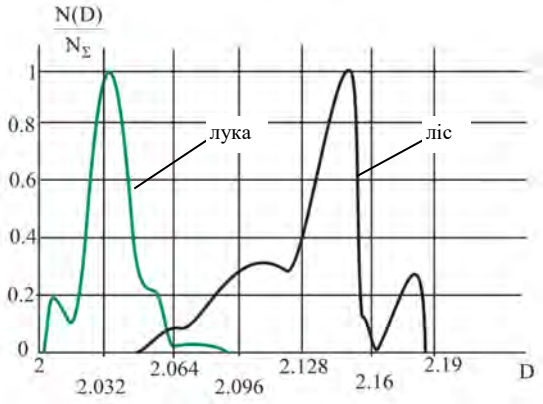


Рис. 15. Графік розкиду значень фрактальної розмірності двох об'єктів («лука» – «ліс»)

Результат обробки зображення наведено на рис. 16 (виділені зони помилкової ідентифікації), аналіз якого показує, що використання фрактальної розмірності, розрахованої за методом призми, дає найкращі результати, але все ж існують незначні зони помилкової ідентифікації.

Окрім зазначених методів опису текстури також проаналізовано можливість використання автокореляційної функції, основними недоліками якої є великій розмір вікна, час на розрахунки та наявність значної кількості помилок правильної ідентифікації текстурованого об'єкта.

Рис. 16. Результат сегментації зображення за методом призми

Результати досліджень показали, що всі проаналізовані методи мають зони помилкового визначення розташування текстурованого об'єкта, тому було прийнято рішення про доцільність комплексування декількох методів. За критерії відбору використовувалися мінімальна апертура сканувального вікна та мінімум помилок ідентифікації. Вибір методів опису текстури об'єктів на знімку здійснювався на підставі методу адитивної згортки критеріїв, який передбачає визначення коефіцієнтів відносної важливості кожного з критеріїв вибору та їх нормалізації, тобто приведення критеріїв до єдиного (безрозмірного) масштабу виміру:

$$A = \min_{i=0...k}\left(\sum_{n} \alpha_n B_n\right),$$

де α_n – відносна важливість критерію;

B_n – нормалізоване значення критерію (розмір апертури та кількість помилок ідентифікації).

Для розрахунку було прийнято, що максимальна оцінка важливості кожного критерію дорівнює 10 балів. Відносна важливість критерію кількості помилок дорівнювала 10, а розміру апертури – 5. На основі важливості критеріїв і кількісної їх оцінки виробляється визначення агрегованих значень варіантів рішень, як суми добутку оцінок, отриманих за погодженими кількісними шкалами, і коефіцієнтів відносної важливості (ваг) кожного з критеріїв. Вибір кращого варіанта здійснюється на основі інтегральної оцінки кожної складової системи. У результаті рекомендовано використовувати методи опису текстури, які ґрунтуються на обчисленні кількості перепадів яскравості на одиницю площі зображення, та розрахунку фрактальної розмірності за методом призми.

Висновки. У зв'язку з тим, що аерокосмічні зображення є сукупністю текстурних областей природного походження і штучних об'єктів із низькою тоновою насиченістю, аналіз методів побудови сегментної карти на підставі колірних ознак пікселей показав, що вони не придатні для виділення текстурованих об'єктів, які мають великий діапазон можливих значень кольору. Для знімків земної поверхні це виокремлення лісових масивів і поодиноких лісових насаджень від луки, степу тощо, які характеризуються аналогічними колірними характеристиками, але відрізняються текстурою. Відповідно виникає необхідність використання текстурних ознак зображення.

Проаналізовані в роботі методи опису текстури показали наявність зон помилкової ідентифікації. Найкращий результат було отримано внаслідок використання методу опису і виміру текстури, який ґрунтується на обчисленні кількості перепадів яскравості на одиницю площі зображення, та методу опису текстури на основі обчислення її фрактальної розмірності за методом знаходження площі піраміди покриття фрагмента зображення. Для отримання більш точної сегментної карти зображення, яке містить текстуровані фрагменти, запропоновано комплексування двох зазначених методів, що є предметом для подальших досліджень.

СПИСОК ЛІТЕРАТУРИ

1. Аналіз відомих методів сегментування зображень, що отримані з бортових систем оптико-електронного спостереження / В. Г. Худов, Г. А. Кучук, О. М. Маковейчук, А. В. Крижний // Системи обробки інформації. 2016. № 9 (146). С. 77–80.

2. Шитова О. В., Пухляк А. М., Дроб Е. М. Анализ методов сегментации текстурных областей изображений в системах обработки изображений // Научные ведомости Белгородского гос. ун-та. 2014. № 8 (179). Вып. 30/1. С. 182–188.

3. Березина С. И., Бутенко О. С., Еременко Д. В. Определение последствий деятельности предприятий, загрязняющих окружающую среду по данным космического мониторинга // Системи обробки інформації. 2014. № 2 (118). С. 237–245.

4. Iris localization based on the Hough transform, a radial-gradient operator, and the gray-level intensity / F. Jan, I. Usman, S. Khan, S. Malik // Optik. 2013. Vol. 124 (23). P. 5976–5985.

5. Nixon M., Aguado A. Feature Extraction and Image Processing // Elsevier Science Linacre House. Jordan Hill, Oxford, 2013. 350 p.

6. Burge M., Kropatsch W. A minimal line property preserving representation of line images // Computing. 1999. Vol. 62, Iss. 4. P. 355–368.

7. Zenzo S., Cinque L., Levialdi S. Run-based algorithms for binary image analysis and processing // IEEE Transactions on Pattern Analysis and Machine Intelligence. 1996. Vol. 18, № 1. P. 83–89.

8. Худов В. Г., Маковейчук О. М. Удосконалений еволюційний метод сегментування багатомасштабної послідовності зображень, отриманих з космічних систем оптико-електронного спостереження // Зб. наук. праць Харків. нац. ун-ту. Повітряних Сил. 2017. № 3 (52). С. 93–97.

9. Krizhevsky A., Sutskever I., Hinton G. Imagenet classification with deep convolutional neural networks // Advances in neural information processing systems. 2012. P. 1097–1105.

10. Long J., Shelhamer E., Darrell T. Fully convolutional networks for semantic segmentation // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2016. Vol. 39, Iss. 4. P. 640–651.

11. Прэтт У. К. Цифровая обработка зображений : в 2-х кн. Москва : Мир, 1982. Кн. 1. 312 с., Кн. 2. 480 с.

12. Таршин В. А., Сотников А. М., Пащенко Р. Э. Метод оперативной подготовки эталонов на основе фрактальной обработки изображений с высокой объектовой насыщенностью // Техническое зрение. 2014. Вип. 1 (5). С. 2–8. URL: http://magazine./

technicalvision.ru/public_ftp/ issue_1(5)/Тех.зрение_1_5__1.pdf (дата обращения: 20.09.2019).
13. Фрактальный анализ процессов, структур и сигналов : коллективная монография / Под ред. Р. Э. Пащенко. Харьков : ХООО «НЭО «Экоперспектива», 2006. 348 с.

Подано 08.11.2019

С. И. Березина, Ю. А. Гордиенко, А. И. Солонец

АНАЛИЗ ПУТЕЙ РЕШЕНИЯ ПРОБЛЕМ СЕГМЕНТАЦИИ ВЫСОКОТЕКСТУРИРОВАННЫХ ОБЪЕКТОВ

Повышение оперативности и достоверности обработки данных аэрокосмических снимков непосредственно связано с решением задачи автоматизации процесса дешифровки, которая достигается минимизацией зон поиска, обнаружения замаскированных объектов и определения динамики изменения в районах наблюдения. Первоочередным этапом, который определяет качество автоматизированной обработки и результатов дешифрования в целом является тематическое сегментирование изображения. В процессе тематического сегментирования изображения необходимо учитывать наличие большого количества текстурированных объектов. В статье проведен анализ путей решения проблемы сегментации высокотекстурированных объектов, которые имеют большой диапазон изменения возможных значений цвета. Исследования проводились относительно выделения лесных массивов и одиночных насаждений от луга, степи и т. п., которые имеют аналогичные цветовые характеристики, но при этом отличаются текстурой, а также жилищных массивов от лесных, которым свойственны одинаковые размеры зерна текстуры и разные цветовые характеристики. Исследованы: метод описания текстуры, основанный на вычислении количества перепадов яркости на единицу площади изображения; метод описания и измерения текстуры, которая характеризуется длиной серии; методы описания текстуры на базе вычисления их фрактальной размерности. Для возможности описания текстуры разными методами, в первую очередь, установлена апертура окна анализа, которая обеспечивает различие разных классов объектов. Проанализированные методы описания текстуры показали во всех случаях наличие зон ошибочной идентификации на результирующих изображениях. Установлено, что наилучший результат получен при использовании метода описания и измерения текстуры, основанного на вычислении количества перепадов яркости на единицу площади изображения, и метода описания текстуры на базе вычисления ее фрактальной размерности по методу нахождения площади пирамиды накрытия фрагмента изображения. Для получения более точной сегментной карты изображения, которая содержит высокотекстурированные фрагменты, предложено комплексирование двух указанных методов.

Ключевые слова: *сегментирование изображений; дешифрирование изображений; кластеризация цветного пространства; текстурные признаки; контуроподобные фильтры; поле фрактальной размерности.*

S. I. Berezina, Yu. O. Gordienko, O. I. Solonets

ANALYSIS OF WAYS OF SOLVING THE SEGMENTATION PROBLEM FOR HIGHLY TEXTURED OBJECTS

Increment of speed and reliability of aerospace images processing is directly related to solution of the task of automation of images interpretation process, which is achieved by minimizing search areas, detecting masked objects and defining the dynamics of changes in surveillance areas. The primary stage that in general determines the quality of results received by automated processing and interpretation is thematic segmentation of the image. In the process of thematic segmentation it is necessary to take into account presence of a large number of textured objects. The paper analyzes the ways of solving the segmentation problem for highly textured objects with large range of variation of possible color values. The research included separation of woodlands and single plants from meadows, steppes, etc., which are characterized by similar color characteristics, but differ in texture. It also included separation of residential areas from forests, which are characterized by the same grain size of texture and different color characteristics. The method of texture description, which is based on calculation of the number of differences in brightness per unit area of the image, the method of description and measurement of texture, characterized by the length of the series, the methods of texture description based on calculation of their fractal dimension have been investigated. In order to describe the texture by different methods, first of all, an aperture of the analysis window was defined. That aperture ensures separation of different classes of objects. The analyzed methods of texture description showed that areas of false identification are always present in the result images. It was determined that the best results were obtained with two of the discussed methods. The first one was the method of texture description and measurement based on calculation of the number of brightness differences per unit area of the image. The second one was the method of texture description based on calculation of fractal dimension by searching the area of the pyramid which covers image fragments. To obtain a more accurate segmented map of an image containing highly textured fragments, a combination of the two methods is suggested.

Keywords: *image segmentation; image interpretation; color space clustering; textural signatures; contouring filters; fractal dimension field.*

УДК 378.1:658.5 DOI: 10.46972/2076-1546.2019.17.04

О. М. Перегуда, О. П. Черкес, П. М. Піонтківський, О. В. Дзюбенко

МЕТОДИКА ВИБОРУ ТА ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ В ДІЯЛЬНІСТЬ ВИЩОГО ВІЙСЬКОВОГО НАВЧАЛЬНОГО ЗАКЛАДУ

У статті визначено проблемні питання вибору та впровадження інформаційної системи у вищому військовому навчальному закладі. Наведено методику у формі методичних рекомендацій для вирішення завдань: опису процесів діяльності, які забезпечують основні спроможності вищого військового навчального закладу; вибору комерційних інформаційних систем та визначення варіантів створення інтегрованої інформаційної системи; розроблення плану заходів з автоматизації діяльності закладу. У ході розроблення методики враховано досвід упровадження засобів автоматизації в комерційній, військовій та освітній сферах. Запропоновано використання процесно-орієнтованого підходу, що дозволяє сформувати системне бачення архітектури організації (установи), визначати керівні, основні процеси освітньої діяльності, процеси забезпечення, що на етапі аналізу є підставою формування функціональних вимог до інформаційної системи, які відповідають потребам вищого військового навчального закладу.

Для проведення аналізу та побудови рейтингу комерційних інформаційних систем обрано кількісний багатокритерійний метод – метод аналізу ієрархій, який дозволяє розв'язувати слабоструктуровані задачі. Для дослідження інформаційних систем проаналізовано та визначено основні критерії, на базі яких приймається рішення, яке якнайкраще задовольнить вищий військовий навчальний заклад.

Вихідними даними є результати опитування експертів у вигляді матриць попарних порівнянь для всіх вузлів ієрархії. Визначення пріоритетності варіантів у ході вибору комерційних інформаційних систем проведено з використанням спеціалізованого програмного забезпечення «MY PRIORITY 1.0». Результати проведеного аналізу можуть бути використані для обґрунтування вибору фірми виробника інформаційних систем.

Особливістю запропонованої методики є комплексність підходу щодо: ідентифікації, формалізованого опису, аналізу та удосконалення процесів діяльності вищого військового навчального закладу; визначення рівня автоматизації, фактичних потреб, особливостей створення та формування вимог до інформаційної системи і засобів автоматизації з орієнтацією на специфічну (військову) спрямованість підготовки у цих закладах.

Ключові слова: *комплексна методика; інформаційна система; вищий військовий навчальний заклад; метод ієрархії.*

Постановка проблеми в загальному вигляді. Розвиток глобальних інформаційно-комунікаційних технологій змінює тенденції впровадження інформаційних систем (ІС) у вищому військовому навчальному закладі (ВВНЗ), відбувається перехід від розробки власних програмних продуктів до придбання комерційних (готових) інтегрованих зразків ІС.

Вибір інтегрованої ІС для ВВНЗ здійснюється в умовах реформування системи військової освіти і підготовки кадрів з урахуванням вимог виконання заходів оборонної реформи, розвитку міжнародної співпраці з метою реалізації стратегічного курсу держави на європейську інтеграцію та євроатлантичне партнерство.

Інтегрована ІС повинна забезпечувати створення єдиного інформаційного освітнього простору, враховувати специфіку організації навчального процесу у військовому закладі вищої освіти (ЗВО) (орієнтуватися на специфіку військового навчання) та повсякденної діяльності, що передбачає виконання завдань житлового, фінансового, тилового, технічного забезпечення.

Проєкт упровадження ІС повинен відповідати стратегічним цілям ВВНЗ. Його метою є не лише автоматизація процесів діловодства, але й підвищення якості оперативного управління та усунення різних організаційно-управлінських протиріч, що, у свою чергу, потребує врахування не тільки поточного стану справ, але і їх стану за минулі періоди часу, а також можливих перспектив розвитку закладу.

У процесі впровадження ІС будь-який навчальний заклад стикається з низкою проблем, оскільки наявні на ринку програмні продукти різноманітні за продуктивністю, масштабами, сферою застосування, вартістю. Кількість факторів, які необхідно враховувати для оптимального вибору та впровадження системи досить велика, що потребує реалізації цілого комплексу різноманітних заходів.

За досвідом створення ІС ЗВО (ВВНЗ) повинна мати: модульну архітектуру, раціональну структуризацію баз даних та інтерфейсів користувача, накопичувально-часовий спосіб зберігання інформації в базі даних, що дозволяє отримати достовірну звітність у будь-який момент часу, визначену функціональність (відповідає специфіці ЗВО чи ВВНЗ) і продуктивність, гнучкість конфігурування інтерфейсів користувачів відповідно до вимог освітньої діяльності, централізоване розмежування повноважень користувачів згідно з вимогами інформаційної безпеки.

Незважаючи на достатньо невеликий різновид ІС, які використовують у ЗВО (порівняно, наприклад, із комерційною чи промисловою галуззю), проблема їх вибору та впровадження залишається достатньо актуальною з таких причин:

процес вибору й упровадження ІС не досить чітко формалізовано та регламентовано, не враховано специфіки діяльності ЗВО та ВВНЗ порівняно з вибором та впровадженням ІС в інших сферах;

не визначено чітких та об’єктивних критеріїв для порівняння ІС для ЗВО (та для ВВНЗ зокрема) між собою, встановлення їх переваг та недоліків;

більшість вимог до ІС ЗВО мають суб’єктивний характер і неформалізований вигляд: думки, міркування, бачення фахівців-експертів у даній галузі;

невизначеність процесу вибору та впровадження ІС не дозволяє чітко спрогнозувати його терміни та обсяги ресурсів, необхідних для цього;

на даний час уже існує велика кількість ІС, які забезпечують часткову автоматизацію діяльності ЗВО (ВВНЗ) та потребують у подальшому інтеграції до єдиної ІС закладу, зокрема забезпечення сумісності ІС різних ЗВО (ВВНЗ), а також інших установ (організацій, органів влади) між собою.

Аналіз останніх досліджень та публікацій. За результатами огляду джерел та узагальнення матеріалів можемо зазначити, що питання обґрунтованого вибору ІС для впровадження в діяльність ВВНЗ розглядається у вузькому контексті. Інформаційне забезпечення управлінської діяльності ЗВО досліджувала Х. В. Середа [1]. Забезпечення навчального процесу вишів інформаційними матеріалами бібліотеки вивчав А. І. Андрухів

[2]. Проблему планування та забезпечення ефективного менеджменту наукових досліджень за допомогою використання електронних інформаційних систем відкритого доступу розкрито в праці А. В. Кільченко [3].

У науково-дослідних роботах під шифрами «Фаркоп», «Діброва-ВНЗ» розроблено методичні основи проєктування автоматизованої системи управління (АСУ) повсякденною діяльністю ВВНЗ, що включають математичні моделі, методики та алгоритми, які доведені до практичної реалізації у вигляді технічного проєкту телекомунікаційної мережі [4].

Різним аспектам оцінювання якості інформаційних систем освітнього призначення присвячені дослідження багатьох сучасних вчених, зокрема, критерії оцінювання електронних освітніх ресурсів досліджувалися М. І. Жалдаком, Г. М. Кравцовим, В. В. Лапінським та іншими.

Формулювання завдання дослідження. Аналіз джерел наукової інформації дозволяє стверджувати про недостатню розробленість визначеної тематики. У наявних дослідженнях комплексно не розглядалося питання вибору та впровадження ІС ВВНЗ (навіть ІС ЗВО), не висвітлювалися особливості організації освітнього процесу в закладах Міністерства оборони України та військових навчальних підрозділах ЗВО України в ході вибору та впровадження ІС, зокрема розглядалася специфіка функціонування спеціалізованих ІС («Дельта», «Дніпро»), які обробляють інформацію з обмеженим доступом та відомості, що становлять державну таємницю.

Метою статті є покращення рівня організаційно-методичного забезпечення процесу впровадження ІС (та інших засобів автоматизації (ЗА)) у діяльність ВВНЗ за рахунок розроблення відповідних методичних рекомендацій, які забезпечать єдиний підхід, визначать структуру та зміст основних етапів щодо: ідентифікації, формалізованого опису, аналізу та удосконалення процесів діяльності закладу; визначення рівня автоматизації, фактичних потреб, особливостей створення та формування вимог до ІС і ЗА для потреб вишу, встановлення порядку та пріоритетності їх упровадження.

Виклад основного матеріалу. Однією з важливих проблем, що виникають під час вибору та впровадження ІС, є нечіткість початкового визначення функціональних вимог до них та постійна зміна, уточнення й модифікація вимог. Доступність різних технологій робить актуальною проблему вибору певного рішення щодо методології, на якій буде ґрунтуватися дослідження [5]. Використання процесно-орієнтованого підходу дає можливість точніше відобразити й охарактеризувати особливості та зміст освітньої діяльності у військовому навчальному закладі в умовах активізації інформаційних потоків. Міжнародні стандарти управління якістю серії 9000, стандарти ISO/IES серії 27001, які визначають систему менеджменту у сфері інформаційної безпеки (СМІБ, англ. Information Security Management System – ISMS), ґрунтуються на процесному підході, коли зміст діяльності описується у вигляді ієрархічної моделі процесів [6]. Тому в основу розроблених методичних рекомендацій покладено процесно-орієнтований підхід, на основі організаційного та процесного аналізу реінжинірингу процесів (побудова моделей типу «ЯК Є»).

Запропоновані методичні рекомендації дозволяють: вирішувати основні завдання проєкту впровадження ІС, такі як опис та аналіз базової («ЯК Є») архітектури ВВНЗ, яка

забезпечує основні спроможності закладу та ґрунтується на відповідних інформаційних й організаційно-технічних елементах; здійснювати опис та аналіз цільової («ЯК МАЄ БУТИ») архітектури ВВНЗ; визначати відмінності між базовою й цільовою архітектурами закладу та формувати план заходів їх дослідження й удосконалення.

Методичні рекомендації пропонують послідовний підхід до дослідження та удосконалення архітектури ВВНЗ, який здійснюється за такими етапами: підготовка до дослідження діяльності закладу; ідентифікація *Процесів* та їх складових; визначення (уточнення) функціонала ІС ЗА; аналіз можливих варіантів автоматизації *Процесів* (впровадження ІС та ЗА); розроблення плану заходів з удосконалення архітектури ВВНЗ; додатковий етап – детальний опис та аналіз *Процесів.*

Для кожного етапу визначають:

основні завдання;

вхідні початкові дані, де зазначено їх найменування та джерело отримання;

обмеження, припущення та особливості виконання етапу;

основні кроки (дії) етапу із зазначенням змісту заходів, вхідної (початкової) інформації для виконання операцій (дій), їх результату, виконавця, посадової особи, яка відповідатиме за контроль;

результати етапу у вигляді переліку розроблених документів та прийнятих рішень.

Етап «Підготовка до проведення дослідження діяльності ВВНЗ» є організаційним, результат його – це документ *«Завдання на дослідження»*, який містить: особливості об’єкта автоматизації; мету та завдання дослідження; склад робочої групи та типові обов’язки категорій осіб, що входять до її складу; календарний план, графік комунікацій.

За обсягом робіт *етап «Ідентифікація Процесів та їх складових»* є достатньо трудомістким. Дослідження починається з одержання загальних відомостей щодо діяльності структурних підрозділів. Не існує стандартного переліку (реєстру) *Процесів* освітніх послуг для ВВНЗ, тому попередньо було складено робочий перелік функціонального призначення тематично згрупованих *Процесів*, виходячи з вимог керівних документів та ґрунтуючись на досвіді інших ЗВО. На цьому етапі роботи виконують ітераційно, використовують метод анкетування експертів, бесіди з фахівцями, метод експертних оцінок, експертним шляхом визначають, уточнюють *Процеси*, підпроцеси. Обговорення результатів проводять за участю представників усіх підрозділів (стейкхолдерів), результати оформлюють у вигляді табл. 1.

Таблиця 1

№ з/п	Назва Процесів	Назва підпроцесів	Реалізація у ВВНЗ	Опис Процесів (підпроцесів), думка експерта для випадків
	Відповідає		***Виконується***	***частково відповідає – виконується, частково відповідає – частково виконується, частково відповідає – не виконується (доцільно впровадити), не відповідає***
	Частково відповідає		***Частково виконується***	
	Не відповідає		***Не виконується (доцільно впровадити)***	
	Не оцінював (не в моїй компетенції)		***Не виконується (відсутня необхідність)***	

Етап «Визначення (уточнення) функціонала ІС та ЗА». З метою визначення (уточнення) функціонала ІС ВВНЗ необхідно виявити особливості реалізації функцій підпроцесів: для керівних *Процесів* (управління розвитком, функціонуванням); основних *Процесів* науково-освітньої діяльності та *Процесів* забезпечення (допоміжних). Приклади опису окремих функцій підпроцесів наведено в переліку *Процесів.* Отже, можна:

визначити першочерговість автоматизації *Процесів* (підпроцесів);

оцінити рівень автоматизації *Процесів* (підпроцесів);

проаналізувати ІС, які використовують у ВВНЗ «ЯК Є»;

визначити функціонал ІС «ЯК МАЄ БУТИ».

На цьому етапі до початку вибору та впровадження нової ІС оцінюють фактичний стан автоматизації ВВНЗ, визначають особливості інформаційної взаємодії закладу.

Визначення (уточнення) функціонала комерційних ІС, його формалізований опис здійснюють шляхом вивчення й аналізу відкритих інформаційних джерел (матеріалів, публікацій, Інтернету, конференцій). У ході аналізу враховують додаткові вимоги до функціонування спеціалізованих ІС «Дельта», «Дніпро», які обробляють інформацію з обмеженим доступом, відомості, що становлять державну таємницю. Перелік ІС, функціонал яких досліджується, визначають за репутацією та досвідом роботи на ринку фірми розробника. Така фільтрація (обмеження) необхідна в умовах недостатньої інформованості. З метою апробації методичних рекомендацій для аналізу функціональних можливостей були обрані відкриті мережеві сервіси, Next Cloud, система дистанційного навчання Національного університету оборони України імені Івана Черняховського, національні та міжнародні науково-освітні комп'ютерні мережі, ІС Сумського державного університету, Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Херсонського державного університету, для яких експерти описують (аналізують) функціонал «ЯК Є» та висловлюють думку «ЯК МОЖЕ БУТИ» [7–9].

Перелік критеріїв, які враховують для вибору ІС, мають різний рівень важливості, тому необхідно зважати на пріоритети різних груп стейкхолдерів.

Особливу увагу слід звернути на таке:

вимоги до безпеки (шифрування, режим доступу та розповсюдження інформації, забезпечення комплексного підходу до організації системи захисту інформації (КСЗІ));

технічні аспекти архітектури (масштабованість, модульний принцип побудови системи з незалежних функціональних блоків із розширенням за рахунок відкритих стандартів API, COM тощо);

рівень інтеграції (брокери, дані, сервіси);

можливість інтеграції з наявними інформаційними системами (якими даними можна здійснювати обмін, забезпечення процедур формалізації, стандартизації даних);

вимоги до обсягів інформації, що зберігається (сховище документів, ієрархічна структура зберігання);

специфічні формати зберігання документів;

засоби пошуку інформації;

спосіб забезпечення обміну інформацією за наявності територіального розподілу підрозділів;

вартість користування (витрати на інсталяцію, супровід впровадження).

Аналіз матеріалів дає можливість одержати необхідні відомості для вибору ІС.

Дослідження методів, в основі яких лежить багатокритерійний вибір, а саме: комплексної оцінки, порівняння з використанням функції корисності та метод аналізу ієрархій – дозволяє підтвердити висновок щодо відсутності універсального методу, який би дозволив врахувати всі без винятку показники та критерії оцінки об’єктів [10].

Ми пропонуємо застосувати метод аналізу ієрархій (MAI) для знаходження одного оптимального рішення, що потребує оцінювання усіх альтернативних варіантів за багатьма критеріями в умовах обмеженої кількості інформації. Перевагою запропонованого підходу є той факт, що ваги критеріїв і оцінки за суб'єктивними критеріями не призначаються адміністративним впливом, як найчастіше намагаються робити, у разі використання експертних підходів, а на основі парних порівнянь. Інша перевага – опис критеріїв у вигляді ієрархії (дерева). Сутність методу полягає в тому, що він не пропонує особі, яка ухвалює рішення, будь-який «правильний» варіант, а дозволяє в інтерактивному режимі віднайти альтернативу, яка щонайкраще узгоджується з розумінням суті проблеми і вимогами до її розв’язку [11].

Приклад реалізації розрахунків для вибору ІС виконано в програмі «MPRIORITY 1.0» [12]. Рішення щодо вибору ІС приймається на основі таких критеріїв:

1) вартість;

2) засоби пошуку інформації за різними критеріями;

3) репутація фірми розробника (досвід на ринку);

4) модульний принцип побудови системи;

5) комплексний підхід до організації СЗІ.

На рис. 1. наведено модель структури ієрархій. Вона складається з трьох рівнів: перший – вибір ІС; другий – критерії, за якими він здійснюється; третій – альтернативи вибору.

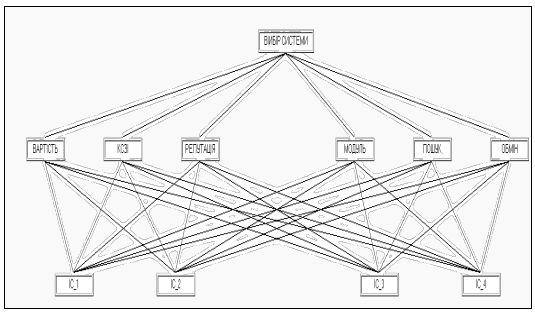


Рис. 1. Структура ієрархій

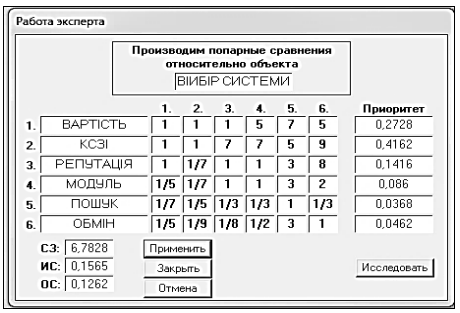


Рис. 2. Результати попарного порівняння критеріїв

Порівняння критеріїв та даних провели за лінгвістичною шкалою Т. Сааті [11]: «немає переваги», «має незначну перевагу» тощо. Пріоритет критеріїв встановлюється на підставі експертного оцінювання, яке здійснюється в ході анкетування. Результати порівняння критеріїв наведено на рис. 2. З таблиці видно, що пріоритетним критерієм є КСЗІ, потім вартість, репутація фірми розробника на ринку, модульність, механізми пошуку та можливість обміну інформацією різного формату.

Наступним кроком є попарне порівняння ІС відносно обраних критеріїв. Приклад порівняння за критерієм КСЗІ наведено на рис. 3., перевірки узгодженості вибору – на рис. 4.

Рис. 3. Порівняння за критерієм КСЗІ

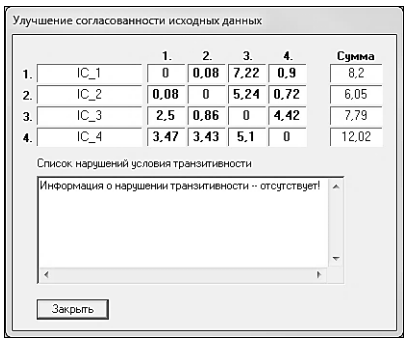


Рис. 4. Перевірка узгодженості за критерієм КСЗІ порівняння критеріїв

Відношення узгодженості (рос. отношение согласованности – ОС) не повинне перевищувати 0,1 (10%), у деяких випадках 0,2 (20%) та наближатися до нуля. Якщо значення дещо більше, ніж передбачалося, можна зробити висновок про неузгодженість тверджень експерта. Перевірка узгодженості вибору дає можливість усунути неузгодженість даних у матриці попарних порівнянь.

Після проведення порівняння ІС відносно обраних критеріїв отримуємо результат, який зображено на рис. 5. Отже, максимальний пріоритет отримала ІС 3.

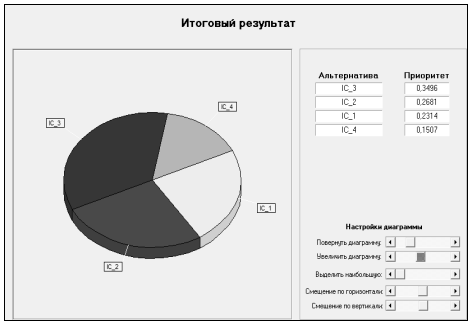


Рис. 5. Сумарний результат визначення пріоритетів у виборі ІС

Інший спосіб побудови ієрархії зображено на рис. 6. Він ускладнений тим, що на другому рівні знаходяться експерти, думка яких є критерієм оцінки наступного вибору. Побудова ієрархії визначається кількістю рівнів декомпозиції та залежить від поставлених завдань. Оцінювання на другому рівні проводить керівник підрозділу (установи), результати відображено на рис. 7.

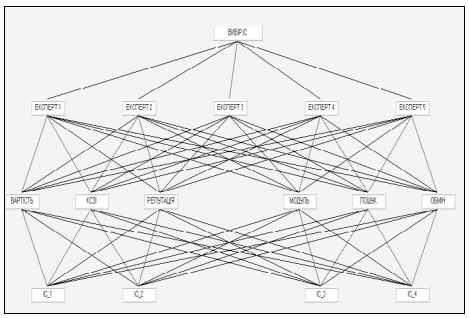


Рис. 6. 4-рівнева ієрархія

Рис. 7. Визначення пріоритетів для другого рівня

Наступні кроки виконуються аналогічно, але з урахуванням ваги кожного експерта. Приклад оцінювання експертами наведено на рис. 8, сумарний результат оцінювання – на рис. 9, він несуттєво відрізняється від попереднього.

Рис. 8. Порівняння експерта 1

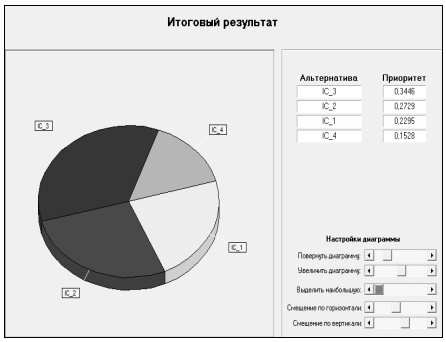


Рис. 9. Сумарний результат визначення пріоритету у ході вибору ІС з урахуванням ваги експертів

На етапі *«Аналіз можливих варіантів автоматизації процесів»* визначають варіанти створення інтегрованої ІС ВВНЗ, яка може складатися з таких компонентів:

1) ІС, що функціонують у закладі й будуть інтегровані силами власних ІТ фахівців або силами сторонніх фірм (організацій) до інтегрованої ІС;

2) готові ІС, що закуповуються та впроваджуються в діяльність ВВНЗ, мають певний фіксований функціонал, який вже відповідає потребам;

3) готові ІС, що закуповуються та впроваджуються в діяльність ВВНЗ, з настроюваним у певних межах функціоналом, який забезпечить після його адаптації визначені потреби;

4) створення нових ІС на замовлення силами сторонніх фірм для забезпечення необхідного функціонала інтегрованої ІС, для якого немає готових рішень;

5) створення ІС силами власних ІТ фахівців ВВНЗ для забезпечення необхідного функціонала інтегрованої ІС, для якого немає готових рішень.

Основні завдання етапу *«Розроблення плану заходів з автоматизації діяльності ВВНЗ»* – це визначення порядку: закупівлі та впровадження комерційних ІС; створення ІС на замовлення; створення ІС власними силами та засобами; демонтажу (утилізації) наявних у ВВНЗ ІС; інтеграції ІС та ЗА (зокрема, уже наявних у закладі ІС) до єдиної інтегрованої ІС; реалізації пілотних проєктів; розроблення плану заходів з автоматизації діяльності ВВНЗ.

Додатковий етап «Детальне дослідження процесів» проводиться для *Процесів,* включених до плану детального дослідження, щодо яких на етапі аналізу можливих варіантів автоматизації процесів прийнято рішення: що вони будуть автоматизуватися власними силами; про необхідність їх удосконалення (реінжинірингу); не прийнято остаточного рішення щодо варіанта їх автоматизації, оскільки вони потребують більш глибокого аналізу. Під час заповнення метаданих у паспортах (картах) процесів необхідно: визначити замовника/споживача процесу (адміністративну підпорядкованість – підрозділ, посадову особу; функціональну – забезпечення функціонування процесу); виконати опис процесу «ЯК Є» у вигляді блок-схеми; окреслити інформаційні потоки, необхідні для ефективного виконання процесу, тобто вхідні та вихідні документи за операціями процесу.

Висновки. Розроблена методика дозволяє розв'язати основні організаційні-методичні завдання, які виникають під час вибору та впровадження ІС ВВНЗ. Використання процесно-орієнтованого підходу дає можливість провести ідентифікацію *Процесів,* що є підґрунтям для визначення функціонала ІС. Застосування методичних рекомендацій забезпечує єдиний підхід до вибору та впровадження ІС та ЗА в діяльність ЗВО, визначає наявний рівень, фактичні потреби автоматизації закладу, особливості впровадження ІС та ЗА, дозволяє встановити порядок та пріоритетність їх впровадження.

Подальші напрямки досліджень: удосконалення розробленої методики за результатами практичної апробації в декількох ВВНЗ.

СПИСОК ЛІТЕРАТУРИ

1. Google Scholar Citations. URL: https://scholar.google.com.ua/citations?user=LuctT5cAAAAJ/&hl=ru (last accessed: 30.11.2019).
2. Microsoft Word-aref_Andrukhiv_last_0809_NEW. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/29653/1/avt_Andrukhiv.pdf (last accessed: 30.11.2019).
3. Кільченко А. В. Концептуальна модель інформаційної системи «Наукові дослідження» НАПН України // Системні дослідження та інформаційні технології (System research & information technologies) : Міжнар. наук.-техніч. журнал. Київ, 2014. № 1. С. 81–91.
4. Автоматизована система управління повсякденною діяльністю вищого військового навчального закладу на базі локальної обчислювальної мережі : автореферат. URL: http://referatu.net.ua/newreferats/7569/181662 (дата звернення: 26.11.2019).
5. Карпенко М. Ю., Манакова Н. О., Гавриленко І. О. Технології створення програмних продуктів та інформаційних систем : навч. посібник. Харків : Харківськ. нац. ун-т міськ. госп-ва ім. О. М. Бекетова, 2017. 93 с.
6. ДСТУ ISO 9001:2009 Національний стандарт України. URL: http://www.gerelo.dp.ua/index/info_dstu_iso_9001-2009.html (дата звернення: 26.11.2019).
7. УРАН – Наукова періодика. URL: http://uran.net.ua/~ukr/ps-journals.htm (дата звернення: 26.11.2019).
8. Nextcloud. URL: https://nextcloud.com/ (last accessed: 30.11.2019).
9. Контрукторське бюро КПІ. URL: http://kbis.kpi.ua/kbis/index.php?lang=ukr (дата звернення: 26.11.2019).
10. Мельник А. П., Балковий А. В. Погляди щодо використання методів порівняння для визначення пріоритетів розвитку ОВТ РВІА // Зб. наук. праць Центр. наук. дослід. ін-ту озброєння та військ. техніки Збройних Сил України. Київ : ЦНДІ ОВТ ЗС України, 2019. Вип. 4 (71). С. 165–172
11. Саати Т. Принятие решений. Метод анализа иерархий. Москва : Радио и связь, 1993. URL: https://www.twirpx.com/file/26182/ (дата обращения: 26.11.2019).
12. To Make Choice: программные системы поддержки принятия оптимальных решений. URL: http://www.tomakechoice.com/program.html (дата обращения: 26.11.2019).

Подано 11.11.2019

А. М. Перегуда, Е. П. Черкес, П. Н. Пионтковский, А. В. Дзюбенко

МЕТОДИКА ВЫБОРА И ВНЕДРЕНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ В ДЕЯТЕЛЬНОСТЬ ВЫСШЕГО ВОЕННОГО УЧЕБНОГО ЗАВЕДЕНИЯ

В статье определены проблемные вопросы выбора и внедрения информационной системы в высшем военном учебном заведении. Предложена методика в форме методических рекомендаций для решения задач: описания процессов деятельности, которые обеспечивают основные возможности высшего военного учебного заведения; выбора коммерческих информационных систем и определения вариантов создания интегрированной информационной системы; разработки плана мероприятий по автоматизации деятельности учреждения. В процессе разработки методики учтен опыт внедрения средств автоматизации в коммерческой, военной и образовательной сферах. Предложено использование процессно-ориентированного подхода, позволяющего сформировать системное видение архитектуры организации (учреждения), определять основные, управленческие процессы образовательной деятельности, процессы обеспечения, что на этапе анализа позволяет формировать функциональные требования к информационной системе, которые соответствуют возможностям высшего военного учебного заведения.

Для проведения анализа и построения рейтинга коммерческих информационных систем использован количественный многокритериальный метод – метод анализа иерархий, который позволяет решать слабоструктурированные задачи. Для исследования информационной системы проанализированы и определены основные критерии, на базе которых принимается решение, максимально обеспечивающее выдвинутые высшим военным учебным заведением требования.

Исходными данными являются результаты опроса экспертов в виде матриц парных сравнений для всех узлов иерархии. Определение приоритетности вариантов в ходе выбора коммерческих информационных систем выполнено с использованием специализированного программного обеспечения «MY PRIORITY 1.0». Результаты проведенного анализа могут быть использованы для обоснования выбора фирмы производителя информационных систем.

Особенностью предлагаемой методики является комплексность подхода к: идентификации, формализованному описанию, анализу и совершенствованию процессов деятельности высшего военного учебного заведения; определению уровня автоматизации, фактических потребностей, особенностей создания и формирования требований к информационной системе и средствам автоматизации с ориентацией на специфическую (военную) направленность подготовки в этих заведениях.

Ключевые слова: *комплексная методика; информационная система; высшее военное учебное заведение; метод иерархии.*

O. M. Pereguda, O. P. Cherkes, P. M. Piontkivskyi, O. V. Dzubenko

METHODOLOGY OF CHOOSING AND IMPLEMENTATION OF THE INFORMATION SYSTEM IN HIGHER MILITARY EDUCATION INSTITUTION ACTIVITY

This article reveals problematic aspects of choosing and implementation of the information system (IS) in higher military education institution activity. Article gives the description of

solving further tasks: describing of operations, which provide main higher military education institution capabilities, choosing commercial information system and determination of integrated IS creation variants, developing of the measures plan for higher military education institution activities automation.

During the methodology development, experience of implementation of automation means in commercial, military and educational spheres was taken into consideration.

Using of process-oriented approach was proposed. this gives ability to figure the system view of organization (institution) architecture, determine peculiarities of realization of managemant (strategy) processes, main processes in scientific and educational activities and enabling (additional) processes, that within the analysis phase plays the role of basis for definition of functional requirements to IS for meeting higher military education institution demands.

For analysis and rating of commercial IS author have chosen quantative multi-criteria method – hierarchy analysis method, which allows to solve ill-structured problems.

For IS analysis were investigated and determinate main criteria's for making the decision which can fully meet higher military education institution demands.

Results of experts consultation are the base data, which is represented like paired comparison matrix for each hierarchy nodes. Determination of options priority while choosing commercial IS was performed using specialized software «MY PRIORITY 1.0». Results of this analysis can be used for argumentation of IS developer choice.

Peculiarity of the given methodology is the complex approach to: identification, formal definition, analysis and improvement of higher military education institution activities; evaluation of automation level, actual needs, peculiarities of creation and IS requirements definition and automation means taking into consideration specific (military) training in higher education institution.

Keywords: *complex methodology; information system; higher military education institution; hierarchy method.*

ISSN 2076-1546

УДК 341.123 (045) DOI: 10.46972/2076-1546.2019.17.05

С. А. Запорожець

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Статтю присвячено дослідженню інформаційної безпеки України в умовах гібридної війни, протистоянню гібридним загрозам з боку Російської Федерації, а також пріоритетним напрямам ефективного забезпечення інформаційної безпеки в нашій державі. Аналіз даної проблеми показує, що сучасний стан системи інформаційної безпеки України характеризується, з одного боку, посиленням уже наявних загроз, а з іншого – появою нових викликів.

Технологічні інноваційні процеси, інформаційний прорив, глобалізація світу та тенденції регіональної інтеграції поряд із наданням колосальних можливостей для поступального розвитку країн зумовлюють багато негативних наслідків. Наприклад, активізувалося ведення гібридної війни між державами, зокрема проти України. Збільшується їх спроможність щодо проведення інформаційних та інформаційно-психологічних операцій, посилення чутливості суспільства до загибелі мирного населення та втрат особового складу військових формувань у воєнних конфліктах. У сучасних умовах глобалізації, технологічною основою якої стали глобальні інформаційно-телекомунікаційні мережі та єдиний інформаційний простір, спостерігається тенденція до зміни принципів і методів управління, зокрема у військовій справі. Здатність інформації впливати на світогляд та настрої людей дає можливість отримувати перевагу над противником, не вступаючи в силове протистояння з ним. Фактично правильна методика роботи з інформацією стала новим способом ведення збройної боротьби, а саме гібридної війни. З огляду на це в провідних країнах світу проходить поступова трансформація підходів до формування воєнної політики держави, які практично втілюються для забезпечення її інформаційної безпеки в умовах гібридної війни. Повномасштабна інформаційна війна Росії проти України продемонструвала важливість забезпечення інформаційної безпеки як однієї з основних складових національної безпеки. Саме тому перед державними і військовими органами управління постало завдання розробки ефективних заходів нейтралізації негативного інформаційного впливу Російської Федерації та протидії його подальшому розгортанню.

У статті також проаналізовано підходи до підвищення ефективності державного реагування на загрози національній безпеці в інформаційній сфері в умовах сучасного збройного конфлікту на сході України. Встановлено, що для досягнення відповідного рівня інформаційної безпеки необхідно сформувати єдиний державний механізм забезпечення інформаційної безпеки. Запропоновано спосіб вирішення завдань, які виникають у даній сфері.

Ключові слова: *інформаційна безпека; гібридна війна; інформаційна зброя; суспільство; державна політика.*

Постановка проблеми в загальному вигляді. Гібридна війна, у стані якої перебуває Україна, деструктивно впливає на свідомість українського населення. Наша держава, як

і більшість цивілізованого світу, у цілому виявилася не готовою до такої агресії з боку Росії. Підтвердження цьому – відсутність чітких правил поведінки в умовах інформаційної агресії та пропаганди. Одним із найбільш відчутних викликів для України є масштабна російська пропаганда, яка вже давно вийшла за межі кордонів. Тому інформаційна безпека є одним із основних чинників стабільного розвитку держави, що формується в руслі об'єктивних процесів забезпечення національної безпеки. Для усунення гібридних загроз національній безпеці або запобігання їх появі доводиться вдаватися до інформаційного захисту держави. У сучасних умовах на усіх рівнях: ідеології, релігії, історії, освіти – застосовуються інформаційні війни. Сьогодні гостро постає питання забезпечення інформаційної безпеки, а саме в умовах гібридної війни. Тому основними напрямами державної інформаційної політики повинно бути гарантування інформаційної безпеки особистості, яка характеризується захищеністю її психіки та свідомості від небезпечних інформаційних впливів, дезінформації та маніпулювання.

Аналіз останніх досліджень і публікацій. Авторами робіт, що становлять методологічну основу досліджень загальнотеоретичних питань інформаційної безпеки, є такі науковці: О. Левченко [15], Р. Грищук [5], В. Горбулін [9], М. Биченок [3], О. Тихомиров [13], І. Грабар [6], В. Антонюк [1], А. Кунинець [14], В. Бондаренко [4], Ю. Горбань [7], Ф. Медвідь [18], В. Ліпкан [17], Д. Дубов [11], Я. Жарков [20] тощо. Усі вони працювали над проблемою забезпечення інформаційної безпеки України, проте, незважаючи на дуже велику кількість наукових праць з цієї тематики, розкриття питання механізму забезпечення інформаційної безпеки держави в умовах гібридної війни не є комплексно спрямованим.

Формулювання завдання дослідження. Мета статті – проаналізувати головні складові інформаційної безпеки України в умовах гібридної війни, адже дана проблема має давнє походження і стала особливо важливою у наш час, коли використання з боку сусідньої держави (Росії) інформаційних технологій поширилося практично у всі сфери нашого життя.

Виклад основного матеріалу. Останнє десятиліття XX століття було відзначене драматичними змінами на міжнародній арені. Крах біполярної геополітичної моделі світоустрою призвів до корінної зміни геополітичної ситуації у всьому світі. Закінчилася епоха відносної стабільності, відбувся фактично крах Ялтинско-Потсдамської системи безпеки. Значні перетворення на політичній карті Європи в 90-ті роки XX століття створили нові геополітичні умови, які призвели до реанімації старих і виникнення нових конфліктних ситуацій. Загострюється боротьба між окремими країнами за глобальне і регіональне лідерство, зокрема і за володіння природними ресурсами. Форми цієї боротьби різні, але її запеклість і безкомпромісний характер свідчать про актуалізацію питань забезпечення національної безпеки для кожної держави окремо, проблем виживання та розвитку в новому тисячолітті.

Глобальні процеси інформатизації суспільства та широке запровадження інформаційних технологій, їх вплив на всі сфери розвитку держав висувають на перший план питання забезпечення інформаційної безпеки. Від виваженої політики інформаційної

безпеки, від ступеня захищеності, достовірності та повноти інформації в цивілізованому сучасному світі залежить стабільна соціальна, економічна, правова ситуації в державі. На тлі всіх цих геополітичних перетворень інформація стає найпотужнішим глобальним стратегічним ресурсом, володіючи яким, суспільство і держава вже сьогодні можуть значно посилити свої позиції на міжнародній арені і управляти світовими політичними, економічними, соціальними, культурними та іншими процесами, що відбуваються в міжнародних системах.

Конвергенція комунікацій, комп'ютерних систем, індустрії розваг і побутової електроніки істотно змінює інформаційне середовище проживання людини. У результаті цих змін, які мають глобальний характер, інформаційна сфера все більшою мірою визначає не тільки технологічні інновації, а й соціокультурну основу суспільного життя, потреби особистості, менталітет і поведінку мільярдів людей. Зміна ролі інформації в житті людства, а також поява нових технологій обробки, передачі, зберігання та подання інформації дозволяють сьогодні говорити про те, що сучасна цивілізація змінює свій вигляд і входить у нову епоху, перетворюючись в інформаційну цивілізацію.

Поступово інформація зачіпає всі сфери життєдіяльності людини, що дозволяє говорити про неї як про нову форму влади. Вона не замінює повністю інші форми влади, а значно розширює можливості як усередині суспільств і держав, так і на міжнародній арені. Інформація пронизує буквально всі сфери життєдіяльності більш-менш розвинених сучасних держав. За допомогою неї та інформаційних технологій сьогодні нерідко скидають одні політичні еліти в державах і підтримують інші. У деяких випадках інформаційний вплив на окремі країни зведено в ранг інформаційної війни. Проблема забезпечення інформаційної безпеки в сучасному світі, особливо для України, набула важливого значення. Досягнення в інформаційній сфері створюють передумови для формування нового типу інформаційного суспільства, основою для якого є бурхливий розвиток та конвергенція інформаційних і телекомунікаційних технологій. Цей процес відбувається в умовах глобалізації [6].

Усе це призводить до того, що провадиться політика глобалізації у своїх інтересах найбільшими країнами, які поступово формують умови для створення керованого й підконтрольного їм суспільства менш захищених держав. Інформаційна глобалізація разом з глобалізацією економічною, політичною та культурною розмиває державні кордони.

У зв'язку з цим забезпечення інформаційної безпеки в умовах гібридної війни для нашої держави стає найпершою проблемою.

Аналіз даного питання показує, що сучасний стан системи інформаційної безпеки України характеризується, з одного боку, посиленням вже наявних загроз, а з іншого – появою нових викликів. Інноваційні технологічні процеси, інформаційна революція, економічна та соціокультурна глобалізація світу, тенденції регіональної інтеграції поряд із наданням колосальних можливостей для поступального розвитку країн і регіонів зумовлюють багато негативних наслідків. Серед них – активізація ведення інформаційних та інформаційно-психологічних війн між окремими країнами, зокрема й проти України. Ці війни називають гібридними, вони виникають в умовах появи нових форм збройної

боротьби, піднесення сепаратистських рухів, посилення діяльності міжнародних терористичних організацій, зниження можливостей держав щодо контролю над процесами, які відбуваються в межах їх національних територій. У зв'язку з формуванням загальносвітового інформаційного простору неухильно зростає роль громадської думки, яка сьогодні стала потужним фактором управління, виховання і регулювання поведінки людей.

Такі процеси супроводжуються спробами встановити повний контроль Російської Федерації (РФ) над ситуацією в Україні, при цьому широко використовуються методи гібридної війни, а також маріонеткові політичні сили для захисту нібито "приниженого російськомовного населення". Тому основною метою Росії, що протистоїть Північноатлантичному альянсу, є утримання України під своїм контролем, використання наших територіальних, матеріальних, трудових, інформаційних та інтелектуальних ресурсів, перешкоджання приходу до влади проєвропейських сил, здатних відновити політичну, економічну та військову конкурентоспроможність держави.

Одним із важливих завдань РФ є позбавлення України її стратегічних і тактичних союзників у країнах НАТО, створення перешкод для досягнення нашою державою своїх національних інтересів у світі, а також для налагодження нових і збереження старих зв'язків із сусідами на пострадянському просторі.

Росія й Україна мають велику кількість пересічних інтересів у світі, щоб зберігати навіть видимість нейтралітету відносно одна одної. У сучасній імперській політиці Україні, як і раніше, відводиться місце домініону РФ, а отже, обмежуються її інтереси у світі. Подібна обставина об'єктивно не може довго існувати, оскільки суперечить не тільки статусу України як суверенної держави, а й здатності Росії тримати під контролем ситуацію в нашій державі.

Таке становище нестійкої рівноваги між Україною та РФ може призвести до значних світових потрясінь. За цих умов наша держава повинна докласти особливих зусиль для відстоювання життєво важливих інтересів, мати чітко вироблену концепцію протидії викликам і загрозам у політичній, економічній, військовій, а також в інформаційній сферах, щоб захистити власну безпеку.

Особливу увагу необхідно звернути на те, що українське суспільство зацікавлене в створенні державних захисних механізмів, які сприяли б формуванню за кордоном об'єктивного погляду на українську дійсність. Як показує практика, діяльність вітчизняних засобів масової інформації (ЗМІ) з роз'яснення закордонній аудиторії цілей і основних напрямків державної політики України, позицій щодо соціально значущих подій українського та міжнародного життя потребує вдосконалення. Це один із найбільш важливих об'єктів забезпечення інформаційної безпеки держави.

На сьогодні Україна має у своєму розпорядженні необхідні ресурси для забезпечення своєї інформаційної безпеки. Вони повинні бути використані в таких сферах: розробка основних напрямів державної політики в галузі вдосконалення інформаційного забезпечення зовнішньополітичного курсу; створення українським представництвам і організаціям за кордоном умов для роботи з нейтралізації поширюваної там дезінформації про зовнішню політику; удосконалення інформаційного забезпечення

з протидії порушення прав і свобод українських громадян та юридичних осіб на території РФ. Зміцнення свого інформаційного впливу у світі необхідно розглядати як найважливішу складову інформаційної політики України. Для успішної відсічі зовнішнім і внутрішнім інформаційним загрозам із боку Росії необхідна перш за все внутрішньополітична стабільність і єдність суспільства. Однак дійсність українського суспільства характеризується наявністю розколу на прихильників національної ідеї та так званого "руського миру", що послаблює протистояння інформаційним загрозам. Усе це вимагає від України посилити свій вплив в інформаційній безпеці з метою захисту інтересів держави, її цілісності та суверенітету.

Агресивні дії Росії проти України спричинили руйнування європейської та глобальної безпеки. Сам російсько-український конфлікт порушив регіональну стабільність та створив глобальні ризики. Термін "гібридна війна" виявився не тільки теоретично, а й практично найбільш придатним для специфіки дій агресора, який, поєднуючи дипломатичні, квазімілітарні, мілітарні, інформаційні, економічні засоби, залякуючи ядерним шантажем, намагається послідовно досягнути власних політичних цілей [9].

Що є гібридної війною? На це питання існує безліч тверджень та думок, але якщо все ж спробувати дати узагальнену відповідь на зазначене питання, то безперечним зараз є розуміння того, що це поєднання численних військових і невійськових типів атак та впливів на противника заради досягнення своєї мети. У процесі гібридної агресії ворог використовує в основному слабкості, недоліки або характеристики противника, які в цілому в мирний час не сприймаються як слабкі сторони. На сучасному етапі для агресора головними методами ведення гібридної війни є використання ЗМІ та соціальних мереж.

Гібридну війну можна трактувати як модель війни, за якої намагаються приховати її військовий характер, а також участь у ній державних структур. Саме тому в ній різко зростає роль інформаційної складової, оскільки реальні фізичні контексти замінюються неадекватними їм інформаційними, що приховують реальний стан справ більш інтенсивно, ніж це має місце у війні звичайного порядку [2]. Гібридна війна має невелику ділянку реально бойових дій, але поширюється в усьому мирному просторі, підключаючи до конфліктних ситуацій абсолютно всі ресурси, включаючи артистів, письменників, політичних діячів інших країн. Говорити про гібридну війну як про невійськову потрібно, адже в ній військові видозмінюються на цивільних, чиновники – на гравців недержавного рівня. Прикладом трансформації "військові – цивільні" є "зелені чоловічки" в Криму, яких російська пропаганда досить довго відмовлялася визнавати військовослужбовцями збройних сил, оскільки у них не було розпізнавальних знаків. Щоправда зброя була, але вони намагалися її не застосовувати, вона слугувала засобом залякування.

Російська гібридна війна в Україні схожа на китайську концепцією "війни без обмежень", у якій багато невійськових інструментів. До російський "гібридних елементів" можна віднести: фінансування політичних партій; інвестиції; придбання недійсного ресурсу; входження до європейських структур російських розвідувальних органів; використання заморожених конфліктів на етнічному підґрунті та релігійних інституцій; підтримка російських ЗМІ за кордоном; кібератаки та їх координація. Країна, що

проводить інформаційно-психологічні заходи, повинна довести справедливість своїх дій як для власного суспільства, так і для народу, на який вони націлені. У неоголошеній війні атакованій країні досить важко давати відсіч. Гібридна війна стала надбанням нового часу саме тому, що багато потрібних для неї завдань можна виконати за рахунок інформаційного компонента. Чим потужніший його розвиток, тим легше досягти поставлених цілей.

Недостатня ефективність наявної на сьогодні інформаційної безпеки в умовах динамічного та малопередбачуваного впливу сучасних факторів геополітичної конкуренції, глобалізації й найбільш гострих форм інформаційного суперництва, яке відобразилося у збройному конфлікті на сході України, вимагає зміни всієї чинної концепції інформаційної безпеки з метою її адаптації до сучасних умов. Істотні труднощі в забезпеченні інформаційної безпеки в умовах гібридної війни дозволяють нам говорити про особливі умови її реалізації та необхідність вироблення механізмів впливу, спеціальних методів, адекватних тим змінам, які відбуваються в суспільстві [3].

Реалізація особливих умов забезпечення інформаційної безпеки в умовах гібридної війни полягає в:

глобальному формуванні інформаційного суспільства;

соціально-політичній, інформаційній, психологічній глобалізації;

геополітичній конкуренції інформаційного простору;

інформаційно-психологічному протистоянні як складовій збройного конфлікту, що виник на окремих окупованих територіях України [5].

На початку війни в 2014 році наша країна зіткнулася з використанням проти неї пропагандистської системи Росії, що діє одночасно на всіх напрямах (українському, російському, міжнародному), застосовуючи всі різновиди засобів масової комунікації.

Аналіз сучасної воєнно-політичної ситуації, що складалася довкола України та на її території, дає підстави вважати, що наша держава від самого початку, коли проголосила незалежність, стала об'єктом для пропагандистських дій (операцій) та довготривалого психологічного впливу з боку РФ.

Гібридна війна при цьому є якісно новим підходом ведення воєнної кампанії, у якій закладена психологічна та інформаційна обробка громадян, застосування жорсткої сили іміджевої дипломатії на підготованій території, що дало змогу реалізувати активну приховану інтервенцію в Україну заздалегідь добре навчених нечисленних диверсійних груп (озброєних сучасною бронетехнікою, ефективними засобами наступу й оборони), які з легкістю анексували на свою користь окремі території, зокрема АР Крим [10].

Зважаючи на викладене вище, пропонуємо спосіб вирішення таких завдань, які повинні покращити забезпечення інформаційної безпеки України в умовах гібридної війни. На рис. 1 відображено основні пріоритетні напрями та організаційні питання в цій сфері.

Отже, майбутнє України залежить від ефективності забезпечення інформаційної безпеки, здатності самої держави захистити й відстояти у своєму інформаційному просторі національні та духовні цінності, забезпечити стійку працездатність державних структур щодо прийняття адекватних рішень у складних ситуаціях та обстановці невизначеності.

Для підвищення ефективності державного реагування на загрози забезпечення інформаційної безпеки в умовах гібридної війни та сучасного збройного конфлікту на території України виокремимо основні чинники реагування (рис. 2).

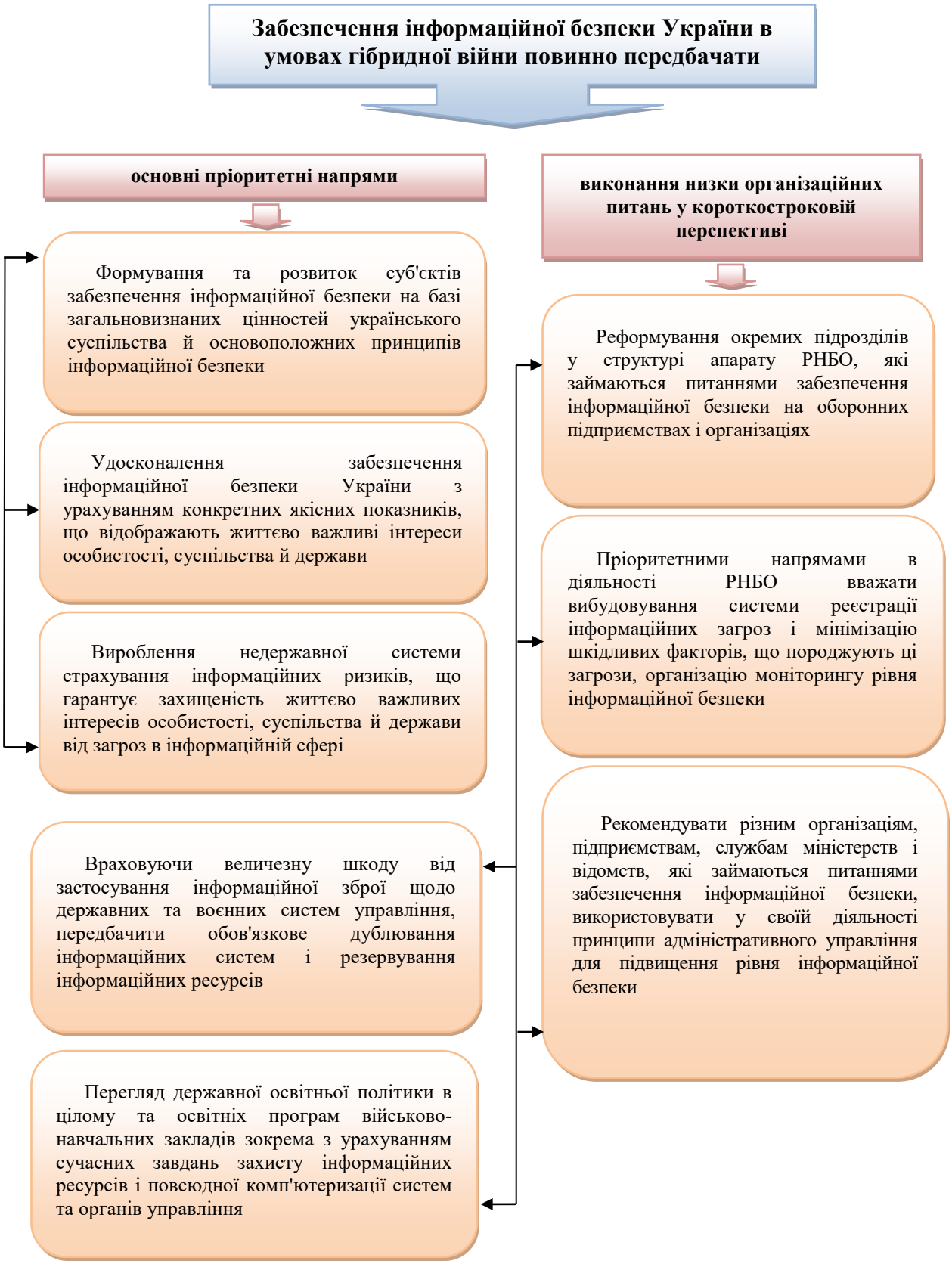


Рис. 1

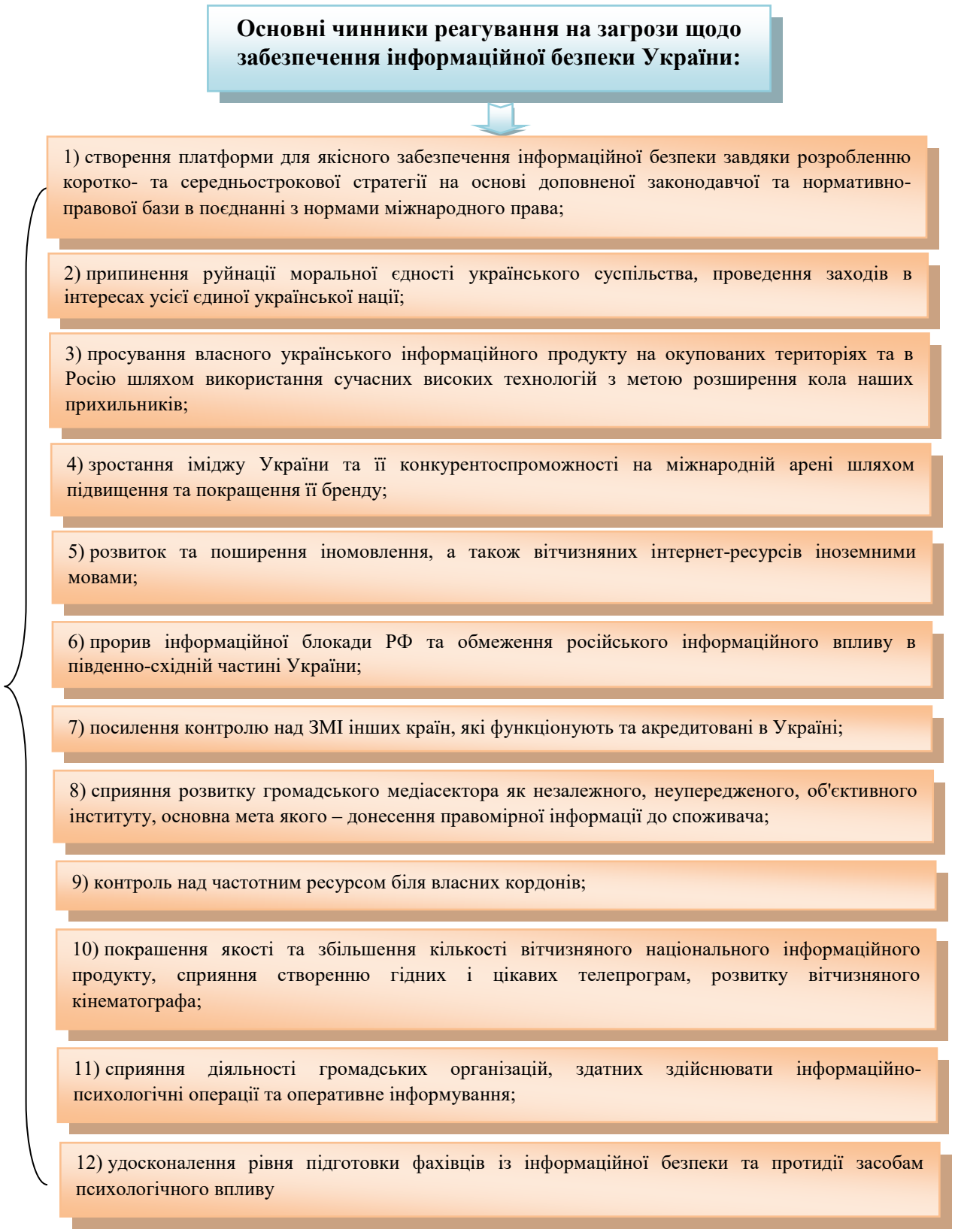


Рис. 2

Підсумовуючи викладене вище, слід визначити відповідний рівень забезпечення інформаційної безпеки України в умовах гібридної війни та сформувати єдиний державний механізм на основі вирішення таких завдань (рис. 3).

Рис. 3

Висновки. Отже, можна стверджувати, що виконання зазначених вище заходів дасть змогу протидіяти гібридним загрозам як традиційними, так і новими центрами протистояння, унеможливить подальше маніпулювання свідомістю суспільства в ході масштабної російської експансії та сприятиме захисту інформаційної безпеки нашої держави.

Можливості забезпечення інформаційної безпеки в умовах гібридної війни залежать від результативності, ефективного впливу на населення України, зростання в суспільстві довіри до керівництва держави, вітчизняних ЗМІ, зниження рівня дестабілізаційної обстановки в країні. Успішне забезпечення інформаційної безпеки сприятиме стійкості українського суспільства до різноманітних деструктивних інформаційно-психологічних впливів, що породжуються з реалізацією гібридних загроз. Ефективний інформаційний вплив з боку України на іноземну цільову аудиторію сприятиме поступовому формуванню проукраїнських поглядів у міжнародній спільноті.

СПИСОК ЛІТЕРАТУРИ

1. Антонюк В. В. Ієрархія керівних документів державної політики з питань забезпечення інформаційної безпеки: шляхи впорядкування // Актуальні проблеми державного управління, педагогіки та психології. 2013. Вип. 2. С. 11–16.

2. Богуш В., Юдін О. Інформаційна безпека держави / Гол. ред. Ю. О. Шпак. Київ : "МК-Прес", 2005. 432 с.
3. Биченок М. М., Шемаєв В. М. Формалізація та оцінювання інформаційних загроз національним інтересам // Труди університету. Київ : НУО України, 2011. № 1 (100). С. 54–61.
4. Бондаренко В. О., Литвиненко О. В. Інформаційна безпека сучасної держави: концептуальні роздуми. URL: http://www.crime-research.iatp.org.ua/library/strateg.htm (дата звернення: 15.10.2019).
5. Грищук Р. В., Молодецька-Гринчук К. В. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах // Сучасний захист інформації. 2017. № 3 (31). С. 86–96.
6. Грабар І. Г., Грищук Р. В., Молодецька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / За заг. ред. Р. В. Грищука. Житомир : ЖНАЕУ, 2019. 280 с.
7. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення URL: http://www.visnyk.academy.gov.ua/wpcontent/uploads/2015/04/20.pdf (дата звернення: 15.10.2019).
8. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть // Вісник Київського ун-ту ім. Т. Шевченка. 1999. Вип. 14: Міжнародні відносини. С. 46–48.
9. Горбулін В. П. Світова гібридна війна: український фронт : монографія. Київ : НІСД, 2017. 496 с.
10. Горбулін В. П., Биченок М. М., Копка П. М. Актуальні проблеми системного забезпечення інформаційної безпеки України // Зб. мат. Міжнар. наук.-практ. конф. ("Форми та методи забезпечення інформаційної безпеки держави", м. Київ, 13 березня 2008 р.). Київ : Нац. академія СБ України, 2008. С. 79–85.
11. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. Київ : НІСД, 2011. 30 с.
12. Почепцов Г. Г. Сучасні інформаційні війни. Київ : Вид. дім "Києво-Могилянська академія", 2015. 497 с.
13. Тихомиров О. О. Забезпечення інформаційної безпеки: теоретико-правовий аспект // Право України. 2011. № 4. С. 252−259.
14. Кунинець А. І, Грицюк Ю. І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній // Науковий вісник НЛТУ України. 2013. Вип. 23 (2). С. 352–360.
15. Левченко О. В. Концептуальний підхід до комплексної оцінки стану інформаційної безпеки // Наука і техніка Повітряних Сил Збройних Сил України. 2015. № 3 (20). С. 47–50.
16. Литвиненко О. Інформація і безпека // Нова політика. 1998. № 1. С. 47–49.
17. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.
18. Медвідь Ф. Інформаційна безпека України: виклики та загрози. URL: http://www.nato.ru.if.ua/journal/2009-2-28.pdf (дата звернення: 15.10.2019).
19. Хоффман Л. Дж. Современные методы защиты информации / [пер. с англ.]. Москва : Советское радио, 1980. 57 с.

20. Історія інформаційно-психологічного протиборства : підруч. / [Я. М. Жарков, Л. Ф. Компанцева, В. В. Остроухов та ін.] ; за заг. ред. Є. Д. Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. 212 с.

Подано 25.11.2019

С. А. Запорожец

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ УКРАИНЫ В УСЛОВИЯХ ГИБРИДНОЙ ВОЙНЫ

Статья посвящена исследованию информационной безопасности Украины в условиях гибридной войны, противостоянию гибридным угрозам со стороны Российской Федерации, а также приоритетным направлениям эффективного обеспечениия информационной безопасности в нашей стране. Анализ данной проблемы показывает, что современное состояние системы информационной безопасности Украины характеризуется, с одной стороны, усилением уже существующих угроз, а с другой – появлением новых вызовов.

Технологические инновационные процессы, информационный прорыв, глобализация мира и тенденции региональной интеграции наряду с предоставлением колоссальных возможностей для поступательного развития стран несут много негативных последствий. Например, активизировалось ведение гибридной войны между государствами, в том числе против Украины. Увеличивается их способность по проведению информационных и информационно-психологических операций, усилению чувствительности общества к гибели мирного населения и потерям личного состава воинских формирований в военных конфликтах. В современных условиях глобализации, технологической основой которой стали глобальные информационно-телекоммуникационные сети и единое информационное пространство, наблюдается тенденция к изменению принципов и методов управления, в том числе в военном деле. Способность информации влиять на мировоззрение и настроения людей дает возможность получать преимущество перед противником, не вступая в силовое столкновение с ним. Фактически правильная методика работы с информацией стала новым способом ведения вооруженной борьбы, а именно гибридной войны. Учитывая это, в ведущих странах мира проходит постепенная трансформация подходов к формированию военной политики государства, которые практически воплощаются для обеспечения информационной безопасности в условиях гибридной войны. Полномасштабная информационная война России против Украины продемонстрировала важность обеспечения информационной безопасности как одной из основных составляющих национальной безопасности. Именно поэтому перед государственными и военными органами управления стоит задача по разработке эффективных мер нейтрализации негативного информационного воздействия Российской Федерации и противодействия его дальнейшему развертыванию.

В статье также проанализированы подходы к повышению эффективности государственного реагирования на угрозы национальной безопасности в информационной сфере в условиях современного вооруженного конфликта на востоке Украины. Установлено, что для достижения соответствующего уровня

информационной безопасности необходимо сформировать единый государственный механизм обеспечения информационной безопасности. Предложен способ решения задач, возникающих в данной сфере.

Ключевые слова: *информационная безопасность; гибридная война; информационное оружие; общество; государственная политика.*

S. A. Zaporozhets

INFORMATION SECURITY OF UKRAINE IN THE CONDITIONS OF THE HYBRID WAR

The article is devoted to the study of information security of Ukraine in the conditions of hybrid war, confrontation of hybrid threats from the Russian Federation, as well as priority directions for the effective provision of information security in our country. The analysis of this problem shows that the current state of Ukraine's information security system is characterized by an increase in existing threats, and on the other hand by the emergence of new challenges.

Technological innovation processes, information breakthroughs, globalization of the world and tendencies of regional integration, along with providing enormous opportunities for the country's progressive development, have many negative consequences. One of the consequences has been the intensification of hybrid warfare between world countries, including against Ukraine. States' capacity to conduct information and information-psychological operations, to increase the sensitivity of society to the death of civilians and to the loss of military personnel in military conflicts are increasing. In the current conditions of globalization, the technological basis of which is the global information and telecommunication networks and a single information space, there is a tendency to change the principles and methods of management, including in military affairs. The ability of information to influence people's worldview and moods gives them the opportunity to gain an advantage over an adversary without engaging in a forceful confrontation with him. In fact, the correct method of working with information has become a new way of conducting an armed struggle, namely a hybrid war. In this regard, the leading countries of the world are undergoing a gradual transformation of approaches to the formulation of military policy of the state, which are practically embodied in ensuring the information security of the state in the conditions of hybrid war. The full-scale information war of Russia against our state has demonstrated the importance of ensuring information security as one of the main components of national security. In view of the above, the state and military authorities of the country were tasked with developing effective measures to neutralize the negative information impact of the Russian Federation and counteract its further deployment.

The article also analyzes well-known approaches to improving the effectiveness of state response to national security threats in the information sphere in the context of the current armed conflict in eastern Ukraine. It is established that in order to achieve the appropriate level of information security it is necessary to create a single state mechanism for ensuring information security. A method for solving problems arising in this field is proposed.

Keywords: *information security; hybrid war; information weapons; society; public policy.*

УДК 355.40:004.82(477) DOI: 10.46972/2076-1546.2019.17.06

С. С. Гаценко, В. П. Дудник, А. І. Сотніченко, О. М. Ліщенко

ОЦІНКА ЕФЕКТИВНОСТІ ТА НАДАННЯ ПРАКТИЧНИХ РЕКОМЕНДАЦІЙ ЩОДО ФУНКЦІОНУВАННЯ СИСТЕМИ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ В ІНТЕРЕСАХ ПІДГОТОВКИ Й ВЕДЕННЯ СТАБІЛІЗАЦІЙНОЇ ОПЕРАЦІЇ

Воєнно-політична обстановка навколо нашої держави характеризується високою динамічністю і нестабільністю подій та процесів. На фоні зазначеного основним завданням Збройних Сил України на сучасному етапі розбудови є активізація розвідки з метою своєчасного попередження вищого воєнно-політичного керівництва країни про можливу відкриту збройну агресію Російської Федерації, приховані дії деяких інших суміжних держав, що можуть загрожувати національним інтересам. У статті на основі дослідженого впливу зовнішніх та внутрішніх факторів на ефективність функціонування системи радіоелектронної розвідки в інтересах ведення стабілізаційної операції угрупованням військ (сил) на території Донецької та Луганської областей з використанням методів аналізу, синтезу та теорії ймовірностей оцінено ефективність функціонування системи радіоелектронної розвідки, спроможності її сил та засобів викривати зміни в режимах функціонування Збройних Сил, приведення у вищі ступені бойової готовності військ (сил), запобігання активним діям незаконних збройних формувань. Слід зауважити, що результати проведеного оцінювання ефективності вказали на неповну реалізацію об'єктивних можливостей системи радіоелектронної розвідки, а інколи й на їх значне зниження. У статті проведено оцінювання ефективності радіоелектронної розвідки в операції Об'єднаних сил в інтересах підготовки та ведення стабілізаційної операції, що дозволило визначити напрямок подальших наукових досліджень та розробити практичні рекомендацій, які дали можливість підвищити ефективність функціонування системи радіоелектронної розвідки з мінімальними фінансовими витратами.

Ключові слова: *система радіоелектронної розвідки; стабілізаційна операція; ефективність; радіо- і радіотехнічна розвідка; імовірність; об'єкти розвідки; джерела розвідувальних відомостей.*

Постановка проблеми в загальному вигляді. Забезпечення інформаційної переваги над противником на сьогодні стає основною умовою для ведення воєнних операцій. Саме в ході збройної агресії проти України з боку Російської Федерації здійснюється систематичне нарощування бойових спроможностей створеного угруповання російських окупаційних військ (РОВ), яке діє на смоленському, орловсько-воронезькому, донському, кримському операційних напрямках. При цьому з метою стійкого управління військами та оперативного обміну інформацією противником проводяться заходи щодо створення єдиного інформаційного простору. В основу даної концепції покладено нові засоби зв'язку та телекомунікаційні системи. Усі ці заходи зумовлюють широке впровадження радіоелектронних засобів (РЕЗ) у ланки управління військами та зброєю, тому в сучасному збройному конфлікті велике значення необхідно приділяти, зокрема,

ефективності ведення радіоелектронної розвідки (РЕР), оскільки вона є основною складовою воєнної розвідки [1–4, 9].

Аналіз останніх досліджень і публікацій. Стабілізаційна операція є основною операцією військ (сил) під час проведення операції з ліквідації збройного конфлікту на державному кордоні та операції з ліквідації збройного конфлікту всередині держави, а також є одною з ключових у ході відбиття збройної агресії [1–2]. Тому широким застосуванням усіх видів РЕР (радіо- та радіотехнічної розвідки(РР та РТР)) під час проведення стабілізаційної операції не можна нехтувати.

Система РЕР є основним і в багатьох випадках єдиним способом добування розвідувальної інформації (РІ) про противника під час ведення бойових дій [1–5]. У сучасних військових конфліктах, які набувають усе більше ознак гібридності, охоплюють великі площі території зі складним рельєфом, без суцільної лінії фронту, в обстановці, що швидко змінюється, дана система передбачає широке використання різнотипних багатофункціональних мобільних комплексів РЕР на суші, воді та в повітрі [2–3]. Тому удосконалення стану та рівня бойової підготовки особового складу і бойової готовності частин РЕР, структури й побудови частин (підрозділів) РЕР, порядку їх бойового застосування, нарощення оперативно-технічних можливостей засобів і комплексів РЕР та зв'язку, впровадження автоматизованої системи управління (АСУ) розвідкою та обміном РІ однозначно приведе до підвищення ефективності застосування частин та підрозділів РЕР, що, у свою чергу, надасть перевагу над противником у цілому та дозволить підвищити оперативність прийняття управлінських рішень, забезпечити ефективне застосування засобів вогневого ураження та уникнути зайвих втрат.

Як показує практичний досвід авторів, ведення РЕР у зоні проведення операції Об'єднаних сил (ООС) порушує низку проблемних питань, що суттєво впливають на ефективність функціонування системи РЕР, а саме:

у складі сил і засобів РЕР, які розгорнуті в інтересах ООС, знаходиться незначна кількість засобів ультракороткохвильового (УКХ) пеленгування, їх наявність та тактико-технічні характеристики не відповідають умовам сучасної радіоелектронної обстановки (РЕО) у районі проведення операцій;

досвід експлуатації засобів радіопеленгування для визначення місцеположення джерел радіовипромінювань у підрозділах технічної розвідки як позаштатних засобів дав можливість виявити низку недоліків:

недостатня дальність пеленгування (до 5 км). Так, для визначення місця положення кореспондентів, які працюють у районах взводних і ротних опорних пунктів, необхідно перебувати на відстані не далі ніж 500–1500 м від переднього краю;

низька точність визначення напрямку на джерело радіовипромінювання (ДРВ) (похибка від 1,5° до 15°). На відстані 5 км помилка становить до 1 км;

нестабільне функціонування радіорелейного каналу між пеленгаторами, що не дозволяє вести синхронне пеленгування ДРВ;

використання в переносному варіанті без бронезахисту, що ставить під загрозу життя та здоров'я бойової обслуги;

фізико-географічні особливості району проведення ООС (наявність перепадів рельєфу місцевості, великі житлові масиви і промислові об'єкти, насиченість високовольтними

лініями електропередач тощо), а також особливості організації системи управління та зв'язку РОВ висувають особливі вимоги до підбору технічних позицій для маневрених груп РЕР;

низький рівень поточної обробки інформації в групах РЕР оперативно-тактичного угруповання (ОТУ) та відсутній зворотній зв'язок між ним і маневреними групами РЕР;

слабка організація взаємодії між маневреними групами РЕР та напрямківцями ОТУ, деякими начальниками розвідок бригад і батальйонів, нерозуміння ними можливостей та особливостей застосування сил та засобів РЕР в районі ООС;

відсутність засобів зв'язку, що не дозволяє швидко передавати широкоформатну інформацію з гарантованою стійкістю;

відсутність у районі проведення ООС засобів РТР, що не дозволяє якісно відслідковувати постійне нарощування та впровадження противником радіотехнічних засобів (РТЗ) у районі проведення ООС.

Формулювання завдання дослідження. З урахуванням аналізу тенденцій сучасної збройної боротьби, воєнно-політичної обстановки, що склалася довкола України, а також проблемних питань РЕР у районі проведення ООС ***метою статті*** є розробити практичні рекомендації для підвищення ефективності системи РЕР в інтересах підготовки і ведення стабілізаційної операції на основі проведеного оцінювання результатів виконання розвідувальних завдань.

Виклад основного матеріалу. Виходячи з того, що досягнення інформаційної переваги над противником на сьогодні стає основною умовою для успішного ведення операцій, бойових дій, можна стверджувати, що воєнна розвідка, як основний вид інформаційного забезпечення військ (сил), набирає якісно нового важливого значення, при цьому РЕР, будучи складовою воєнної розвідки, викриває до 80% об'єктів (ОР) через роботу їх РЕЗ [1, 6, 8, 12].

Система РЕР Збройних Сил України, як і сам процес її ведення, потребує кількісного оцінювання щодо ефективності її функціонування. Складність і різноманіття завдань розвідки, наявність великої кількості елементів, що взаємопов'язані та залежать один від одного, потоки інформації про результати моніторингу та управління ДРВ зумовлюють необхідність науково обґрунтованого підходу до визначення відповідності результатів функціонування системи РЕР матеріальним, технічним та іншим витратам.

Ведення РЕР – це конфлікт, у якому беруть участь дві протиборчі сторони (системи), що переслідують взаємопротилежні цілі. У даній ситуації противник прагне проводити усі заходи в таємниці, швидко, а також застосовувати дезінформацію і радіомаскування.

У свою чергу, підрозділи, частини РЕР вишукують методи, способи та прийоми для виконання своїх завдань і досягнення цілей розвідки, тобто прагнуть розв'язати поставлені перед ними задачі з максимально можливою ефективністю.

Ефективність, як правило, визначають за результатами функціонування об'єктів та систем, що оцінюються, у межах їхнього цільового призначення. Тобто ефективність є ступенем реалізації можливостей об'єкта (системи) відповідно до його (її) призначення [13–22].

Під ефективністю системи РЕР та її елементів (підрозділів, частини або з'єднання РЕР) розуміємо здатність складових і системи в цілому виконати розвідувальні завдання

та досягти цілей моніторингу у встановлений термін із максимальною повнотою й достовірністю [13–22].

За узагальнений показник (критерій) оцінки ефективності функціонування системи РЕР, як чисельної характеристики, яка кількісно відображає якість виконуваних завдань, можна обрати відношення значень узагальненого показника призначення до значення показника, що вимагається:

$$Z = W / W_{TP}, \qquad (1)$$

де Z – узагальнений критерій ефективності;

W – значення узагальненого показника призначення;

W_{TP} – значення показника, що вимагається.

Одним із головних розвідувальних завдань, що вирішується силами та засобами РЕР, є викриття об'єктів противника в смузі розвідки на задану глибину та відстеження їхнього стану. За результатами його виконання викривається склад і розміщення угруповання противника на місцевості, а також діяльність і наміри військ протиборчої сторони. Враховуючи це, за основний узагальнений показник призначення слід використовувати показник, що характеризує кількість ОР, що очікується викрити або підтвердити в заданих межах розвідки з необхідною достовірністю за певний період часу. Він є узагальненою характеристикою бойових можливостей сил і засобів РЕР та функціонально включає загальні показники: повноту, достовірність та своєчасність виконання розвідувальних завдань.

У свою чергу, загальні показники визначають за сукупністю відповідних часткових показників, основною вимогою при цьому є наявність між ними однозначної відповідності з необхідною точністю. Крім того, часткові показники ефективності повинні мати фізичний сенс (наочність), розрахунковість, критичність щодо завдань дослідження, бути суттєвими (значно впливати на результати розрахунку ефективності).

До основних часткових показників функціонування системи РЕР належать:

імовірність електромагнітної доступності до джерел у смузі розвідки, кількість (у відсотках) доступних джерел;

імовірність виявлення та очікувана кількість (у відсотках) виявлених джерел за заданий час;

точність визначення місцеположення радіоелектронних засобів;

імовірність пошуку будь-якого випромінювання;

ефективність спостереження;

очікувана кількість (у відсотках) радіомереж (РЕЗ), що викриваються за певний час ведення розвідки.

Створення сучасної розвідувальної системи здійснюється шляхом реформування частин та підрозділів РЕР, оптимізації їх організаційно-штатної структури. Це, у свою чергу, вимагає:

удосконалення процесу ведення РЕР, а саме добування РІ, її збір, обробка, аналіз та накопичення;

розробки новітніх та удосконалення наявних засобів РЕР, які знаходяться на озброєнні частин та підрозділів РЕР.

Одним із нових підходів можна вважати практику більш широкого та гнучкого застосування маневрених груп РЕР у стабілізаційній операції.

Використовуючи відому методику розрахунку показників ефективності бойового застосування сил і засобів розвідки, але з урахуванням особливостей ведення РЕР у районі проведення ООС та відповідних вихідних даних, розрахунок усіх часткових показників здійснюємо послідовно, зважаючи на те, як вони залежать один від одного [23, 24].

Оцінка ймовірності електромагнітної доступності $P_{ЕМД}$ джерел у смузі розвідки та очікуваної кількості доступних джерел

Розрахунок $P_{ЕМД}$ здійснюємо для усіх РЕЗ ОР відповідно до прогнозованого угруповання в смузі розвідки і РЕО, що створюється сукупністю працюючих РЕЗ противника [23]. Середнє значення $\overline{P_{ЕМД}}$ визначаємо для кожного типу ОР за формулою

$$\overline{P_{ЕМД}} = \frac{\sum_{i=1}^{n} P_{РМДi}}{n}, \tag{2}$$

де $\overline{P_{ЕМД_i}}$ – імовірність електромагнітної доступності РЕЗ *i*-го типу на об'єкті;

n – кількість РЕЗ *i*-го типу на ОР.

Оцінюємо $P_{ЕМД}$ усіх джерел на об'єктах різних типів усередненням значень $P_{ЕМД}$ за усіма типами об'єктів.

Орієнтовну кількість доступних джерел (радіомереж) оцінюємо як відношення очікуваної кількості доступних РЕЗ для РР до середньої кількості радіостанцій у радіомережах:

$$N_{р/мдост} = \frac{N^{\Sigma}_{РЕЗдост}}{\overline{n_{р/м}}}, \tag{3}$$

де $N_{р/мдост}$ – орієнтовна кількість радіомереж у смузі розвідки;

$\overline{n_{р/м}}$ – середня кількість радіостанцій у радіомережі.

Імовірність пошуку будь-якого випромінювання в разі послідовного перегляду діапазону пошуку для підсистеми РР розраховуємо за такою формулою:

$$P_{пош}(\Delta t) = 1 - \left[\frac{\overline{T_u} - \overline{t_u}}{\overline{T_u}} e^{-\frac{F_c + \Delta F}{\gamma_f (\overline{T_u} + \overline{t_u})}} \right]^{\frac{\Delta t_p}{\overline{T_{пр}}}}, \tag{4}$$

де $\overline{t_u}$ – середня тривалість випромінювання РЕЗ;

$\overline{T_u}$ – середній період роботи РЕЗ;

ΔF – смуга пропускання приймального пристрою;

F_c – ширина спектра сигналу;

γ_f – середня швидкість перестроювання за частотою;

Δt_p – оцінюваний період часу ведення розвідки;

$\overline{T_{пр}} = \overline{\Phi_{vi} / \gamma_f}$ – період проходу ділянки діапазону пошуку;

$\overline{\Phi_{vi}} = \dfrac{\Delta F_\Sigma}{N_{постів}}$ – відношення загального діапазону пошуку на кількість виділених для цього постів.

Ефективність спостереження $P_{спостер}$ розраховуємо за виразом

$$P_{спостер} = 1 - \left[\frac{T_{сп} - T_{випр}}{T_{сп}} e^{-\frac{T_{пп} - T_{випр}}{T_{сп} - T_{випр}}} \right]^{\frac{\Delta t_{розв}}{T_{прох}}}, \tag{5}$$

де $T_{сп}$ – час спостереження, що дорівнює сумі часу випромінювання джерела та часу пропуску між випромінюваннями $T_{проп}, T_{випр}$;

$T_{пп}$ – час перебудови за банком частот, який дорівнює сумі часу затримки на одній чарунці та часу пропуску між повторним налаштуванням на дану чарунку $T_{розв} + T_{проп}$.

Розрахунки місцевизначення є важливими для оцінювання ефективності системи РЕР в інтересах стабілізаційної операції, але не проводилися з причини відсутності вихідних даних щодо наявності (відсутності) радіопеленгаторних (РПл) мереж у системі РЕР у зоні проведення ООС.

Важливим показником, який впливає на виконання завдання РЕР у сучасних умовах, є ймовірність викриття роботи засобів стільникового зв'язку P_{GSM}, що знаходимо за таким виразом:

$$P_{GSM} = \frac{N_{i\text{поста}}}{N_{важл}}, \tag{6}$$

де $N_{i\text{поста}} = \dfrac{N_{важл}}{m}$;

$N_{важл} = N_{заг.\,поста} * 0{,}1$;

m – кількість маневрених груп.

Розрахуємо ефективність функціонування підсистеми РР системи РЕР:

$$P_{РР} = P_{ЕМД} P_{пош}(\Delta t) P_{спост} P_{GSM}. \tag{7}$$

Визначимо ефективність функціонування підсистеми РТР системи РЕР:

$$P_{РТР} = P_{ЕМД} P_{мсп} P_{спост} P_{роб}. \tag{8}$$

Загальну оцінку ефективності системи РЕР у стабілізаційній операції розраховуємо за таким виразом:

$$P_{РЕР} = \left(1 - \left(1 - P_{РР}\right)\left(1 - P_{РТР}\right)\right). \tag{9}$$

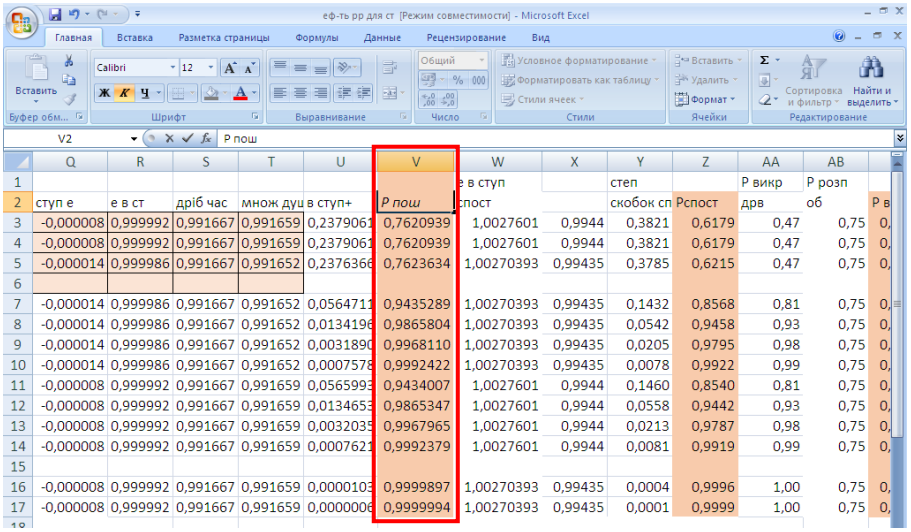
Значення цих показників залежать від варіантів бойового застосування сил і засобів РЕР, що дозволить у результаті їх оцінювання отримати найбільш ефективний, який найбільше сприятиме виконанню розвідувальних завдань. Отже, загальна ефективність системи РЕР у стабілізаційній операції є складною системою взаємопов'язаних показників функціонування сил і засобів РЕР.

Для проведення розрахунків були використані вихідні дані щодо можливостей з організації зв'язку та застосування активних РТЗ у системі управління військами та зброєю ОТУ незаконних збройних формувань (НЗФ) та РОВ на тимчасово окупованій території (ТОТ) Донецької та Луганської областей. Станом на жовтень 2019 року на постійному спостережені сил і засобів РЕР ООС знаходиться близько 120 радіомереж системи зв'язку 1 та 2 армійських корпусів.

Розрахунок показників ефективності системи РЕР проведено відповідно до описаної вище методики з використанням програмного забезпечення Microsoft Office Excel 2007.

Як показує досвід ведення РЕР, не всі маневрені групи мають однакову ймовірність електромагнітної доступності $P_{ЕМД}$ РЕЗ противника у зв'язку з впливом зовнішніх факторів. Виходячи з цього, прийнято, що: 60% маневрених груп $P_{ЕМД} \approx 0{,}85$; 30% маневрених груп $P_{ЕМД} \approx 0{,}65$; 10% маневрених груп $P_{ЕМД} \approx 0{,}45$. Отже, середнє значення ймовірності для розрахунку дорівнює $\overline{P_{ЕМД}} \approx 0{,}755$.

Розрахунок імовірності виявлення та очікуваної кількості виявлених джерел за заданий час проводимо відповідно до (4) та за допомогою Microsoft Office Excel 2007 (рис. 1).

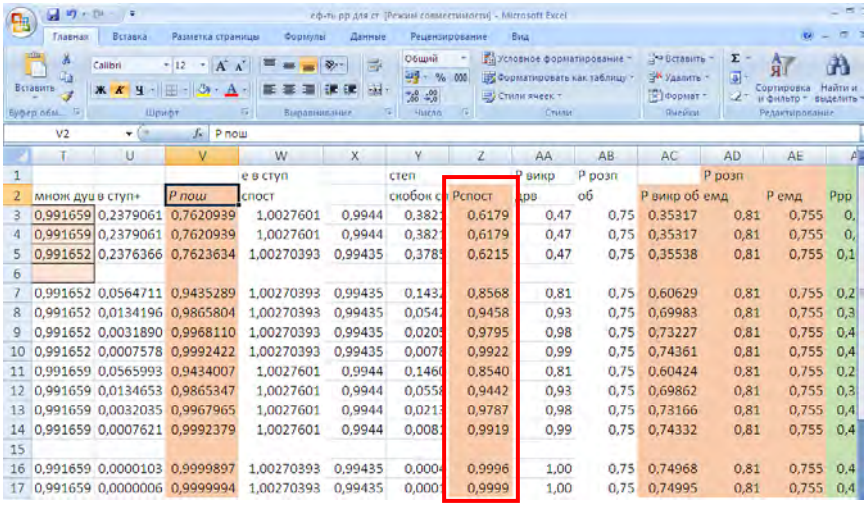


	Q	R	S	T	U	V	W	X	Y	Z	AA	AB
1							е в ступ		степ		Р викр	Р розп
2	ступ е	е в ст	дріб час	множ дуц	в ступ+	Р пош	спост		скобок сп	Рспост	дрв	об
3	-0,000008	0,999992	0,991667	0,991659	0,2379061	0,7620939	1,0027601	0,9944	0,3821	0,6179	0,47	0,75
4	-0,000008	0,999992	0,991667	0,991659	0,2379061	0,7620939	1,0027601	0,9944	0,3821	0,6179	0,47	0,75
5	-0,000014	0,999986	0,991667	0,991652	0,2376366	0,7623634	1,00270393	0,99435	0,3785	0,6215	0,47	0,75
6												
7	-0,000014	0,999986	0,991667	0,991652	0,0564711	0,9435289	1,00270393	0,99435	0,1432	0,8568	0,81	0,75
8	-0,000014	0,999986	0,991667	0,991652	0,0134196	0,9865804	1,00270393	0,99435	0,0542	0,9458	0,93	0,75
9	-0,000014	0,999986	0,991667	0,991652	0,0031890	0,9968110	1,00270393	0,99435	0,0205	0,9795	0,98	0,75
10	-0,000014	0,999986	0,991667	0,991652	0,0007578	0,9992422	1,00270393	0,99435	0,0078	0,9922	0,99	0,75
11	-0,000008	0,999992	0,991667	0,991659	0,0565993	0,9434007	1,0027601	0,9944	0,1460	0,8540	0,81	0,75
12	-0,000008	0,999992	0,991667	0,991659	0,0134653	0,9865347	1,0027601	0,9944	0,0558	0,9442	0,93	0,75
13	-0,000008	0,999992	0,991667	0,991659	0,0032035	0,9967965	1,0027601	0,9944	0,0213	0,9787	0,98	0,75
14	-0,000008	0,999992	0,991667	0,991659	0,0007621	0,9992379	1,0027601	0,9944	0,0081	0,9919	0,99	0,75
15												
16	-0,000008	0,999992	0,991667	0,991659	0,0000103	0,9999897	1,00270393	0,99435	0,0004	0,9996	1,00	0,75
17	-0,000008	0,999992	0,991667	0,991659	0,0000006	0,9999994	1,00270393	0,99435	0,0001	0,9999	1,00	0,75

Рис. 1. Результати розрахунків імовірності виявлення та очікуваної кількості виявлених ДРВ

Ефективність спостереження $P_{спостер}$ розраховуємо за (5), результати наведено на рис. 2.

Одна маневрена група в зоні ООС була укомплектована пеленгаторною технікою, що дає можливість створення РПл мережі та проведення розрахунків місцевизначення ДРВ. Розраховано $N_{ДРВ\ виявл.\ ij}$ за умови, що за одну годину один пеленгаторний пост виявляє 30% ДРВ у смузі розвідки. Визначено: $N_{ДРВ\ викр.}(\Delta t)$ становить 25%; $N_{викр.об}(\Delta t)$ – 19%; $N_{викр.}$ ОР, які викриваються силами і засобами РР через роботу РЕЗ, становить 0,0179.



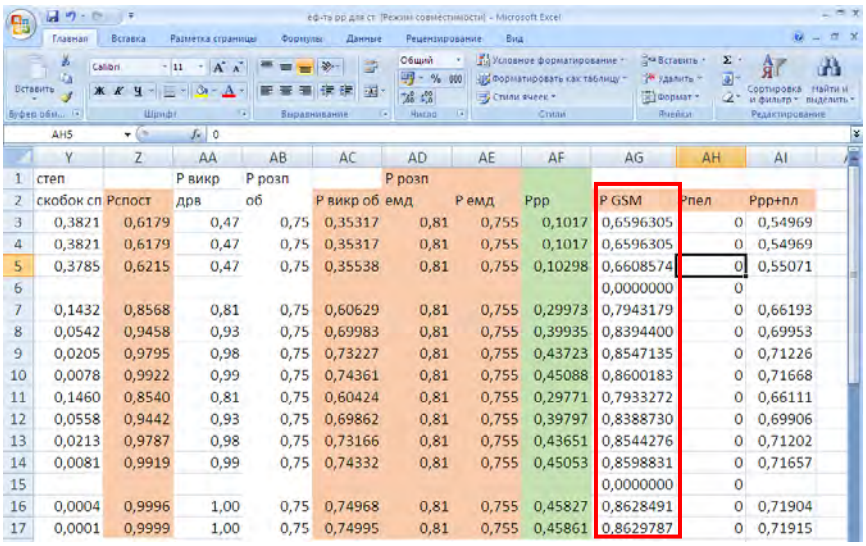
	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE
1				е в ступ		степ		Р викр	Р розп		Р розп	
2	множ дуп	в ступ+	*Р пош*	спост		скобок сп	Рспост	дрв	об	Р викр об	емд	Р емд	Рпр
3	0,991659	0,2379061	0,7620939	1,0027601	0,9944	0,3821	0,6179	0,47	0,75	0,35317	0,81	0,755	0,
4	0,991659	0,2379061	0,7620939	1,0027601	0,9944	0,3821	0,6179	0,47	0,75	0,35317	0,81	0,755	0,
5	0,991652	0,2376366	0,7623634	1,00270393	0,99435	0,3785	0,6215	0,47	0,75	0,35538	0,81	0,755	0,1
6													
7	0,991652	0,0564711	0,9435289	1,00270393	0,99435	0,1432	0,8568	0,81	0,75	0,60629	0,81	0,755	0,2
8	0,991652	0,0134196	0,9865804	1,00270393	0,99435	0,0542	0,9458	0,93	0,75	0,69983	0,81	0,755	0,3
9	0,991652	0,0031890	0,9968110	1,00270393	0,99435	0,0205	0,9795	0,98	0,75	0,73227	0,81	0,755	0,4
10	0,991652	0,0007578	0,9992422	1,00270393	0,99435	0,0078	0,9922	0,99	0,75	0,74361	0,81	0,755	0,4
11	0,991659	0,0565993	0,9434007	1,0027601	0,9944	0,1460	0,8540	0,81	0,75	0,60424	0,81	0,755	0,2
12	0,991659	0,0134653	0,9865347	1,0027601	0,9944	0,0558	0,9442	0,93	0,75	0,69862	0,81	0,755	0,3
13	0,991659	0,0032035	0,9967965	1,0027601	0,9944	0,0213	0,9787	0,98	0,75	0,73166	0,81	0,755	0,4
14	0,991659	0,0007621	0,9992379	1,0027601	0,9944	0,0081	0,9919	0,99	0,75	0,74332	0,81	0,755	0,4
15													
16	0,991659	0,0000103	0,9999897	1,00270393	0,99435	0,0004	0,9996	1,00	0,75	0,74968	0,81	0,755	0,4
17	0,991659	0,0000006	0,9999994	1,00270393	0,99435	0,0001	0,9999	1,00	0,75	0,74995	0,81	0,755	0,4

Рис. 2. Результати розрахунків ефективності спостереження за ДРВ

Отже, для викриття одного об'єкта розвідки у визначеному секторі одним пеленгаторним постом $N_{викр.} = 1$ необхідно витратити значний час, що є вкрай не ефективно.

Важливою складовою функціонування підсистеми РР є викриття роботи засобів стільникового зв'язку P_{GSM}, що становить значну частку РІ, яку добувають маневрені групи в зоні проведення ООС (близько 300 000 сеансів зв'язку за добу).

На рис. 3 показано результати розрахунків $P_{GSM} = 0{,}68$ згідно з виразом (6).

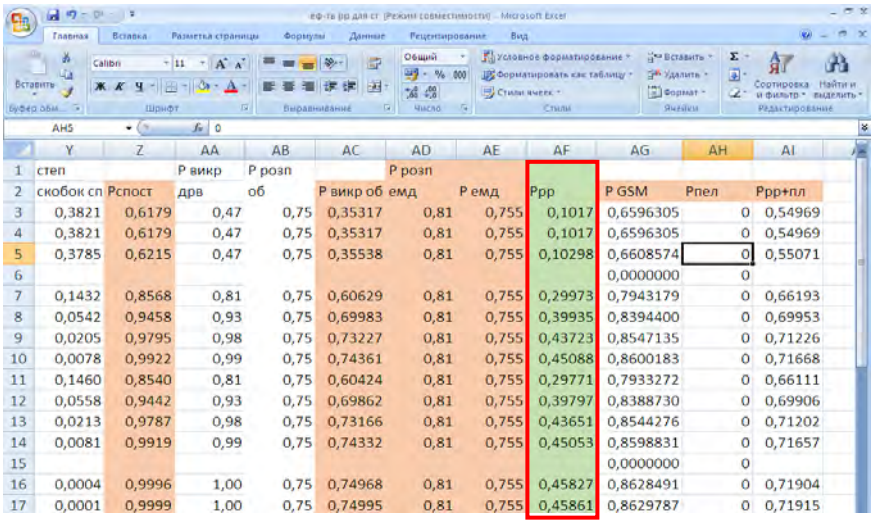


	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI
1	степ		Р викр	Р розп		Р розп					
2	скобок сп	Рспост	дрв	об	Р викр об	емд	Р емд	Рпр	Р GSM	Рпел	Рпр+пл
3	0,3821	0,6179	0,47	0,75	0,35317	0,81	0,755	0,1017	0,6596305	0	0,54969
4	0,3821	0,6179	0,47	0,75	0,35317	0,81	0,755	0,1017	0,6596305	0	0,54969
5	0,3785	0,6215	0,47	0,75	0,35538	0,81	0,755	0,10298	0,6608574	0	0,55071
6									0,0000000	0	
7	0,1432	0,8568	0,81	0,75	0,60629	0,81	0,755	0,29973	0,7943179	0	0,66193
8	0,0542	0,9458	0,93	0,75	0,69983	0,81	0,755	0,39935	0,8394400	0	0,69953
9	0,0205	0,9795	0,98	0,75	0,73227	0,81	0,755	0,43723	0,8547135	0	0,71226
10	0,0078	0,9922	0,99	0,75	0,74361	0,81	0,755	0,45088	0,8600183	0	0,71668
11	0,1460	0,8540	0,81	0,75	0,60424	0,81	0,755	0,29771	0,7933272	0	0,66111
12	0,0558	0,9442	0,93	0,75	0,69862	0,81	0,755	0,39797	0,8388730	0	0,69906
13	0,0213	0,9787	0,98	0,75	0,73166	0,81	0,755	0,43651	0,8544276	0	0,71202
14	0,0081	0,9919	0,99	0,75	0,74332	0,81	0,755	0,45053	0,8598831	0	0,71657
15									0,0000000	0	
16	0,0004	0,9996	1,00	0,75	0,74968	0,81	0,755	0,45827	0,8628491	0	0,71904
17	0,0001	0,9999	1,00	0,75	0,74995	0,81	0,755	0,45861	0,8629787	0	0,71915

Рис. 3. Результати розрахунків ефективності спостереження за роботою засобів стільникового зв'язку

Відповідно до розрахунків за (8) ефективність функціонування підсистеми РР системи РЕР у стабілізаційній операції за досвідом проведення ООС становить $P_{PP} = 0{,}45$. У зв'язку з відсутністю в складі маневрених груп РЕР у зоні проведення ООС засобів РТР $P_{PTP} = 0$. Отже, цей показник у розрахунку загальної оцінки ефективності системи РЕР не враховувався. Таким чином, загальну оцінку ефективності системи РЕР у стабілізаційній

операції за досвідом ООС розраховуємо за одним показником ефективності підсистеми РР системи РЕР, маємо P_{PP} = 0,45 (рис. 4). Даний показник вказує на те, що система РЕР може виконувати поставлені бойові завдання в зоні проведення ООС щодо викриття намірів, діяльності та змін у системі управління ОТУ НЗФ та РОВ на ТОТ Донецької та Луганської областей, але не в повній мірі відповідає необхідним вимогам ефективності щодо ведення РЕР в інтересах операції в сучасних умовах.



	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI
1	степ		Р викр	Р розп		Р розп					
2	скобок сп	Рспост	дрв	об	Р викр об	емд	Р емд	Ррр	Р GSM	Рпел	Ррр+пл
3	0,3821	0,6179	0,47	0,75	0,35317	0,81	0,755	0,1017	0,6596305	0	0,54969
4	0,3821	0,6179	0,47	0,75	0,35317	0,81	0,755	0,1017	0,6596305	0	0,54969
5	0,3785	0,6215	0,47	0,75	0,35538	0,81	0,755	0,10298	0,6608574	0	0,55071
6									0,0000000	0	
7	0,1432	0,8568	0,81	0,75	0,60629	0,81	0,755	0,29973	0,7943179	0	0,66193
8	0,0542	0,9458	0,93	0,75	0,69983	0,81	0,755	0,39935	0,8394400	0	0,69953
9	0,0205	0,9795	0,98	0,75	0,73227	0,81	0,755	0,43723	0,8547135	0	0,71226
10	0,0078	0,9922	0,99	0,75	0,74361	0,81	0,755	0,45088	0,8600183	0	0,71668
11	0,1460	0,8540	0,81	0,75	0,60424	0,81	0,755	0,29771	0,7933272	0	0,66111
12	0,0558	0,9442	0,93	0,75	0,69862	0,81	0,755	0,39797	0,8388730	0	0,69906
13	0,0213	0,9787	0,98	0,75	0,73166	0,81	0,755	0,43651	0,8544276	0	0,71202
14	0,0081	0,9919	0,99	0,75	0,74332	0,81	0,755	0,45053	0,8598831	0	0,71657
15									0,0000000	0	
16	0,0004	0,9996	1,00	0,75	0,74968	0,81	0,755	0,45827	0,8628491	0	0,71904
17	0,0001	0,9999	1,00	0,75	0,74995	0,81	0,755	0,45861	0,8629787	0	0,71915

Рис. 4. Результати розрахунків загальної ефективності функціонування системи РЕР у стабілізаційній операції за показником ведення РР

Практичні рекомендації щодо підвищення ефективності ведення РЕР. Рекомендації щодо підвищення ефективності ведення РР та місцевизначення ДРВ

Для визначення місцеположення вузлів зв'язку (радіостанцій) тактичної ланки управління необхідно розгорнути РПл мережу УКХ діапазону в складі п'яти мобільних РПл груп, кожна з яких повинна відповідати таким вимогам:

висока точність пеленгування (виходячи з теоретичних основ пеленгування на відкритій місцевості в УКВ діапазоні (100–800 мГц) точність пеленгування не повинна перевищувати 0,8–1°);

висока чутливість РПл (оскільки більшість радіостанцій противника функціонують у смузі пропускання до 6 кГц, РПл повинні мати ширину смуги пропускання 9 кГц та чутливість 1 мкВ/м у діапазоні 100–800 мГц (діапазон, який переважно використовується РОВ) і 5 мкВ/м у діапазоні 25–100 мГц; 800–2000 мГц);

невелика тривалість часу розгортання та згортання, що дасть можливість швидкої зміни місцеположення в разі необхідності (виявлення противником, здійснення манеру на місцевості для забезпечення потрібного рівня електромагнітної доступності (ЕМД)).

Однією з ключових вимог до розгортання пеленгаторної групи є підбір технічної позиції для кожного РПл, яка забезпечить стійку ЕМД до ДРВ.

Із досвіду застосування засобів РЕР в ООС відомо, що маневрені групи РЕР діють у районах, де переважає місцевість із пагорбами з перепадами висот від 10 м до 250 м. Враховуючи, що радіохвилі в УКХ діапазоні розповсюджуються на дальність прямої видимості й не здатні огинати великогабаритні природні та штучні перешкоди, для досягнення найбільшого значення ЕМД позицію для РПл обирають на панівних висотах (рис. 5).

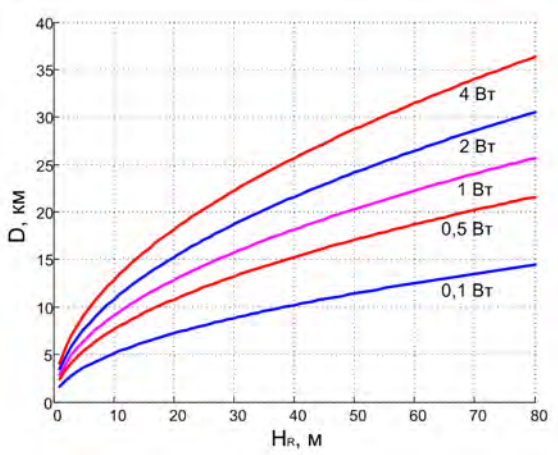


Рис. 5. Графік залежності дальності виявлення ДРВ від висоти підйому приймальної антени з урахуванням рівня ЕМД

При цьому під час вибору бойового порядку РПл групи необхідно забезпечити оптимальну базу між центральною та відомими РПл станціями.

Враховуючи наведені вище значення, можливо знайти значення бази між РПл. У разі використання РПл з чутливістю 1 мкВ/м та підйомом антенної системи на висоту 10–18 м для пеленгування радіостанції потужністю 1 Вт, база між пеленгаторами не повинна перевищувати 15 км.

Для визначення місцеположення радіостанції потужністю 5 Вт антенну систему достатньо підняти на 2 м. Відстань між пеленгаторами не повинна перевищувати 14 км. При цьому дальність виявлення ДРВ становитиме не менше 20 км.

З метою розрахунків кутів закриття з урахуванням місцевості рекомендовано використовувати спеціалізоване програмне забезпечення (рис. 6).

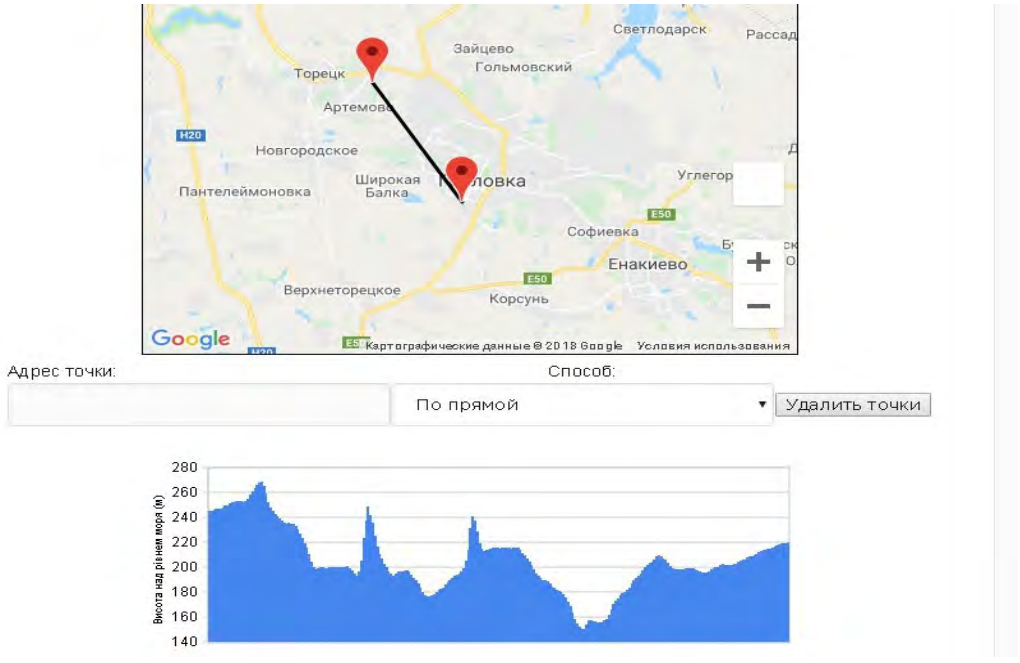
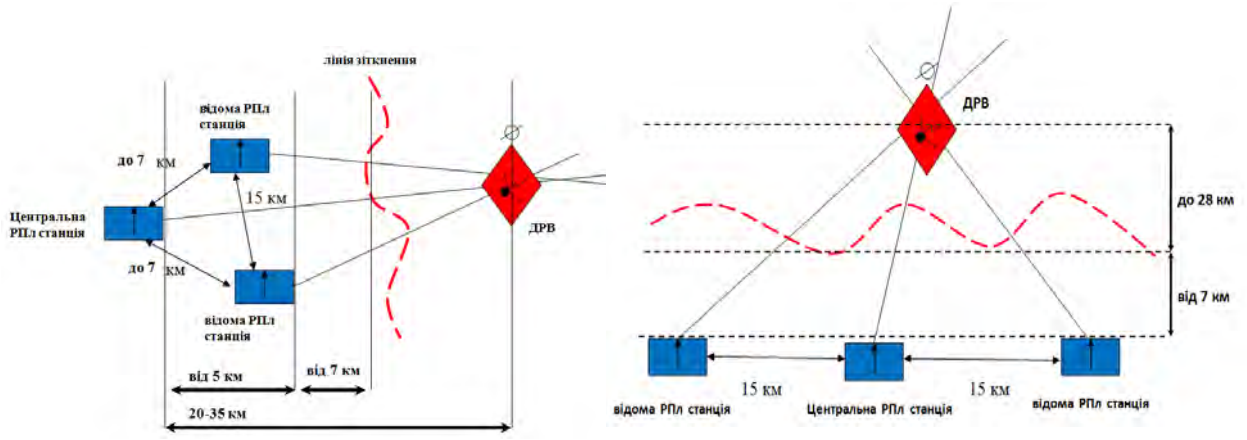


Рис. 6. Приклад програмного забезпечення для визначення перепаду висот (https://qrz.pp.ua/vysota)

Для розгортання пеленгаторної групи пропонуємо використовувати бойові порядки, наведені на рис. 7.



а) *б)*

Рис. 7. Варіанти бойового порядку РПл групи у складі трьох радіопеленгаторів: а) забезпечує високу точність пеленгування; б) забезпечує максимальне використання бази по фронту, збільшує дальність виявлення ДРВ

З урахуванням визначених вимог, а також бойового порядку противника, протяжності лінії бойового зіткнення, найбільш ефективним буде застосування п’яти комплексів УКХ пеленгування (по 3 РПл у кожному), які розташовані в бойових порядках на відстані не ближче 7 км від лінії зіткнення (рис. 8).

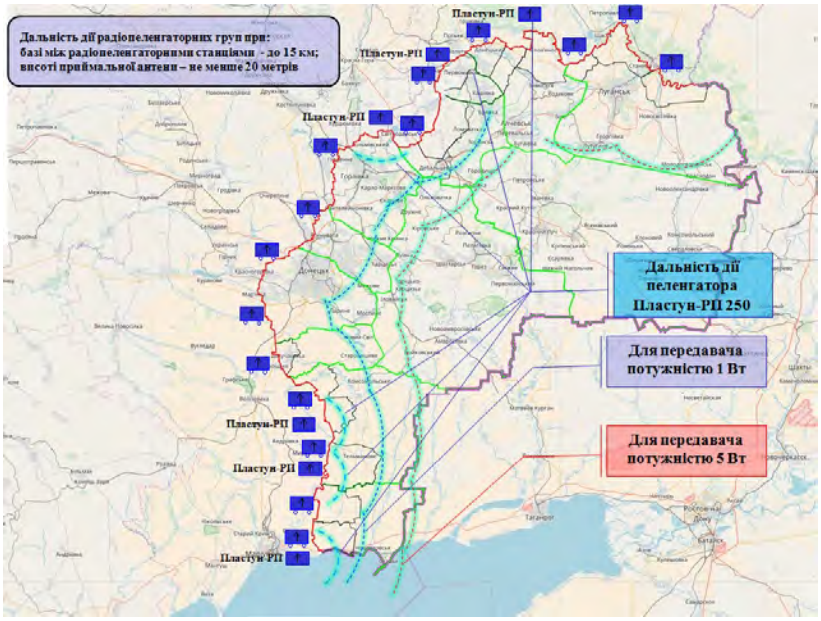


Рис. 8. Варіант розгортання РПл мережі УКХ діапазону в ООС

Обґрунтовано раціональну кількість комплексів УКХ пеленгування та вибір позицій розташовування в бойових порядках угруповання військ в операції для підвищення ЕМД до ДРВ та покращення точності їх місцевизначення.

Висновки. Здійснені розрахунки показників ефективності функціонування системи РЕР в ООС вказують на те, що вона може виконувати поставлені бойові завдання з ведення РЕР , зокрема викриття намірів, діяльності та змін у системі управління ОТУ НЗФ і РОВ на ТОТ Донецької та Луганської областей, але при цьому вона не в повній мірі відповідає необхідним вимогам ефективності щодо ведення РЕР в інтересах проведення операції в сучасних умовах.

Розроблені практичні рекомендації дозволяють нарощувати можливості системи РЕР та покращувати її ефективність у стабілізаційній операції. Подальшим актуальним напрямком наукових досліджень є автоматизація процесу обробки значних об'ємів добутих розвідувальних відомостей для підвищення оперативності обробки.

СПИСОК ЛІТЕРАТУРИ

1. 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 наук.-практ. семінару "Основні напрямки застосування космічних систем та геоінформаційного забезпечення в інтересах національної безпеки і оборони". Київ : НУО України, 2015. С. 35–41.

2. Калашніков Є. М., Гаценко С. С., Шишацький А. В. Аналіз характеру сучасних воєнних конфліктів // International scientific and practical conference ("Challenges of hybrid war: information dimension" : conference proceedings, August 16–17, 2019). Vilnius : Izdevnieciba «Baltija Publishing». 2019.P. 24–27.

3. Гаценко С. С., Бігун Н. С. Проблеми забезпечення інформаційної безпеки в умовах ведення гібридних війн // Тези доповідей наук.-практ.конф. («Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн», 24–25 жовтня 2019 р., м. Житомир). Житомир : ЖВІ, 2019. С. 155–159.

4. Богданович В. Ю., Воробйов Г. П. Шляхи удосконалення методичних основ та інструментальних засобів підтримки процесів прийняття рішень в системі забезпечення національної безпеки // Сучасні інформаційні технології у сфері безпеки та оборони. Київ : НУО України, 2016. № 3 (27). С. 15–20.

5. Лаврут О. О., Грищук К. П. Сучасний стан та тенденції розвитку перспективних систем та засобів зв'язку в Збройних Силах України за досвідом антитерористичної операції // Труди університету. Київ : НУОУ, 2015. № 6 (133). С. 181–190. Інв. № 46819т – НУО України.

6. Варламов І. Д., Гаценко С. С., Бучинський Ю. А. Особливості побудови та практичної реалізації автоматизованої системи управління розвідкою // Труди університету. Київ : НУО України, 2017. № 6 (145). С. 44–54. Інв. № 1923т – ЖВІ.

7. Небога О. В., Кокорін В. О., Цвєтков Є. В. Розвідувальне забезпечення антитерористичної операції : інф.-аналіт. матеріал. Київ : НУО України, 2015. 17 с.

8. Автоматизована система підтримки прийняття рішення щодо визначення типів джерел радіовипромінювань / І. Д. Варламов, М. А. Роговець, С. С. Гаценко, Ю. А. Бучинський. // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2017. Вип. 14. С. 146–156.

9. Організація системи управління (пункти управління та вузли зв'язку) та зв'язку військ ЗС РФ, що беруть участь у збройному конфлікті на Сході України : довідник. Київ : ГУР МО України, 2019. 31 с.
10. Пермяков О. Ю., Варламов І. Д., Гаценко С. С., Панкратова О. С. Удосконалення автоматизованих систем управління військами на основі раціонального розподілу інформаційних потоків в інтегрованому командному середовищі // Тези доповідей XX Всеукр. наук.-практ. конф. ("Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення", м. Житомир, 28 листоп. 2014 р.). Житомир : ЖВІ, 2014. С. 49–50.
11. Щерба А. А. Еволюція розвідувально-вогневої технології на основі мережецентричних принципів управління // Вісник Хмельницького нац. ун-ту. Хмелницький : 2014. № 4. С. 109–112.
12. Гаценко С. С. Аналіз існуючого стану автоматизованих систем управління військами Збройних Сил України та шляхи їх удосконалення // Зб. наук. праць Центру воєнно-стратегічних досліджень НУО України ім. Івана Черняховського. 2015. № 2 (54). С. 85–90.
13. Соловйов В. В. Можливі шляхи інтенсифікації процесу збору, обробки та передачі інформації за протидіючу сторону в системі управління АК // Труди академії. Київ : НАО України, 2004. № 48. С. 78–86.
14. Інструкція з організації та ведення радіоелектронної розвідки в Міністерстві оборони України та Збройних Силах України. Київ : ГУР МО України, 2016. 52 с. Інв. № 1515–ЖВІ.
15. Військовий стандарт 01.101.104. Воєнна розвідка. Інформаційна діяльність. Терміни та визначення. Вид. 1. Київ : МО України, 2009. 24 с.
16. Військовий стандарт 01.101.001. Воєнна розвідка. Терміни та визначення. Вид. 2. Київ : МО України, 2011. 24 с.
17. Військовий стандарт 01.101.103. Воєнна розвідка. Радіоелектронна розвідка. Терміни та визначення. Київ : МО України, 2008. 22 с.
18. Організація оперативно-інформаційної роботи в системі РЕР Збройних Сил України : підручник / За заг. ред. О. В. Небога. Київ : НУОУ, 2016. 248 с.
19. Інструкція з ОІР у з'єднаннях (військових частинах) РЕР. Київ : ГУР МО України, 2004. 59 с. Інв. № 585т – ЖВІ.
20. Про затвердження Тимчасової настанови з оперативної розвідки : наказ нач-ка Генерального штабу – Головнокомандувача Збройних Сил України від 05.07.2016 № 09. Київ : МО України, 2016. 178 с. Інв. № 47264т – НУО України.
21. Гончаров Ю. И. Теоретические основы радио и радиотехнической разведки. Ленинград : ВАС, 1989. 374 с.
22. Смірнов Ю. О. Основи радіоелектронної розвідки. Ч. 1. Розвідувально-інформаційний процес, основні моделі системи РЕР: ефективність і напрями її подальшого розвитку. Київ : НДІ ГУР МО України, 2009. 155 с.
23. Бакуменко Ф. О. Методика оцінки ефективності воєнної розвідки в операції і бою. Київ : НАО України, 1998. 64 с.
24. Смирнов Ю. А. Радиотехническая разведка. Москва : Воениздат, 2001. 456 с.

Подано 17.12.2019

С. С. Гаценко, В. П. Дудник, А. И. Сотниченко, А. Н. Лищенко

ОЦЕНКА ЭФФЕКТИВНОСТИ И ПРЕДОСТАВЛЕНИЯ ПРАКТИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО ФУНКЦИОНИРОВАНИЮ СИСТЕМЫ РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ В ИНТЕРЕСАХ ПОДГОТОВКИ И ВЕДЕНИЯ СТАБИЛИЗАЦИОННОЙ ОПЕРАЦИИ

Военно-политическая обстановка вокруг нашего государства характеризуется высокой динамичностью и нестабильностью событий и процессов. На фоне указанного основной задачей Вооруженных Сил Украины на современном этапе развития является активизация разведки с целью своевременного предупреждения высшего военно-политического руководства страны о возможной открытой вооруженной агрессии Российской Федерации, скрытых действиях других сопредельных государств, которые могут угрожать национальным интересам. В статье на основе исследованного влияния внешних и внутренних факторов на эффективность функционирования системы радиоэлектронной разведки в интересах ведения стабилизационной операции группировкой войск (сил) на территории Донецкой и Луганской областей с использованием методов анализа, синтеза и теории вероятности проведена оценка эффективности функционирования системы радиоэлектронной разведки, возможностей ее сил и средств разоблачать изменения в режимах функционирования Вооруженных Сил, приведения в высшие степени боевой готовности войск (сил), предупреждения активных действий незаконных вооруженных формирований. Следует отметить, что проведенное оценивание эффективности указало на неполную реализацию объективных возможностей системы радиоэлектронной разведки, а в ряде случаев и на их значительное снижение. В статье оценена эффективность радиоэлектронной разведки в операции Объединенных сил в интересах подготовки и ведения стабилизационной операции, что позволило определить направление дальнейших научных исследований и разработать практические рекомендации, позволившие повысить эффективность функционирования системы радиоэлектронной разведки с минимальными финансовыми затратами.

Ключевые слова: *система радиоэлектронной разведки; стабилизационная операция; эффективность; радио- и радиотехническая разведка; вероятность; объекты разведки; источники разведывательных сведений.*

S. S. Hatsenko, V. P. Dudnik, A. I. Sotnichenko, O. M. Lishchenko

EVALUATION OF THE EFFICIENCY AND PROVISION OF PRACTICAL RECOMMENDATIONS ON THE FUNCTIONING OF THE RADIOELECTRONIC INTELLIGENCE SYSTEM IN THE INTERESTS OF PREPARATION AND STABILIZATION OF STABILIZATION

The military-political situation around Ukraine is characterized by high dynamics and instability of events and processes. Against the background of the above-mentioned task of the Armed Forces of Ukraine at the present stage of development is the intensification of intelligence in order to timely warn the top military-political leadership of Ukraine about possible open armed aggression of the Russian Federation, hidden actions of some other neighboring states

that may threaten national interests. In the article on the basis of investigated influence of external and internal factors on the efficiency of the operation of the radio-electronic intelligence system in the interests of conducting a stabilization operation by grouping troops (forces) in the territory of Donetsk and Lugansk regions, using methods of analysis, synthesis and theory of probability, the evaluation of the efficiency of the electronic system's functioning, the capabilities of its forces and means to expose changes in the modes of operation of the armed forces, bringing to the highest levels of combat readiness K (forces), active prevention actions of illegal armed groups. The impact of the investigated factors on the performance evaluation indicated that the objective capabilities of the electronic intelligence system were not fully realized and, in some cases, significantly reduced. The paper evaluated the effectiveness of radio-electronic intelligence in the Joint Forces operation in the interest of preparation and conduct of the stabilization operation, which allowed to determine the direction of further research and to develop practical recommendations that made it possible to improve the efficiency of the electronic intelligence system with minimal cost.

Keywords: *electronic intelligence system, stabilization operation, efficiency, radio and radio intelligence, probability, intelligence objects, intelligence sources.*

УДК 621.396.6 DOI: 10.46972/2076-1546.2019.17.07

Ю. Б. Бродський, С. О. Ковтун, С. В. Ковальчук, П. П. Топольницький

МЕТОДИЧНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК КОДОФАЗОМАНІПУЛЬОВАНОГО СИГНАЛУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Розглянуто методичний підхід до визначення статистичних характеристик фазоманіпульованого сигналу, що спостерігається на фоні білого шуму. Для перевірки гіпотези про вид закону розподілу ймовірності випадкової величини знайшли широке застосування параметричні й непараметричні критерії узгодженості. До параметричних належать критерій χ^2 Пірсона та його модифікація – χ^2 Нікуліна. Непараметричні критерії: Колмогорова – Смирнова, ω^2 Мізеса, Андерсона – Дарлінга, Реньї та інші. В іноземній науковій літературі для критерія Андерсона – Дарлінга використовують термін «критерій Ω^2 Мізеса».

Для перевірки простих гіпотез перевага надається такому порядку критеріїв (за їх потужністю): χ^2 Пірсона; Андерсона – Дарлінга; Колмогорова – Смирнова; ω^2 Мізеса. У ході перевірки складних гіпотез порядок змінюється: ω^2 Мізеса; Колмогорова – Смирнова; Андерсона – Дарлінга; χ^2 Нікуліна; χ^2 Пірсона.

У разі відомого об'єму вибірки згідно з обраним правилом розраховується кількість інтервалів гістограми, вона будується відповідно до сукупності реалізацій прийнятого сигналу. Після цього її порівнюють з еталонним законом розподілу. Етапи порівняння загальновідомі, тому окремого пояснення не потребують.

Проведено математичне моделювання й обробку його результатів за допомогою програмного пакета Mathcad 14. Перевірено гіпотезу про нормальний закон розподілу вхідної суміші сигналу та шуму за критерієм узгодженості χ^2 Пірсона.

Результати імітаційного моделювання та обчислювального експерименту за наведеним підходом свідчать, що статистичні характеристики адитивної суміші фазоманіпульованого сигналу та білого шуму в разі енергетично прихованого режиму роботи радіоелектронних засобів підпорядковуються законам, які якісно близькі та в загальному випадку апроксимуються нормальним законом розподілу.

Ключові слова: *адитивна суміш; гістограма; закон розподілу; фазова маніпуляція; рівень значущості; статистичні характеристики; густина ймовірності.*

Постановка проблеми в загальному вигляді. Останнім часом спостерігається тенденція впровадження радіоелектронних систем різного призначення з розширеним спектром (spread spectrum) випромінювань. Для побудови радіоелектронних засобів (РЕЗ) з такими сигналами (складними, широкосмуговими, шумоподібними) досить широко застосовуються радіовипромінювання з кодовою фазовою маніпуляцією (КФМ).

Синтез алгоритмів обробки вхідних радіосигналів під час ведення радіоелектронного моніторингу (РЕМ) можна здійснювати на основі методів статистичної радіотехніки. При цьому однією з необхідних умов для синтезу радіоприймальних пристроїв РЕМ є знання статистичних характеристик адитивної суміші вхідних сигналів, найбільш повна

характеристика яких міститься в законі розподілу ймовірності випадкової величини. Для його визначення необхідно мати адекватну модель суміші вхідних сигналів.

Обробці результатів моделювання щодо визначення закону розподілу параметрів вхідних сигналів присвячено досить багато наукових праць, але на цей час вони не в повній мірі систематизовані й залишають певну невизначеність щодо побудови експериментальної функції щільності розподілу та вибору критерію узгодженості. Встановлення кількості інтервалів (груп) для побудови гістограми вхідної вибірки покладено на розсуд дослідника, тому обґрунтування методичного підходу до визначення закону розподілу за результатами моделювання є досить актуальним.

Аналіз останніх досліджень і публікацій. Відомо [1, 2], що для перевірки гіпотези про вид закону розподілу ймовірності випадкової величини знайшли широке застосування параметричні й непараметричні критерії узгодженості. До параметричних належать критерій χ^2 Пірсона і його модифікація – χ^2 Нікуліна. Непараметричні критерії: Колмогорова – Смирнова, ω^2 Мізеса, Андерсона – Дарлінга, Реньї та інші. В іноземній науковій літературі критерій Андерсона – Дарлінга називають критерієм Ω^2 Мізеса. Для перевірки простих гіпотез перевага надається такому порядку критеріїв (за їх потужністю): χ^2 Пірсона; Андерсона – Дарлінга; Колмогорова – Смирнова; ω^2 Мізеса. У разі перевірки складних гіпотез порядок змінюється: ω^2 Мізеса; Колмогорова – Смирнова; Андерсона – Дарлінга; χ^2 Нікуліна; χ^2 Пірсона.

Припустимо, що на вході радіоприймального пристрою присутня двокомпонентна адитивна суміш сигналу і шуму [3]:

$$y(t) = s(t) + \xi(t), \tag{1}$$

де $s(t)$, $\xi(t)$ – сигнальна і шумова складова відповідно.

Як сигнальна складова розглядається КФМ коливання з рівномірно розподіленою початковою фазою, а як шумова – гаусівський стаціонарний білий шум з нульовим математичним сподіванням. У цьому разі потужність (дисперсія) сукупності сигналу σ_S^2 і шуму σ_ξ^2 дорівнює їх сумі [4]:

$$\sigma_y^2 = \sigma_S^2 + \sigma_\xi^2. \tag{2}$$

За фіксованого моменту часу сумісна густина ймовірності для незалежних процесів $s(t)$ і $\xi(t)$ дорівнює добутку їх одномірних густин ймовірності [4]:

$$p_{S+\xi}(y) = p_S(y)\, p_\xi(y) = \frac{1}{\pi\sqrt{2\pi\sigma_\xi^2\left(S^2 - x^2\right)}} exp\left(-y^2 / 2\sigma_\xi^2\right) \text{ для } |x| < S, \tag{3}$$

де S – амплітуда КФМ гармонічного коливання.

У разі $\sigma_S^2 << \sigma_\xi^2$ згідно з (2) у вхідній суміші буде домінувати шумова складова, тому на основі співвідношення (3) закон розподілу адитивної суміші (1) буде одномодальним [4].

Виділення не вирішених раніше частин загальної проблеми, яким присвячено статтю. Відомо [4], що густина ймовірності сигнальної складової виразу (1) має

U-подібну форму і підпорядковується закону розподілу арксинуса, а його шумова складова, тобто білий шум, – нормальному закону розподілу випадкової величини [4]. Тоді, виходячи з наведеного вище, можна висунути гіпотезу про нормальний закон розподілу вхідної суміші. Для перевірки цієї простої гіпотези слід обрати критерій узгодженості χ^2 Пірсона.

Попередньо з'ясувавши характер розподілу за механізмом його утворення, оцінювання закону розподілу випадкової величини за емпіричними даними проводиться в такій послідовності [1, 2]: побудова функції щільності розподілу за результатами експериментальних даних (вибірки) об'ємом N; підбір теоретичного розподілу (згладжування дослідного розподілу теоретичним); перевірка узгодженості дослідного розподілу за підібраним.

На основі викладеного вище необхідно провести перевірку гіпотези про нормальний закон розподілу вхідної суміші за критерієм узгодженості χ^2 Пірсона.

Формулювання завдання дослідження. З урахуванням наведеного **метою статті** є виклад основних положень методичного підходу до визначення статистичних характеристик адитивної суміші нормального шуму і набагато слабшого КФМ сигналу.

Виклад основного матеріалу. Для визначення статистичних характеристик адитивної суміші (1) було проведено імітаційне моделювання методом Монте-Карло за допомогою програмного пакета Mathcad 14. Сигнальна складова представлена фрагментом *M*-послідовності КФМ сигналу з початковим десятирозрядним кодом [0,0,0,0,0,0,1,0,0,1] (рис. 1), що містить 128 елементарних радіоімпульсів (дискрет) і відношенням сигнал/шум $\sigma_S^2/\sigma_\xi^2 = 0{,}1;\ 0{,}05$. Елементарний радіоімпульс із несучою частотою 1 ГГц і тривалістю елементарного імпульсу 4 нс (4 періоди в дискреті). Кількість відліків у періоді гармонічного коливання сигналу становить 2^5.

Елементарний радіоімпульс (дискрету) опишемо виразом [5]:

$$s(t) = S\,exp\left(j\left\{2\pi f_0 t + \varphi\right\}\right) \text{ для } 0 < t < \tau_d\,, \qquad (4)$$

де f_0 , $\varphi = 0,\pi$ – середня лінійна частота заповнення і код фази елементарного радіоімпульсу відповідно.

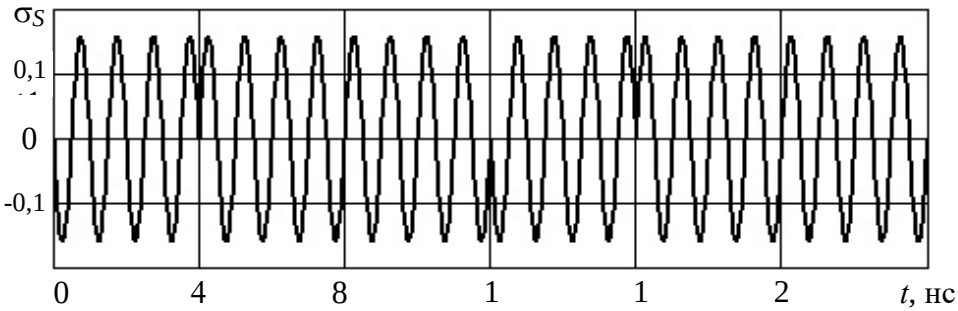


Рис. 1 Фрагмент M-послідовності КФМ сигналу

За шумову складову було використано випадкову послідовність із нормальною щільністю розподілу (білий шум) із нульовим математичним сподіванням ($m_\xi = 0$) і одиничною дисперсією ($\sigma^2_\xi = 1$). Кількість відліків у дискреті КФМ сигналу становить 2^7.

Було проведено чотири серії обчислювального експерименту по 100 вибірок у кожній. Обсяг кожної вибірки містить $N = 2^{14}$ значень, тобто можна вважати їх представницькими.

За отриманими результатами моделювання необхідно побудувати гістограму функції щільності розподілу, використовуючи експериментальні дані (вибірки) об'ємом N. Для цього необхідно визначити кількість інтервалів (груп) k, на які буде розбита вибіркова сукупність. Ця кількість груп пов'язана з об'ємом вибірки (для критерію χ^2 Пірсона $N > 50…150$).

Для вибору інтервалів рівної довжини h визначальною є вимога, щоб кількість реалізацій, які потрапили в інтервали, була не менше 10, а в крайніх інтервалах – не менше 5. У разі одномодального закону розподілу кількість реалізацій в інтервалі може зменшуватися до 1 або нуля.

Довжина інтервалу дорівнює [1]

$$h = \frac{(y_{\max} - y_{\min})}{k}, \tag{5}$$

де $y_{\max}$, $y_{\min}$ – максимальне й мінімальне значення елемента вибірки відповідно.

На сьогодні відомо [6–11] чимало підходів до визначення кількості інтервалів (груп). У багатьох джерелах можна знайти посилання на досить розповсюджену формулу Стерджеса [6]:

$$k = [1 + \log_2 N] \approx [1 + 3{,}322 \lg N], \tag{6}$$

де N – об'єм вибірки;

$[\bullet]$ – результат округлюють до найближчого цілого числа.

Досить розповсюджена і проста формула, поширена для визначення кількості інтервалів, має такий вигляд [2]:

$$k = \left[\sqrt{N}\right]. \tag{7}$$

Для визначення оптимальної кількості інтервалів у [7] запропоновано формулу Брукса – Карузера:

$$k = [5 \lg N]. \tag{8}$$

Відома формула [8], за якою визначають співвідношення кількості інтервалів до об'єму вибірки:

$$k = \left[1{,}87 \sqrt[5]{N^2}\right]. \tag{9}$$

Також має місце співвідношення для рівноймовірних інтервалів [2]:

$$k \approx \left[4 \sqrt[5]{2\left(\frac{N}{z}\right)^2}\right], \tag{10}$$

де z – квантиль стандартного нормального розподілу для заданого рівня значущості.

У [2] наведено модифікацію виразу (10) і рекомендовано застосовувати співвідношення

$$k = [4 \lg N]. \tag{11}$$

На основі виразу (11) у [2] запропоновано формулу

$$k = [5\lg N - 5]. \tag{12}$$

У дослідженні [9] використано таке співвідношення:

$$k \approx \left[\frac{4}{\mathrm{E}}\lg\frac{N}{10}\right], \tag{13}$$

де $\mathrm{E} = 1/(\mu_4/\sigma^4)^{1/2}$ – значення контрексцесу;

μ_4 – момент четвертого порядку;

σ^2 – дисперсія процесу.

Для однакових інтервалів їх кількість за правилом Скотта [10] становитиме величину

$$k = \left[\sqrt[3]{\frac{2N}{3}}\right]. \tag{14}$$

Кількість інтервалів за правилом Фрідмана – Діаконіса [11] дорівнює

$$k = \left[\frac{\sqrt[3]{N}}{2\Delta}\right], \tag{15}$$

де Δ – різниця між верхнім і нижнім квартилями.

Оптимальну кількість інтервалів k за інформаційним критерієм Акаіке знаходимо з такого рівняння [12]:

$$\left[\ln(2k-1) + \frac{2k}{2k-1}\right]\frac{N}{6k^3} = 1. \tag{16}$$

Однак для визначення оптимальної кількості інтервалів критерій Акаіке застосовують рідко [12].

Також відомі [13] рекомендації щодо вибору кількості інтервалів залежно від об'єму вибірки (табл. 1).

Таблиця 1

Рекомендована кількість інтервалів залежно від об'єму вибірки

Об'єм вибірки (N)	40–100	100–500	500–1 000	1 000–10 000
Кількість інтервалів (k)	7–9	8–12	10–16	12–22

Для великих об'ємів (N) вибіркових сукупностей співвідношення Скотта, Фрідмана – Діаконіса й Акаіке є асимптотичними, тобто їх слід застосовувати в разі великих об'ємів вибіркових сукупностей, на відміну від інших формул кількість інтервалів буде пропорційною $n^{1/3}$, а не $\lg N$.

Отже, для визначення кількості інтервалів вибіркової сукупності з метою побудови гістограми для визначення закону розподілу вхідної суміші за критерієм χ^2 Пірсона перевагу слід надати правилу Скотта, яке є досить обґрунтованим і простим у застосуванні та рекомендує більшу кількість інтервалів (табл. 2) порівняно з формулою Стерджеса.

Таблиця 2

Кількість інтервалів гістограми для функції густини ймовірності

Об'єм вибірки (N)	Оптимальна кількість інтервалів (k)		
	Формула Стерджеса	Правило Скотта	Критерій Акаіке
500	10	7	7
1 000	11	9	9
5 000	14	15	15
10 000	15	19	19
50 000	17	33	32
100 000	18	41	41
200 000	19	52	51
500 000	20	70	70
1 000 000	21	88	87

У разі відомого об'єму вибірки ($N = 2^{14}$) за правилом (14) розраховуємо кількість інтервалів гістограми ($k = 23$). Враховуючи співвідношення (5), будуємо гістограму (рис. 2) сукупності реалізацій співвідношення (1) і порівнюємо з еталонним нормальним законом розподілу на основі визначених параметрів (математичного сподівання та дисперсії) за методом моментів з вибіркової сукупності. Міру розходження цих обох розподілів визначаємо за такою формулою [1, 4, 14]:

$$\chi^2 = \sum_{j=1}^{k} \left\{ \left(n_j - N \hat{p}_j \right)^2 \Big/ N \hat{p}_j \right\}, \qquad (17)$$

де n_j – кількість елементів вибірки в j-му інтервалі;

$\hat{p}_j$ – оцінка ймовірності потрапляння випадкової величини вибірки в j-й інтервал.

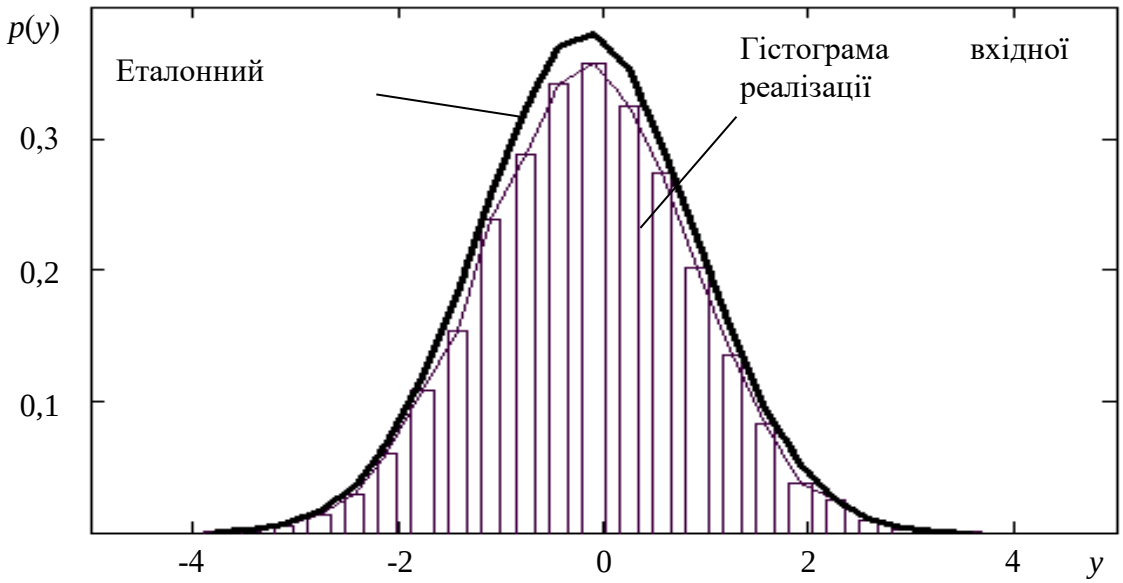


Рис. 2. Приклад гістограми вхідної реалізації випадкового процесу та її згладжувальна лінія й еталонний (теоретичний) нормальний закон розподілу

Величина, яка визначає відносну частоту (імовірність) потрапляння випадкової величини y у j-й інтервал, дорівнює [1, 4, 14]

$$\hat{p}_j = \frac{n_j}{N}. \qquad (18)$$

Сума (16) має наближений χ^2-розподіл з $\nu = k\text{-}l\text{-}1$ ступенями свободи, де l – кількість параметрів еталонного (теоретичного) розподілу, які визначають за вибіркою. Гіпотеза про закон розподілу приймається, якщо $\chi^2_{спост} < \chi^2_{1-\alpha}$ у разі обраного рівня значущості α, де $\chi^2_{1-\alpha}$ – квантиль χ^2 розподілу (розподілу Пірсона) для рівня ймовірності $1-\alpha$ для кількості ступенів свободи ν. Тобто можна зробити висновок, що прийняте припущення (гіпотеза) не суперечить отриманим дослідним даним.

На основі наведеного вище розглянемо результати статистичної обробки результатів математичного моделювання за допомогою програмного пакета Mathcad 14. Перевіримо гіпотезу про нормальний закон розподілу вхідної суміші КФМ сигналу і шуму за критерієм узгодженості χ^2 Пірсона.

Нормальний закон розподілу характеризується двома параметрами, тому кількість ступенів свободи дорівнює величині $\nu = 23\text{-}2\text{-}1 = 20$. На основі обраного рівня значущості α визначаємо величину квантиля $\chi^2_{1-\alpha}$ розподілу Пірсона. Це значення можна отримати за допомогою функції *qchisq*(α,ν) у Mathcad 14 (табл. 3) або з таблиць, наведених у довідковій літературі, наприклад, у [14].

Таблиця 3

Значення квантилів χ^2 розподілу від рівня значущості для $\nu = 20$

Джерело відомостей	Значення квантила ($\chi^2_{1-\alpha}$)				
	$\alpha = 0,3$	$\alpha = 0,2$	$\alpha = 0,1$	$\alpha = 0,05$	$\alpha = 0,01$
Mathcad 14	22,775	25,037	28,412	31,410	37,566
Довідник [14]	22,8	25,0	28,4	31,4	37,6

За формулою (17) розраховуємо величину $\chi^2_{спост}$ вибіркової сукупності та порівнюємо її з величинами, наведеними в табл. 2.

Отримані результати проведених розрахунків показують, що закон розподілу вхідного процесу (1) КФМ сигналу за $\sigma_S^2 << \sigma_\xi^2$ є одномодальним для обох значень розглянутих відношень сигнал/шум: $\sigma_S^2/\sigma_\xi^2 = 0,1; 0,05$.

Для КФМ сигналу, коли $\sigma_S^2/\sigma_\xi^2 = 0,1$, максимальні значення математичного сподівання знаходиться в межах [-0,021…0,016], а коли $\sigma_S^2/\sigma_\xi^2 = 0,05$, то [-0,013…0,023]. Дисперсія лежить у межах [1,083…1,129] і [1,043…1,073] відповідно, що не суперечить співвідношенню (2).

Для відношення сигнал/шум $\sigma_S^2/\sigma_\xi^2 = 0,1$ з рівнем значущості $\alpha = 0,05$ 91% реалізацій апроксимується нормальним законом розподілу. Закону розподілу Стьюдента підпорядковується 7% реалізацій, а 2% виходять за межі обраного рівня значущості для обох розподілів.

Для відношення сигнал/шум $\sigma_S^2/\sigma_\xi^2 = 0,05$ з рівнем значущості $\alpha = 0,05$ 95% реалізацій апроксимується нормальним законом розподілу. Закону розподілу Стьюдента підпорядковується 4% реалізацій, а 1% виходить за межі обраного рівня значущості для обох розподілів.

Відомо [4], що за формою графік функції щільності розподілу ймовірності Стьюдента нагадує розподіл стандартного нормального закону, але товсті “хвости” розподілу Стьюдента повільніше наближаються до нуля, ніж “хвости” нормального розподілу. Для $N \to \infty$ послідовність функції щільності розподілу ймовірності Стьюдента наближається до функції $f(y) = (2\pi)^{-1/2} exp(-y^2/2)$, яка є щільністю розподілу ймовірності нормального закону з нульовим математичним сподіванням і дисперсією, рівною одиниці, тому появу цього розподілу можна пояснити обмеженістю вхідної вибірки.

Отже, за отриманими результатами статистичної обробки можна зробити висновок, що адитивна суміш КФМ сигналу і білого шуму в разі енергетично прихованого режиму роботи РЕЗ ($\sigma_S^2/\sigma_\xi^2 = 0{,}1;\ 0{,}05$) апроксимується нормальним (гаусівським) законом розподілу випадкової величини, тобто на вході радіоприймльних пристроїв слід очікувати адитивну суміш, яка апроксимується нормальним законом розподілу.

Висновки. Отже, методичний підхід до визначення статистичних характеристик радіовипромінювань з лінійною частотною модуляцією сигналів, що спостерігаються на фоні завад і в умовах повної або часткової невизначеності параметрів, складається з таких етапів: перевірка гіпотези про обраний закон розподілу вхідної суміші сигналів за критерієм узгодженості χ^2 Пірсона, що проводиться на основі побудованої гістограми щільності розподілу на основі вхідних даних; підбір теоретичного закону розподілу випадкової величини шляхом порівняння отриманого результату; перевірка узгодженості закону розподілу вхідної вибірки з підібраним (еталонним) розподілом.

Результати імітаційного моделювання та обчислювального експерименту за наведеним підходом свідчать, що статистичні характеристики адитивної суміші КФМ сигналу та білого шуму для енергетично прихованого режиму роботи радіоелектронних засобів підпорядковуються законам, які якісно близькі та в загальному випадку апроксимуються нормальним законом розподілу.

Отримані результати не суперечать і добре узгоджуються з основними положеннями, викладеними в роботах вітчизняних та іноземних вчених [1, 4, 10, 14], що свідчить про коректність проведених досліджень та їх достовірність.

Напрямами подальших досліджень слід вважати синтез, визначення й аналіз характеристик приймача енергетично прихованого сигналу.

СПИСОК ЛІТЕРАТУРИ

1. Демидов Б. А. Методы военно-научных исследований. Ч. 3. Кн. 1. Харьков : ВИРТА ПВО, 1988. 419 с.

2. О выборе числа интервалов в критериях согласия типа χ^2. URL: http://www.ami.nstu.ru/~headrd/seminar/publik_html/Z_lab_8.htm/ (дата обращения: 15.11.2019).

3. Ковтун С .О. Визначення енергетичного показника на виході автокореляційного виявляча під час розвідки сигналів на фоні білого гаусівського стаціонарного шуму // Зб. наук. праць НДІ ГУР МО України. 2012. № 34. С. 102–116.

4. Тихонов В. И. Статистическая радиотехника. Москва : Радио и связь, 1982. 624 с.

5. Варакин Л. Е. Системы связи с шумоподобными сигналами. Москва : Радио и связь, 1985. 384 с.

6. Ковалевський Г. В. Статистика : Підручник. Харків : Харківська нац. академія міського господарства, 2012. 445 с.
7. Шторм Р. Теория вероятностей. Математическая статистика. Статистический контроль качества / Пер. с нем. Н. Н. и М. Г. Федоровых; под ред. Н. С. Райбмана. Москва : Мир, 1970. 368 с.
8. Крамер Г., Лидбеттер М. Стационарные случайные процессы. Свойства выборочных функций и их приложения / Пер. с англ. Ю. К. Беляева и М. П. Ершова; под ред. Ю. К. Беляева. Москва : Мир, 1969. 398 с.
9. Алексеева И. У. Теоретическое и экспериментальное исследование законов распределения погрешностей, их классификация и методы оценки их параметров : автореф. дис. на соиск. учен. степени кан. техн. наук. Ленинград, 1975. 20 с.
10. Scott D. W. On optimal and data-based histograms // Biometrika. 1979. Vol. 66 (3). P. 605–610.
11. Определение числа групп при построении гистограммы. URL: http://www.planetcalc.ru/484/ (дата обращения: 15.11.2019).
12. Taylor C. Akaike's information criterion and the histogram // Biometrika. 1987. Vol. 74. P. 636–639.
13. Бурдун Г. Д., Марков Б. Н. Основы метрологии. Москва : Изд-во стандартов, 1985. 120 с.
14. Бронштейн И. Н., Семендяев К. А. Справочник по математике. Москва : Наука, 1981. 720 с.

Подано 27.12.2019

Ю. Б. Бродский, С. А. Ковтун, С. В. Ковальчук, П. П. Топольницкий

МЕТОДИЧЕСКИЙ ПОДХОД К ОПРЕДЕЛЕНИЮ СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК КОДОФАЗОМАНИПУЛИРОВАННОГО СИГНАЛА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Рассмотрен методический подход к определению статистических характеристик фазоманипулированного сигнала, который наблюдается на фоне белого шума. Для проверки гипотезы о виде закона распределения вероятности случайной величины нашли широкое применение параметрические и непараметрические критерии согласованности. К параметрическим относятся: критерий χ^2 Пирсона и его модификация – χ^2 Никулина. Непараметрические критерии: Колмогорова – Смирнова, ω^2 Мизеса, Андерсона – Дарлинга, Реньи и другие. В иностранной научной литературе для критерия Андерсона – Дарлинга используется термин «критерий Ω^2 Мизеса».

При проверке простых гипотез предпочтение отдается таком порядку критериев (по их мощности): χ^2 Пирсона; Андерсона – Дарлинга; Колмогорова – Смирнова; ω^2 Мизеса. При проверке сложных гипотез порядок меняется: ω^2 Мизеса; Колмогорова – Смирнова; Андерсона – Дарлинга; χ^2 Никулина; χ^2 Пирсона.

При известном объеме выборки согласно выбранного правила рассчитывается количество интервалов гистограммы, она строится в соответствии с совокупностью реализаций принятого сигнала. После этого происходит сравнение с эталонным законом распределения. Этапы сравнения общеизвестны, поэтому отдельного объяснения не требуют.

Проведены математическое моделирование и обработка его результатов с помощью программного пакета MathCAD 14. Проверена гипотеза о нормальном законе распределения входящей смеси сигнала и шума по критерию согласованности χ^2 Пирсона.

Результаты имитационного моделирования и вычислительного эксперимента по предложенному подходу свидетельствуют, что статистические характеристики аддитивной смеси фазоманипулированного сигнала и белого шума при энергетически скрытом режиме работы радиоэлектронных средств подчиняются законам, которые качественно близки и в общем случае аппроксимируются нормальным законом распределения.

Ключевые слова: *аддитивная смесь; гистограмма; закон распределения; фазовая манипуляция; уровень значимости; статистические характеристики; плотность вероятности.*

Y. B. Brodsky, S. A. Kovtun, S. V. Kovalchuk, P. P. Topolnytsky

METHODICAL APPROACH TO DETERMINING THE STATISTICAL CHARACTERISTICS OF CODE PHASE MANIPULATED SIGNAL IN INFORMATION SYSTEMS

A methodological approach to determining the statistical characteristics of the phase-shifted signal observed against a white noise background is considered. Parametric and non-parametric consistency criteria have been widely used to test the hypothesis of the form of the law of probability distribution of random variables. The parametric criteria include Pearson's χ^2 *and its modification of Nikulin's* χ^2*. Nonparametric criteria – Kolmogorov – Smirnov,* ω^2 *Mises, Anderson – Darling, Rainy and others. In the foreign scientific literature, the term* Ω^2 *Mises is used for the Anderson – Darling criterion.*

When testing simple hypotheses, the following order of criteria (by their power) is given preference: χ^2 *Pearson; Anderson – Darling; Kolmogorov – Smirnov;* ω^2 *Mises. When testing complex hypotheses, the order changes:* ω^2 *Mises; Kolmogorov – Smirnov; Anderson – Darling;* χ^2 *Nikulin;* χ^2 *Pearson.*

With the known sample volume, according to the selected rule, the number of intervals of the histogram is calculated and it is constructed according to the set of realizations of the received signal. After that, a comparison is made with the reference law of distribution. The steps of comparison are well known and do not need a separate explanation.

Mathematical modeling and processing of its results with the help of Mathcad software package 14 is carried out. We will test the hypothesis about the normal law of distribution of the input mixture of signal and noise by the criterion χ^2 *Pearson.*

The results of simulation modeling and computational experiment with the above approach show that the statistical characteristics of the additive mixture of phase-manipulated signal and white noise in the energy-hidden mode of operation of electronic means are subject to laws that are qualitatively close and generally approximated by normal laws.

Keywords: *additive mixture; histogram; distribution law; phase manipulation; significance level; statistical characteristics; probability density.*

УДК 378:004.9:355.085.5 DOI: 10.46972/2076-1546.2019.17.08

С. М. Марченков

ФОРМУВАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ ОФІЦЕРІВ ЗБРОЙНИХ СИЛ УКРАЇНИ: НАУКОВО-ПЕДАГОГІЧНИЙ АСПЕКТ

У статті обґрунтовано необхідність формування інформаційно-аналітичної компетенції як однієї з важливих складових фахової компетентності майбутніх офіцерів Збройних Сил України під час професійної підготовки у вищому військовому навчальному закладі. Реалізація інформаційної функції досягається формуванням інформаційно-аналітичної компетентності військовослужбовця. Виходячи з розуміння сутності професійної компетентності та змісту професійної освіти майбутніх офіцерів, можна стверджувати, що якісною характеристикою оволодіння курсантами професійною діяльністю є їх інформаційно-аналітична компетентність. Майбутній офіцер повинен бути підготовлений до професійної, соціально-педагогічної, культурно-освітньої, організаційно-управлінської, фізкультурно-спортивної та спеціальної діяльності. Інформаційно-аналітична компетентність фахівця передбачає логічну культуру мислення: навички аналізу ідей, використання методів раціонального мислення та аргументації. Отже, майбутній офіцер Збройних Сил України повинен володіти професійною компетентністю в цих видах діяльності. Проведено теоретичний аналіз наукових досліджень щодо формування та розвитку професійної компетентності майбутніх військових фахівців, що дає можливість констатувати таке: збільшується розрив між рівнем професійної підготовки майбутніх офіцерів та вимогами до їхньої професійної компетентності; як свідчить досвід діяльності військових навчальних закладів, в установлені терміни навчання важко сформувати повний перелік професійних компетенцій у зв'язку з тенденцією до постійного розвитку у сфері інформаційних технологій, а також через втрати сьогоденної значущості та концентрації обсягу знань; методологія в системі професійної підготовки майбутніх офіцерів є недосконалою.

Визначено провідні критерії оцінювання підготовки майбутніх військових фахівців до виконання функціональних обов'язків за напрямком професійної підготовки, а також проаналізовано основні вимоги до формування інформаційно-аналітичної компетенції майбутніх офіцерів. Проаналізовано основні методологічні підходи та принципи організації інформаційно-аналітичної діяльності. Окреслено педагогічні умови формування інформаційно-аналітичної компетентності курсантів в освітньому середовищі вищого військового навчального закладу. Визначено структурні компоненти інформаційно-аналітичної компетентності та провідні аспекти її формування й розвитку. У розв'язанні проблем формування інформаційно-аналітичної компетентності майбутніх офіцерів Збройних Сил України актуальними є питання впровадження в освітній процес військових закладів вищої освіти технології формування зазначеної компетентності. Впровадження практичних способів викладання в освітній процес підготовки військових фахівців сприятиме тому, що після закінчення вищого

навчального закладу випускники на достатньому рівні будуть здатні до формування власних висновків, ідей та обґрунтованого вибору на основі опрацьованої інформації, володітимуть прийомами і методами інформаційної аналітики, вмітимуть їх практично застосовувати, будуть готові до ведення інформаційно-аналітичної діяльності в структурних підрозділах Збройних Сил України.

Ключові слова: *професійна підготовка; компетентність; інформаційно-аналітична компетентність; інформаційно-аналітична діяльність; педагогічні умови.*

Постановка проблеми в загальному вигляді. Сьогодні впровадження інформаційних технологій є необхідним та актуальним завданням у всіх галузях суспільства, зокрема й у військовій сфері. Розвиток інформаційних технологій зумовлює наповнення інформаційного простору неструктурованою інформацією, яка найчастіше знаходить своє відображення у вигляді інформаційних повідомлень з різнотипних джерел. Тому сучасне суспільство ставить перед випускником вищого військового навчального закладу дещо інші вимоги, ніж раніше. До уваги беруться не лише його знання, вміння та навички, а й особистісні якості, здатність та готовність до професійного зростання, самовдосконалення, професійної мобільності тощо. Система вищої освіти сьогодні має бути спрямована на формування компетентнісної моделі майбутнього фахівця. Сучасний освітній стандарт повинен окреслити результати навчання у вищому військовому навчальному закладі в першу чергу з погляду компетентнісної освіти.

Інформаційно-аналітична компетентність необхідна для вирішення кваліфікаційних фахових завдань як один із ключових складників професійної компетентності. Вона є головним компонентом здатності теоретизувати, знаходити причинно-наслідкові зв'язки між явищами, становить основу загальних здібностей і необхідна для успішного освоєння людиною різних видів діяльності. Тому актуальним завданням є удосконалення методів формування інформаційно-аналітичної компетентності майбутніх офіцерів у ході професійної підготовки.

Аналіз останніх досліджень і публікацій. Проблема формування професійної компетентності тривалий час досліджується вітчизняними і закордонними науковцями (Л. Васильченко, В. Введенський, В. Гриньова, О. Дубасенюк, Л. Карпова, В. Лозова, Дж. Равен тощо). Проте як у визначенні понять «компетентність» і «компетенція» (які іноді ототожнюють, а іноді диференціюють), так і в класифікації компетентностей сьогодні ще немає однозначності [9].

Крім того, проблеми фахової підготовки у військовій сфері досліджені недостатньо. Окремі аспекти формування компетентності курсантів у сфері їх професійної діяльності порушені в працях О. Барабанщикова, В. Балашової, І. Грязнова, О. Діденка, А. Лігоцького, О. Пономаренка, А. Радванського, Ю. Сердюка, В. Ягупова та багатьох інших дослідників. Учені зазначають, що показником ефективності фахової підготовки є компетентність у багатьох аспектах діяльності. Але комплексного дослідження з питань формування інформаційно-аналітичної компетентності в майбутніх офіцерів на основі системного, міжпредметного, технологічного і компетентнісного підходів на сьогодні немає: не обґрунтовано педагогічних умов формування інформаційно-аналітичної компетентності в курсантів, не розроблено методики її формування.

Формулювання завдання дослідження. Метою досліджень є проведення аналізу та обґрунтування науково-теоретичних основ змісту інформаційно-аналітичної компетентності та особливостей її формування в майбутніх офіцерів у процесі професійної підготовки.

Виклад основного матеріалу. У сучасних умовах назріла нагальна необхідність у суттєвому вдосконаленні наявних підходів до формування професійної компетентності офіцерського складу. Відповідно до чинного стандарту майбутній офіцер повинен бути підготовлений до професійної, соціально-педагогічної, культурно-освітньої, організаційно-управлінської, фізкультурно-спортивної та спеціальної діяльності. Отже, він повинен володіти професійною компетентністю в цих видах діяльності, а інтегруючими компонентами в ній, на наш погляд, є інформаційна та аналітична компетентність.

Розглянемо сутність понять «компетентність», «інформаційно-аналітична компетентність». Для цього визначимося з термінологією, яка вживається в педагогічній літературі в контексті компетентнісного підходу.

А. Хуторський вважає, що компетентність передбачає опанування людиною відповідної компетенції, яка містить особистісне ставлення до неї і предмета діяльності [10]. Крім того, результати проведеного аналізу щодо застосування понять «компетентність» та «компетенція» надають нам можливість зробити висновок, що українська освіта поняттям «компетентність» оперує в значенні, запропонованому європейськими країнами: здатність успішно задовольняти індивідуальні та соціальні потреби, діяти та виконувати поставлені завдання. Отже, компетентність – це не проста сума знань, умінь і навичок, а психосоціальна риса, яка надає тому, хто навчається, сил та впевненості у власній успішності, можливості ефективно взаємодіяти з навколишнім середовищем [1].

Л. Петренко наголошує, що термін «компетенція» логічно використовувати, характеризуючи коло повноважень, прав, обов'язків робітника. певні знання, уміння, навички з професійно значущими властивостями та якостями, які у своїй інтегративній сукупності і визначають його здатність до діяльності [8].

В. Байденко вважає, що компетенції охоплюють здібність, підготовленість до виконання функціональних обов'язків та ставлення до них (образ поведінки), які необхідні для діяльності [5].

О. Діденко звертає увагу, що в професійній підготовці майбутніх офіцерів доцільно зосередитися не на поінформованості курсантів, а на їх уміннях використовувати інформацію для вирішення проблем, що виникають у всіх видах професійної діяльності та сферах відносин. Автор зазначає, що нагальною потребою в зміні пріоритетів вищої освіти є підсилення її практичної зорієнтованості [4]. Усе це дає змогу констатувати необхідність визначення та дослідження інформаційно-аналітичної компетентності як однієї з ключових, що перебуває у невідривному зв'язку із професійною діяльністю. Вона є однією з основних у фаховій підготовці майбутніх офіцерів та забезпечує навички в роботі з інформацією, що міститься в навчальних предметах і професійній діяльності, а також у навколишньому середовищі.

Як вважає В. Ягупов, інформаційно-аналітична компетентність – це ставлення до інформації та критичне усвідомлення її цінності, інформаційно-аналітичні знання,

навички, вміння, здатності, професійно важливі якості, особистий досвід у сфері пошуку, оцінювання, використання, збереження, аналізу, оформлення та передачі інформації за допомогою різних засобів, методів і форм інформаційно-аналітичної діяльності, що дозволяє оперативно орієнтуватися в інформаційному просторі, брати участь у його формуванні [7].

Саме тому фундаментальність інформаційно-аналітичної компетентності є безсумнівною, оскільки ця компетентність є інтегральною характеристикою особистості майбутнього офіцера, що спрямована: на уміння аналізувати інформацію з метою її використання в освітній та професійній діяльності; на виконання навчальних та професійних завдань методом аналізу в умовах неповної проінформованості; на уміння аналізувати власну освітню та професійну діяльність з метою підвищення її ефективності; на розуміння та усвідомлення відповідних питань освітньої та професійної діяльності через аналітичну діяльність.

Ефективність процесу формування зазначеної компетентності залежить від вибору комплексу педагогічних умов. Розглянемо тлумачення терміну «педагогічні умови». У педагогічній літературі існує декілька його визначень.

На думку Н. Іполітової, Н. Стерхової [6], педагогічні умови є одним із компонентів педагогічної системи, що відображають сукупність можливостей освітнього та матеріально-просторового середовища, впливають на особистісний і процесуальний аспекти даної системи й забезпечують її ефективне функціонування і розвиток.

Зокрема, С. Г. Мельничук визначає педагогічні умови як чинники управління процесом навчання, які активізують студентів і стимулюють свідоме засвоєння навчального матеріалу. Педагогічні умови є сукупністю дій та взаємодій, що забезпечують досягнення максимально можливого корисного результату діяльності [7].

Отже, педагогічні умови – це сукупність різних факторів, які нерозривно пов’язані однин з одним, у процесі їх використання можливе досягнення поставленої мети. Педагогічні умови формування будь-якої компетентності – це комплекс певних складових, за допомогою яких особистість буде набувати компетентності в певній галузі.

Отже, на основі зазначеного вище під педагогічними умовами формування інформаційно-аналітичної компетентності майбутніх офіцерів в освітньому середовищі вищого військового навчального закладу будемо розуміти необхідні й достатні обставини, сукупність можливостей освітнього середовища, за яких відбувається цілісний продуктивний навчально-виховний процес, що забезпечує ефективне формування в курсантів інформаційно-аналітичної компетентності. У ході дослідження виділено педагогічні умови, які підвищують інтерес тих, хто навчається, до своєї майбутньої професії та спонукають їх до виконання інформаційно-аналітичної діяльності. Розглянемо їх детальніше.

1. Формування в майбутніх офіцерів мотивації до інформаційно-аналітичної діяльності як засобу професійного становлення та кар’єрного зростання.

2. Поетапне виконання інформаційно-аналітичної діяльності від алгоритму до практичного застосування в різних ситуаціях, що сприяє формуванню умінь пошуку, аналізу, синтезу, порівняння, структурування, класифікації інформації для виконання поставленого завдання.

3. Створення відкритого освітнього середовища у вищому військовому навчальному закладі, яке дозволяє будувати індивідуальну освітню траєкторію кожного курсанта та враховує специфіку професійної діяльності.

Зазначені педагогічні умови перебувають у нерозривній єдності між собою і становлять єдину систему, що характеризується наявністю компонентів, які знаходяться в тісному зв'язку один з одним і мають характер взаємодії в досягненні бажаного результату, а саме готовності майбутніх офіцерів до ефективної інформаційно-аналітичної діяльності.

Щодо проблеми формування інформаційно-аналітичних вмінь у науковій літературі існують певні підходи: компетентнісний, особистісно зорієнтований, комунікативний, діяльнісний, аксіологічний, інтегративний тощо.

Компетентнісний підхід в освіті більшістю дослідників (Г. Селевко, І. Зимняя, Б. Хасан, А. Хуторський та ін.) розглядається як комплексна орієнтація навчання на досягнення інтегрованого результату в професійній підготовці визначених суспільством ціннісних орієнтацій, досить високого рівня знань, умінь і навичок, обізнаності, досвіду, здібностей, готовності до життя та діяльності в різних професійних сферах.

І. Демешко досліджував особистісно зорієнтований підхід до навчання, який формується на основі гуманістичної психології А. Маслоу. Суть його з позиції того, кого навчають, полягає в: організації суб'єкт-суб'єктивної взаємодії; гарантуванні безпеки особистісного прояву; формуванні активності того, хто навчається, його готовності до вирішення проблемних завдань; забезпеченні єдності зовнішніх і внутрішніх мотивацій; отриманні задоволення від виконання навчальних завдань у співпраці з товаришами; забезпеченні умов для самооцінювання, саморегуляції та самоактуалізації особистості; зміні позиції педагога від передавача та контролера знань до фасалітатора (помічника, чия діяльність спрямована не на передачу знань, а на організацію діяльності учня) [3].

На думку О. Березюк, С. Тарасенко, комунікативний підхід орієнтований на організацію навчання, адекватного процесу реального спілкування завдяки моделюванню основних закономірностей мовленнєвого спілкування. Він передбачає органічне поєднання свідомих і підсвідомих компонентів у ході професійної підготовки, тобто засвоєння правил оперування професійними моделями відбувається одночасно з оволодінням їх комунікативною функцією [1].

Діяльнісний підхід передбачає зорієнтованість освітнього процесу безпосередньо на особистість курсантів та потребує урахування їх індивідуальних особливостей, його сутність полягає в персоналізації педагогічної взаємодії, яка ґрунтується на відмові від рольових масок, адекватному включенні особистісного досвіду (почуттів, емоцій, вчинків) майбутніх офіцерів.

Аксіологічний (ціннісний) підхід дозволяє вивчати явища з погляду виявлення їх можливостей задовольняти потреби людини, виконувати завдання з гуманізації суспільства. Через культурні та духовні цінності особистість задовольняє свої власні потреби. Отже, аксіологічний підхід реалізується у формуванні здатності до навчання, бажанні змінити життя на краще, в інтересах та внутрішній мотивації, умінні робити вибір та встановлювати власні цілі, визначати свої ролі в суспільстві, у соціальних та громадянських навичках та вміннях. Аксіологічний підхід до професійної підготовки передбачає формування системи ціннісних орієнтацій, ієрархію індивідуальних переваг, мотиваційну програму діяльності.

Інтегративний підхід у формуванні ключових компетентностей розглядається науковцями як загальнонаукова методологія, на основі якої формуються цілісні педагогічні системи та їх підсистеми. Він відповідає філософському трактуванню цілого, але не як суми частин, а як нової якості за рахунок змін способів зв'язку елементів цієї структури, що надає можливість створити з різних частин систему як цілісну сукупність елементів, що взаємопов'язані між собою і виступають як органічне єдине ціле. Процеси інтеграції можуть мати місце як у межах системи, що вже склалася, тоді вони зумовлюють підвищення рівня її цілісності та організованості, так і в разі виникнення нової системи з раніше непов'язаних елементів.

Отже, з урахуванням комплексного психолого-педагогічного вивчення, цілісного теоретико-методологічного обґрунтування формування інформаційно-аналітичної компетентності майбутніх офіцерів у процесі фахової підготовки визначено компоненти інформаційно-аналітичної компетентності: мотиваційно-ціннісний (прагнення майбутніх офіцерів до здійснення пошуку й аналітико-синтетичної обробки інформації, до освіти та самоосвіти); діяльнісно-технологічний (володіння алгоритмами, способами, методами, вміння застосовувати різноманітні технології в пошуковій та аналітичній діяльності); когнітивно-аналітичний (обізнаність у сфері інформаційно-комунікативних технологій); оцінно-рефлексійний (усвідомлення майбутніми офіцерами необхідності інформаційно-аналітичної діяльності, уміння аналізувати особистий досвід, оцінювати результати діяльності).

На превеликий жаль, дуже часто ми спостерігаємо, як курсанти під час своєї відповіді не можуть висловити власної думки, не володіють навіть мінімумом логічних навичок для формулювання висновків. Усе це свідчить про низький рівень логічної культури, тому формування інформаційно-аналітичної компетентності в професійній підготовці майбутніх офіцерів Збройних Сил України є актуальним сьогодні.

Спираючись на роботи вітчизняних і закордонних дослідників, можна стверджувати, що основними ознаками інформаційно-аналітичної компетентності є: розуміння природи інформаційних процесів, володіння методами аналізу даних, уміння розпізнавати логічні зв'язки в системі зібраної інформації, здатність до проблематизації, розгляду явищ та процесів з різних поглядів, уміння знаходити необхідну інформацію з різних джерел, зокрема з інформаційних потоків у режимі реального часу, володіння навичками аналізу конкретних виробничих ситуацій, використання інформаційних технологій у пошуку джерел та літератури.

Завдяки формуванню аналітичної компетентності курсант набуває таких особистісних якостей, як: аналітичне мислення, здатність працювати із великими обсягами інформації, уважність, добра пам'ять, розвинена інтуїція, спостережливість, старанність, відповідальність, креативність, увага до дрібниць, широкий кругозір, цілеспрямованість, здатність доводити справу до завершення тощо.

Формування аналітичної компетентності майбутніх офіцерів передбачає: поглиблення мотивації до аналітичної діяльності як засобу професійного становлення та подальшого кар'єрного зростання; спрямування змісту освітньо-професійних програм на вироблення аналітичної компетентності, яка вважається основним інструментом наукового пізнання, що здійснюється за допомогою логічних операцій, відповідно до яких явища та предмети розглядаються за окремими та спільними ознаками; використання практико-зорієнтованих освітніх технологій у процесі включення майбутніх фахівців у професійну аналітичну

діяльність з метою формування аналітичних умінь та навичок курсантів; стимулювання рефлексивної позиції тих, хто навчається, на всіх етапах розвитку аналітичної компетентності.

З метою забезпечення формування аналітичної компетентності викладач має створити умови для самостійної роботи курсанта, використовувати демократичний та егалітарний методи і форми навчання. Важливим підґрунтям такої освітньої системи є: динамічна структура навчальних курсів; інтерактивні, ігрові, проєктні технології; використання матеріально-технічної бази, що доповнюється потужними інформаційними системами; використання різних способів активізації мислення. Ці елементи сприяють формуванню мотивів до навчальної діяльності курсантів: зацікавленість, отримання задоволення від досягнутого результату; навчання з метою самореалізації в житті; відповідальність; зміщення акценту на самоконтроль та самооцінку; кар'єрне зростання; спрямованість навчання на оволодіння сучасними технологіями та професійною компетентністю офіцера.

Висновки. Отже, інформаційно-аналітична компетентність майбутніх офіцерів є важливою складовою фахової компетентності та становить динамічне інтегративне особистісне утворення, що характеризує здатність застосовувати знання, уміння, навички й власні якості в процесі аналітичної роботи з метою одержання якісно нового знання для оперативного та продуктивного забезпечення процесу ухвалення рішень у професійній діяльності. Перспективами подальшого дослідження є визначення проблем самоорганізації та саморозвитку аналітичної компетентності в майбутніх офіцерів Збройних Сил України.

СПИСОК ЛІТЕРАТУРИ

1. Березюк О. С. Системний підхід до формування полікультурної компетентності майбутніх фахівців в сучасному освітньому просторі : монографія. Житомир : Вид-во ЖДУ ім. І. Франка, 2015. С. 193–209.
2. Горовий В. М. Особливості розвитку соціальних інформаційних баз сучасного українського суспільства : монографія. Київ : НБУВ, 2005. С. 274–279.
3. Демешко І. М. Застосування інноваційної методики в курсі «Інформаційно-аналітична діяльність» // Наукові записки. Кіровоград, 2003. Вип. 147. С. 57–62.
4. Діденко О. В. Компетентнісний підхід до професійної підготовки майбутніх офіцерів правоохоронних органів України // Наукові записки Вінницького держ. пед. ун-ту. Серія : Педагогіка і психологія. Вінниця, 2010. Вип. 33. С. 218–222.
5. Захарова І. В., Філіпова Л. Я. Основи інформаційно-аналітичної діяльності : навч. посіб. для ВНЗ // Київ : Центр учб. літ-ри, 2013. 336 с.
6. Ипполитова Н. Анализ понятия «педагогические условия» : сущность, классификация // General and Professional Education. 2012. № 1. С. 8–14.
7. Мельничук С. Г. Формування естетичної культури майбутніх вчителів (історико-педагогічний аспект, 1860–1970 роки). Київ : Наукова думка, 1995. 198 с.
8. Петренко Л. М. Інформаційно-аналітична компетентність керівника професійно-технічного навчального закладу: алгоритми ефективної діяльності : навч.-метод. посіб. Дніпропетровськ : ІМА-прес, 2013. 252 с.
9. Степко М. Ф., Андрущенко В. П. Стратегія реформування освіти в Україні : рекомендації з освітньої політики. Київ : "К.І.С.", 2003. 296 с.

10. Хуторський А. В. Ключевые компетенции как компонент личностно ориентированной парадигмы образования // Нар. образование. 2003. № 2. С. 58–64.
11. Ягупов В. В. Педагогіка : навч. посіб. Київ : Либідь, 2002. 560 с.

Подано 26.12.2019

С. Н. Марченков

ФОРМИРОВАНИЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ КОМПЕТЕНТНОСТИ БУДУЩИХ ОФИЦЕРОВ ВООРУЖЕННЫХ СИЛ УКРАИНЫ: НАУЧНО-ПЕДАГОГИЧЕСКИЙ АСПЕКТ

В статье обоснована необходимость формирования информационно-аналитической компетенции как одной из важных составляющих профессиональной компетентности будущих офицеров Вооруженных Сил Украины во время подготовки в высшем военном учебном заведении. Реализация информационной функции достигается путём формирования информационно-аналитической компетентности военнослужащего. Исходя из понимания сущности профессиональной компетентности и содержания профессионального образования будущих офицеров, можно утверждать, что качественной характеристикой овладения курсантами профессиональной деятельностью является их аналитическая и проектная компетентность. Будущий офицер должен быть подготовлен к профессиональной, социально-педагогической, культурно-образовательной, организационно-управленческой, физкультурно-спортивной и специальной деятельности. Аналитическая компетентность специалиста предусматривает логическую культуру мышления: навыки анализа идей, использование методов рационального мышления и аргументации. Таким образом, будущий офицер Вооруженных Сил Украины должен обладать профессиональной компетентностью в этих видах деятельности. Проведен теоретический анализ научных исследований по формированию и развитию профессиональной компетентности будущих военных специалистов, который позволяет констатировать следующее: увеличивается разрыв между уровнем профессиональной подготовки будущих офицеров и требованиями к их профессиональной компетентности; как показывает опыт деятельности военных учебных заведений, в установленные сроки обучения трудно сформировать полный перечень профессиональных компетенций в связи с тенденцией постоянного развития в сфере информационных технологий, а также потерей сегодняшней значимости и концентрации объема знаний; методология в системе профессиональной подготовки будущих офицеров несовершенна.

Определены ведущие критерии оценки подготовки будущих военных специалистов к выполнению функциональных обязанностей, а также проанализированы основные требования к формированию информационно-аналитической компетенции будущих офицеров, перечислены и определены основные методологические подходы и принципы организации информационно-аналитической деятельности. Указаны педагогические условия формирования информационно-аналитической компетентности курсантов в образовательной среде высшего военного учебного заведения. Определены структурные компоненты информационно-аналитической компетентности и ведущие аспекты относительно ее формирования и развития. В решении проблем формирования информационно-аналитической компетентности будущих офицеров Вооруженных Сил Украины актуальными являются вопросы внедрения в образовательный процесс высших

военных учебных заведений технологии формирования указанной компетентности. Применение практических способов преподавания в процессе подготовки военных специалистов способствует тому, что после окончания высшего учебного заведения выпускники на достаточном уровне способны к формированию собственных выводов, идей и обоснованному выбору на основе обработанной информации, владеют приемами и методами информационной аналитики, умеют их практически применять, готовы к ведению информационно-аналитической деятельности в структурных подразделениях Вооруженных Сил Украины.

Ключевые слова: *профессиональная подготовка; компетентность; информационно-аналитическая компетентность; информационно-аналитическая деятельность; педагогические условия.*

S. M. Marchenkov

THE PROBLEM OF INFORMATION AND ANALYTICAL COMPETENCE IN PROFESSIONAL PREPARATION OF FUTURE OFFICERS OF THE ARMED FORCES OF UKRAINE: SCIENTIFIC AND PEDAGOGICAL ASPECTS

In this article explains needs of preparation the information and analytic competence for the future officers in the Ukraine Armed Forces during their study in the military high educational institutes. Information function realizes by the future officer as information and analytic competence. Professional level of analytic and project activities of the future officers provides their education content. Modern officer should be ready for professional, social and pedagogic, culture and education, management, physical-training and special activities. Analytic competence means logic: methods of rational thinking, arguments, ideas analysis. According theoretical analysis of the preparation and development professional competences: there is large difference between level of professional skills and requirements for the capabilities. The current methodology of education and professional training of the military specialist is not perfect because there is so difficult to create require full list of capabilities during all term of education. The leading criteria for assessing the training of future military specialists to carry out tasks and responsibilities in the direction of professional training are identified. Also was analyzed the basic requirements for the formation of information and analytical competence of future officers, lists and defines the main methodological approaches and principles of organization of information and analytical activities. There was indicated pedagogical conditions for formation information and analytic competences in the military education environment.

The structural components of information and analytical competences and leading aspects regarding its formation and development was determined. In solving the problems of the formation of informational and analytical competence of future officers of the Armed Forces of Ukraine, the urgent issues are the introduction of the technology of forming this competence in the educational process of higher military educational institutions. The introduction of practical teaching methods in the educational process of training specialists in the socio-cultural sphere will contribute to the fact that after graduation, graduates at a sufficient level will be able to form their own conclusions, ideas and informed choices based on certain information, master the techniques and methods of information analytics, be able to practically apply, will be ready to conduct information and analytical activities in the structural units of the Armed Forces Ukraine.

Keywords: *professional training; competence; information-analytical competence; information-analytical activity; pedagogical conditions.*

ISSN 2076-1546

УДК 621.396.62 DOI: 10.46972/2076-1546.2019.17.09

О. А. Нагорнюк, Ю. О. Колос

ВПЛИВ КОНСТРУКТИВНИХ РІШЕНЬ КОМПОНУВАННЯ ТА ПОХИБОК ВИГОТОВЛЕННЯ ЕЛЕМЕНТІВ ШИРОКОСМУГОВОЇ РУПОРНОЇ АНТЕНИ НА ЇЇ ТЕХНІЧНІ ХАРАКТЕРИСТИКИ

У статті подано результати дослідження основних варіантів компонування двогребеневої рупорної антени, які відрізняються способами кріплення елементів: болтове з'єднання (заклепки) та паяння (зварювання). Проаналізовано вплив неточностей виготовлення окремих елементів антени (похибки геометричних розмірів хвилеводу і розкриву рупора, похибки розміщення провідника живлення, відмінності діелектричної проникності ізолювального матеріалу від розрахованої тощо) і в їх з'єднанні між собою (ширина щілин між пластинами розкриву рупора, відстань між гребенями в точці збудження) на основні характеристики антени (коефіцієнт стоячої хвилі за напругою, коефіцієнт підсилення, діаграма спрямованості). Дослідження проводилися з використанням програмних середовищ автоматизованого проєктування, моделювання та оптимізації тривимірних електромагнітних систем ANTENNA MAGUS *та CST STUDIO SUITE. Встановлено, що в разі однакової точності виготовлення елементів широкосмугової рупорної антени розглянуті варіанти компонування забезпечують близькі за значенням технічні характеристики. Дослідження похибок виготовлення елементів антени та їх з'єднання між собою показали, що найбільший вплив на характеристики антени мають поздовжні розміри хвилеводу, відстань між гребенями в точці збудження, місце розміщення та діаметр провідника живлення, а також діелектричні характеристики ізолювального матеріалу. Встановлено, що зміна окремих розмірів антени на 10% може призводити до суттєвого погіршення її узгодженості. Обґрунтовано систему допусків на розміри та з'єднання елементів антени, дотримання яких забезпечить відповідність характеристик виготовленого зразка отриманим у процесі моделювання та оптимізації з використанням спеціалізованих програмних засобів.*

Ключові слова: *двогребенева рупорна антена; широкосмуговість; моделювання; компонування; похибки; хвилевід; характеристика; параметр; допуск.*

Постановка проблеми в загальному вигляді. Сучасними тенденціями розвитку радіотехнічних та телекомунікаційних засобів є розширення діапазону робочих частот та застосування широкосмугових радіосигналів із складними видами модуляції. Для приймання та передавання таких сигналів необхідно використовувати широкосмугові антени з високим коефіцієнтом перекриття за частотою та доброю узгодженістю з лінією живлення. У діапазоні сантиметрових хвиль це можуть бути рупорні антени зі складною формою поперечного перерізу [1]. У літературі запропоновано низку методик розрахунку конструктивних розмірів та параметрів таких видів антен, а також результатів їх оптимізації з використанням спеціалізованого програмного забезпечення CST STUDIO SUITE, ALTAIR FEKO, ANSOFT HFSS тощо [1–10]. Типові конструкції рупорних антен зі складною формою поперечного перерізу застосовуються в діапазоні від 0,6 ГГц до 30 ГГц та забезпечують коефіцієнт стоячої хвилі за напругою (КСХН) менше 2.

Аналіз останніх досліджень і публікацій. У [2–6] запропоновано різні конструкції широкосмугових рупорних антен зі складною формою поперечного перерізу з робочим діапазоном від 0,6 ГГц до 30 ГГц, які відрізняються типом системи живлення, наявністю та матеріалом бокових стінок розкриву. Для покращення характеристик антен доцільно в розкриві рупора застосувати лінзу спеціальної форми [7–8]. У [10] подано результати дослідження двогребеневої рупорної антени, виготовленої з використанням сучасних технологій тривимірного друку та струмопровідної фарби. Однак у наявних у відкритому доступі роботах мало уваги приділяється дослідженню впливу конструктивних рішень компонування та похибок виготовлення елементів широкосмугової рупорної антени на її технічні характеристики.

Формулювання завдання дослідження. Метою статті є дослідження впливу різних схем компонування широкосмугових рупорних антен, похибок у розмірах елементів та неточностей їх з'єднання між собою на технічні характеристики антен.

Нехай розглядається конструкція рупорної антени зі складною формою поперечного перерізу, яка має два гребені та металеві бокові стінки. Така антена є широкосмуговою, має лінійну поляризацію, низький рівень бічних та задньої пелюсток, високий коефіцієнт корисної дії, порівняно малий вплив сторонніх предметів (елементи кріплення, блоки з апаратурою тощо) на її технічні характеристики. На відміну від конструкцій без бокових стінок або з металевими стержнями, антена з металевими боковими стінками має значно кращий коефіцієнт підсилення (КП) в нижній частині робочого діапазону [6].

Конструктивні розміри двогребеневої рупорної антени були розраховані для частотного діапазону 2–15 ГГц відповідно до відомих методик [1–7]. Профілі гребенів отримані на основі кривої Безьє третього порядку [3]. Завданням дослідження було створення програмних моделей антени, побудованих за різними схемами компонування, та визначення впливу схем компонування, похибок виготовлення і з'єднання елементів антени на її технічні характеристики.

Виклад основного матеріалу. Дослідження програмних моделей антени реалізовано з використанням пакета програм CST STUDIO SUITE, який є набором інструментів для проєктування, моделювання та оптимізації тривимірних електромагнітних систем і використовується передовими технологічними й інжиніринговими компаніями провідних держав світу [11].

Проведені дослідження складалися з таких етапів:

розробки базової програмної моделі двогребеневої рупорної антени, задання її конструктивних розмірів та визначення основних характеристик;

створення програмної моделі двогребеневої рупорної антени, виконаної з окремих елементів із використанням технології спаювання (зварювання), та визначення її основних параметрів і характеристик;

створення програмної моделі двогребеневої рупорної антени, виготовленої з окремих елементів із використанням технології болтового (заклепкового) з'єднання, та визначення її основних параметрів і характеристик;

дослідження зміни основних параметрів та характеристик антени з урахуванням похибок у розмірах елементів і неточностей їх з'єднання між собою.

Для створення і параметризації базової програмної моделі двогребеневої рупорної антени сантиметрового діапазону хвиль використано спеціалізоване програмне забезпечення автоматизованого проєктування антен ANTENNA MAGUS, що дозволяє створювати стандартну параметризовану тривимірну (3D) модель антени відповідно до заданих її технічних характеристик [12]. Процес формування базової програмної моделі включає:

задання специфікації антени відповідно до її параметрів, основними з яких є діапазон робочих частот 2–15 ГГц та коефіцієнт підсилення 12 дБ;

вибір конструкції двогребеневої рупорної антени з металевими боковими стінками;

розрахунок розмірів 3D моделі антени;

попереднє оцінювання параметрів та характеристик отриманої моделі;

експорт 3D моделі антени в спеціалізований файл програми CST MICROWAVE STUDIO.

Зовнішній вигляд та конструктивні розміри отриманої базової моделі зображено на рис. 1, а її основні технічні характеристики – на рис. 2.

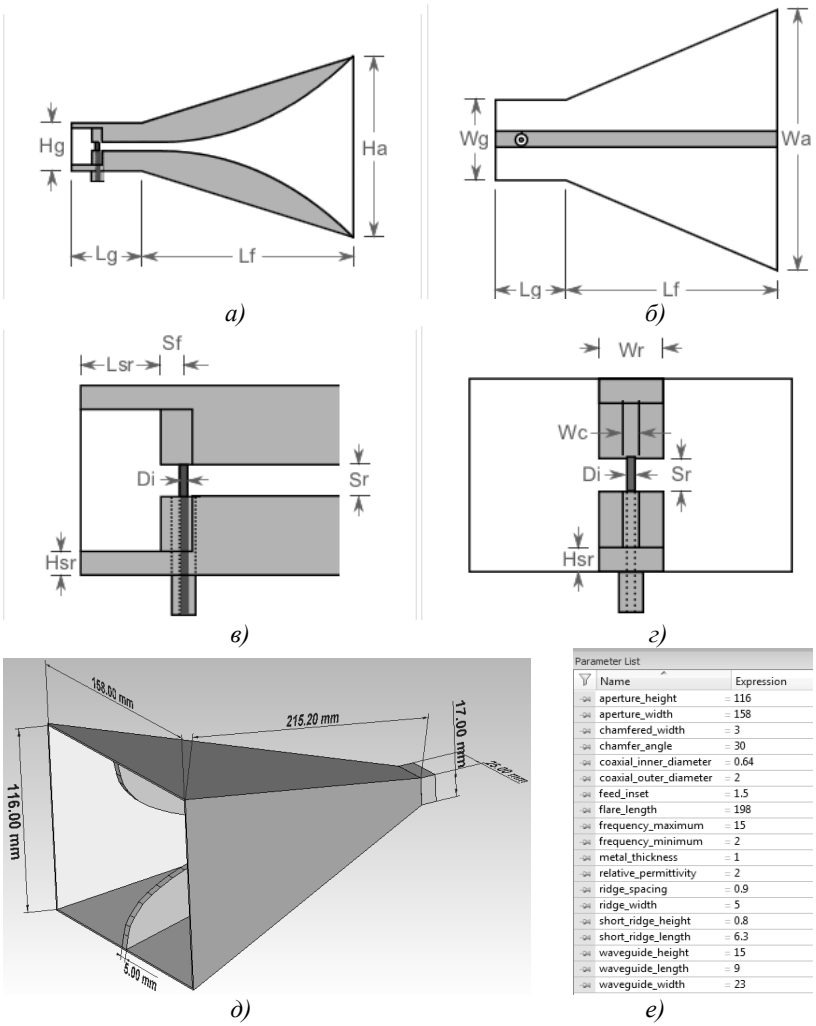


Рис. 1. Конструктивні розміри та програмна модель двогребеневої рупорної антени: а) загальний вигляд збоку; б) загальний вигляд зверху; в) вигляд схеми живлення збоку; г) вигляд схеми живлення ззаду; д) вигляд програмної моделі CST MICROWAVE STUDIO; *е) параметри програмної моделі*

На рис. 1 застосовано такі позначення конструктивних розмірів: H_g – висота хвилеводу; W_g – ширина хвилеводу; L_g – довжина хвилеводу; H_a – висота розкриву; W_a – ширина розкриву; L_a – довжина рупора; S_r – відстань між гребенями; W_r – ширина гребенів; H_{sr} – висота короткої ділянки гребеня; L_{sr} – довжина короткої ділянки гребеня; W_r – ширина фаски гребеня; D_i – діаметр провідника живлення; S_f – відстань від центра провідника живлення до кінця гребеня.

Схема живлення антени зображена на рис. 1в, г. Провідник живлення входить посередині широкої стінки хвилеводу, проходить через один із гребенів та з'єднується з іншим гребенем. Нижній гребінь ізольований від провідника живлення діелектриком, що має діелектричну проникність ε.

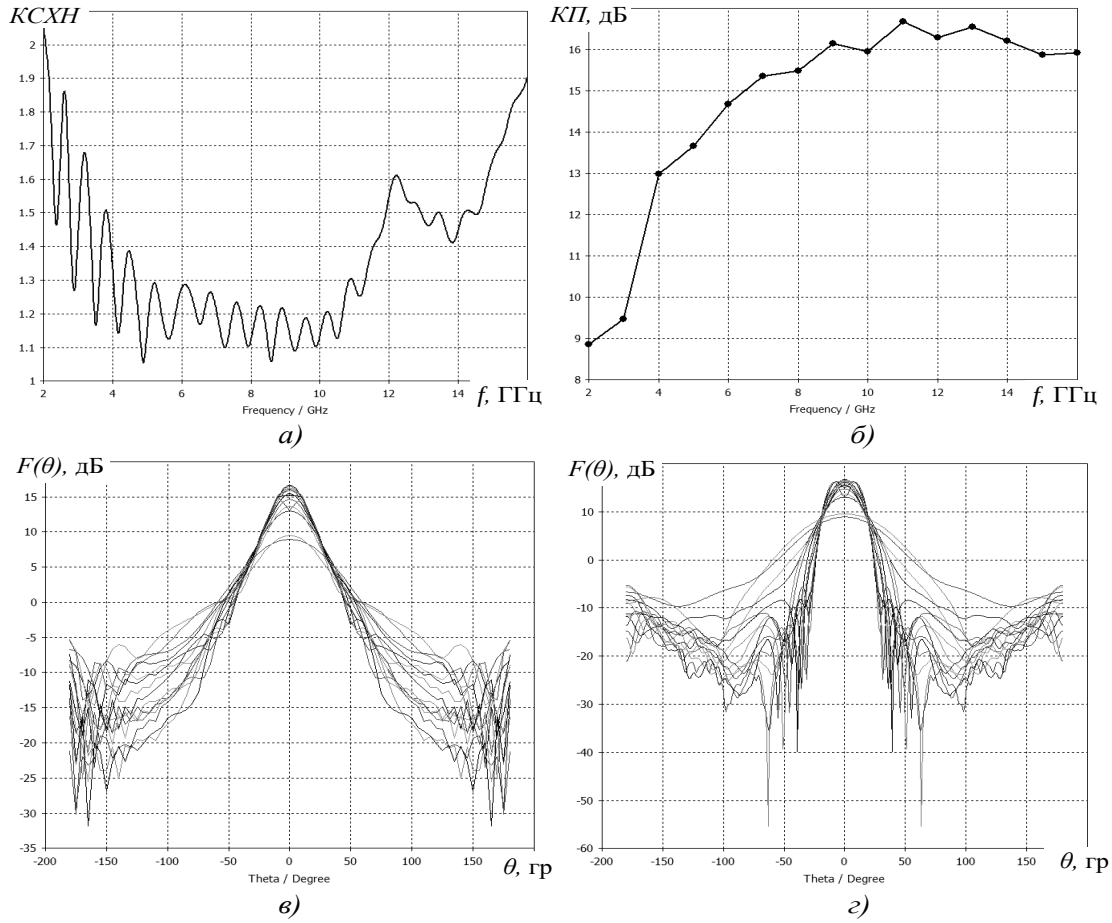
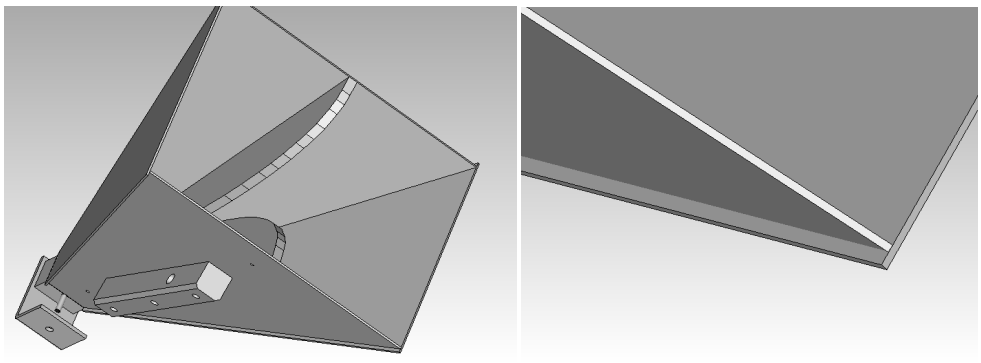


Рис. 2. Характеристики двогребеневої рупорної антени:
а) КСХН; б) КП; б) ДС у площині Е; б) ДС в площині Н

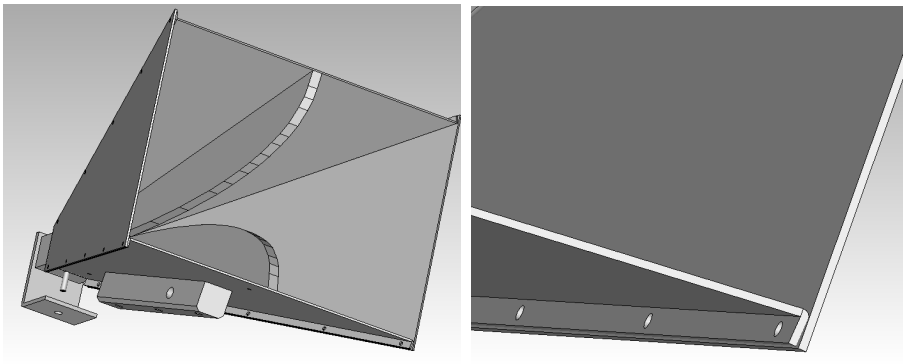
Аналіз характеристик базової моделі двогребеневої рупорної антени (рис. 2) показує відповідність їх відомим результатам [1–9], що підтверджує достовірність проведених розрахунків та адекватність розробленої програмної моделі.

У рамках першого завдання досліджень проаналізовано два можливі варіанти компонування елементів антени, які відрізняються між собою способом з'єднання кутів елементів розкриву. Перший варіант передбачає з'єднання поверхней, що утворюють розкрив, за допомогою припою (зварювання), другий – з'єднання механічним способом (використанням болтових кріплень або заклепок). Для вказаних варіантів компонувань створено програмні моделі, зовнішній вигляд яких зображено на рис. 3–4.



а) *б)*

Рис. 3. Програмна модель антени за схемою компонування з використанням технології спаювання: а) загальний вигляд; б) з'єднання нижньої та бокової пластин розкриву



а) *б)*

Рис. 4. Програмна модель антени за схемою компонування з використанням технології болтового з'єднання: а) загальний вигляд; б) з'єднання нижньої та бокової пластин

Програмні моделі антени мають можливість автоматичного масштабування в разі зміни розмірів рупора, а до їх конструктивних розмірів додано низку параметрів, які належать до елементів вказаних конструктивних рішень. За результатами досліджень розроблених моделей отримано залежності КСХН, КП, ширини діаграми спрямованості (ШДС) у площині *E* та *H* від частоти (рис. 5). Для порівняння на рис. 5 також зображено вказані характеристики для базової моделі антени.

Із рис. 5 видно, що розглянуті варіанти компонування забезпечують близькі за значенням технічні характеристики. Так, КСХН змінюється в діапазоні ±0,01, а КП у діапазоні ±0,04 дБ. Можна зробити висновок, що за однакової точності виготовлення елементів широкосмугової рупорної антени досліджені схеми компонування забезпечують близькі за значенням технічні характеристики.

У ході дослідження впливу неточностей у виготовленні елементів антени та їх з'єднанні між собою вносилися похибки в такі конструктивні розміри та параметри програмної моделі:

геометричні розміри хвилеводу і розкриву рупора;

положення провідника живлення та відстань між гребенями в точці збудження;

діаметр провідника живлення;

діелектричну проникність ізолювального матеріалу;

ширину щілин між пластинами розкриву рупора.

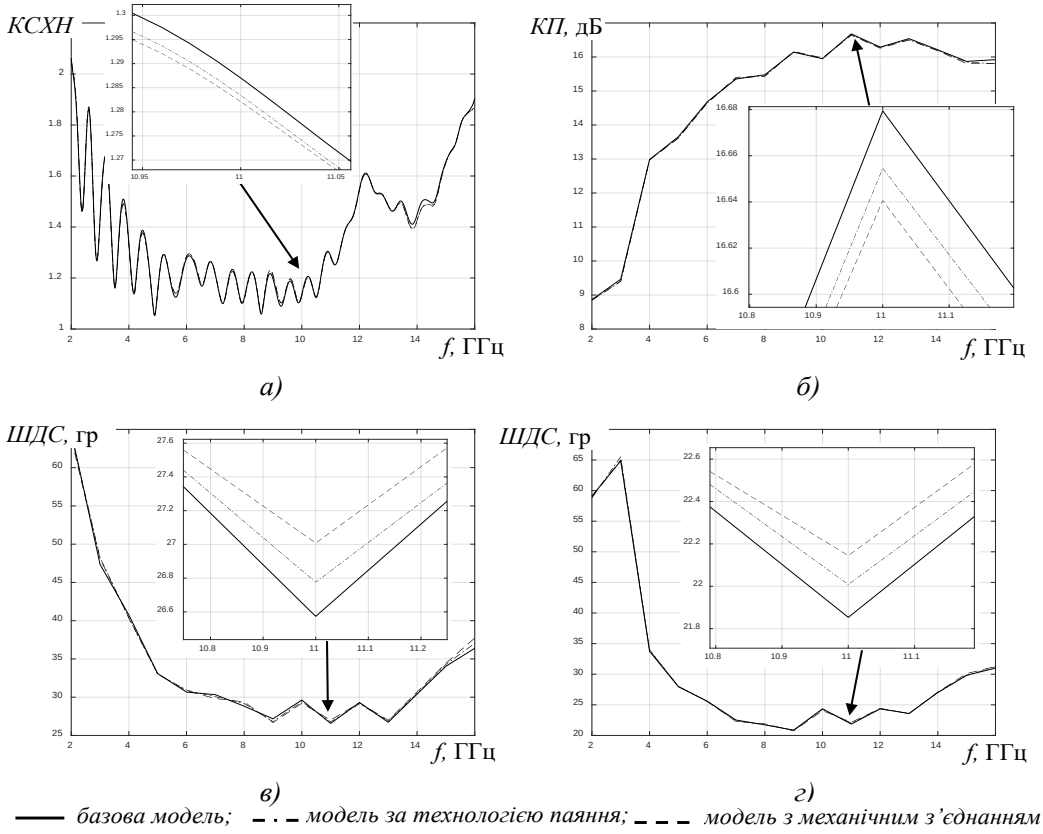


Рис. 5. Характеристики антени, отримані для різних схем компонування: а) КСХН; б) КП; в) ШДС в площині E; г) ШДС в площині H

Оскільки наявність вказаних похибок у виготовленні антени має найбільший вплив на її характеристики узгодженості, то в ході дослідження проаналізовано лише зміну КСХН у діапазоні робочих частот.

Для дослідження впливу похибок у геометричних розмірах хвилеводу на характеристики антени змінювалися ширина W_g (похибка ± 2 мм), висота H_g (похибка ± 2 мм) та довжина L_g (похибка ± 3 мм) хвилеводу і визначалися залежності КСХН від частоти. Отримані графіки зображено на рис. 6.

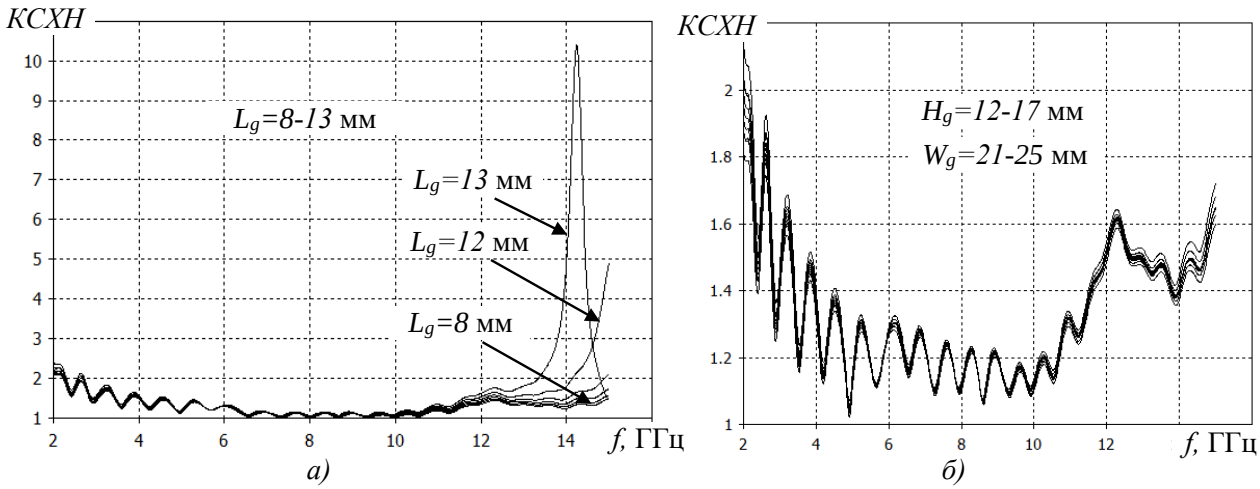


Рис. 6. Залежності КСХН від частоти: а) для різних довжин хвилеводу; б) для різних висоти та ширини хвилеводу

З рис. 6б випливає, що збільшення чи зменшення поперечних розмірів хвилеводу на 2 мм (8–13%) не призводить до суттєвої зміни КСХН, тому отримані графічні залежності практично зливаються в одну. Зміна ж поздовжніх розмірів (рис. 6а) негативно впливає на узгодженість антени, особливо на частотах вище 13 ГГц, де КСХН підвищується більш ніж у 6 разів.

Для дослідження впливу похибок у системі збудження рупора на характеристики антени змінювалися:

відстань від провідника збудження до кінця хвилеводу S_f (похибка ± 0,2 мм);

відстань між гребенями в точці збудження S_r (похибка ± 0,1 мм);

діаметр провідника збудження D_i (похибка ± 0,1 мм);

діелектрична проникність ізолювального матеріалу ε (похибка ± 0,8).

Отримані залежності КСХН від частоти для різних значень параметрів S_f та S_r наведено на рис. 7.

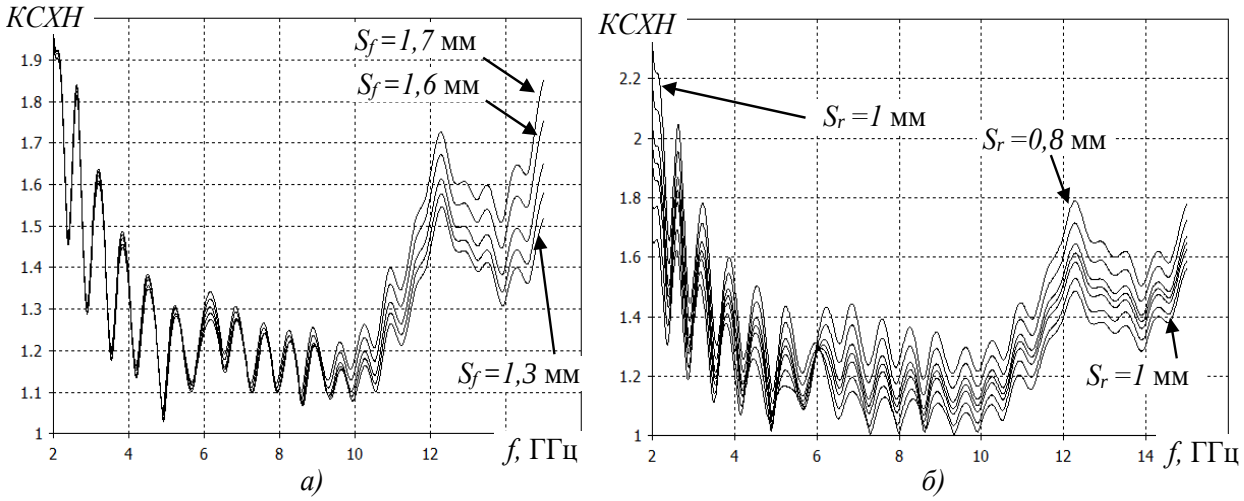


Рис. 7. Залежності КСХН від частоти:
а) для відстані до центра провідника збудження;
б) для відстані між гребенями в точці збудження

З рис. 7 випливає, що похибки у виготовленні елементів системи збудження призводять до зміни КСХН рупорної антени. Величина вказаних змін КСХН знаходиться в межах 20% та залежить від робочої частоти. Так, збільшення розміру S_r на 0,1 мм (9%) зменшує КСХН на 10% для частот вище 6 ГГц та підвищує його до 15% для частот нижче 6 ГГц. Тому для забезпечення розрахункових параметрів рупорної антени під час виготовлення її елементів живлення допуски на розміри мають бути мінімальними (менше 0,1 мм).

Вплив похибок значень діелектричної проникності ізолювального матеріалу та діаметра провідника збудження на максимальне $КСХН_{max}$ та середнє $КСХН_{mean}$ значення у робочій смузі антени зображено на рис. 8.

На рис. 8а видно, що зміна діелектричної проникності з 2 до 3 призводить до підвищення максимального значення КСХН на 23%, а зміна діаметра центрального провідника на 0,1 мм – до підвищення максимального значення КСХН на 21%.

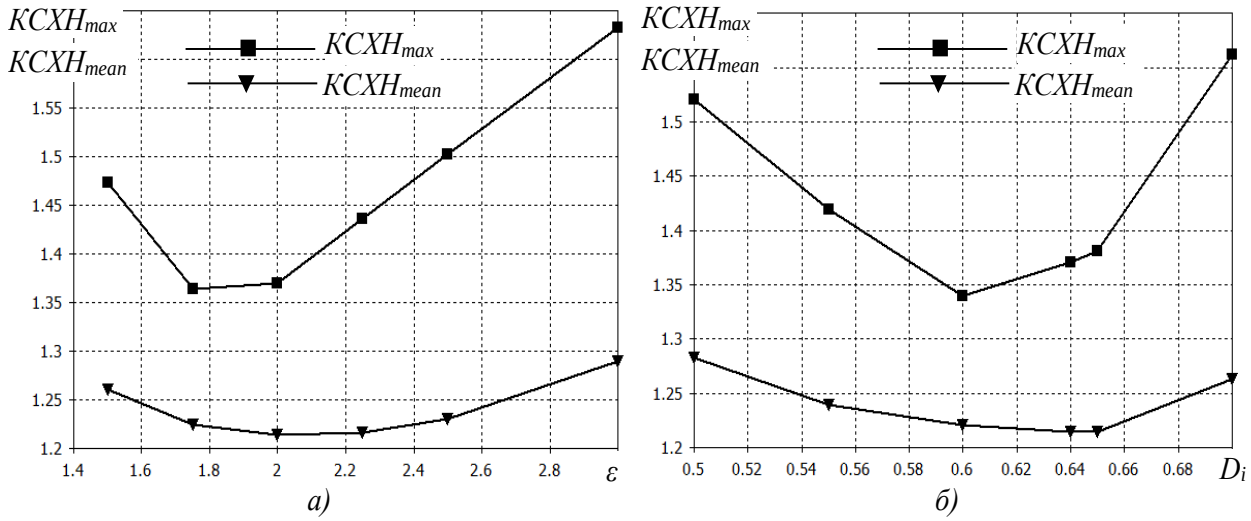


Рис. 8. Залежності максимального та середнього КСХН від частоти:
а) для діелектричної проникності ізолювального матеріалу;
б) для діаметра провідника збудження

На рис. 9 зображено залежності КСХН від ширини щілин w_s, що можуть виникати в місцях кріплення металевих поверхонь, які утворюють розкрив рупора. Ширина щілин w_s змінювалася від 0 до 0,4 мм із кроком 0,1 мм.

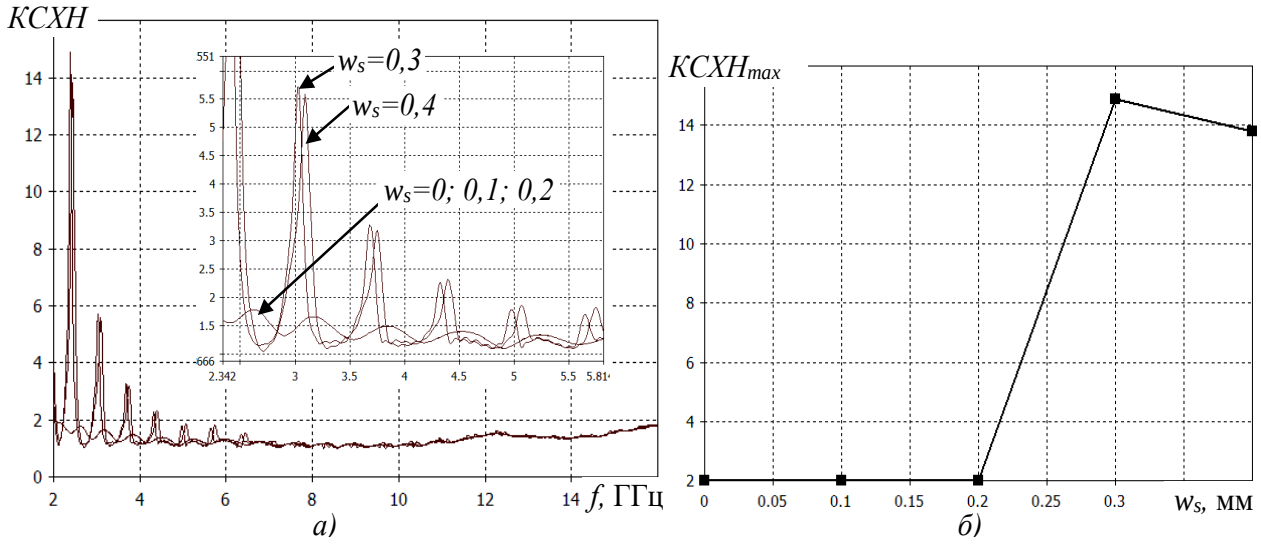


Рис. 9. Залежності:
а) КСХН від частоти для різних значень w_s;
б) максимального КСХН у смузі 2–15 ГГц від w_s

З рис. 9 видно, що в разі ширини щілин від 0,3 мм у розкриві рупора виникають резонансні явища і КСХН підвищується більше ніж в 7 разів (до 15), особливо це характерно для частот нижче 6 ГГц.

Якщо щілини між поверхнями рупора заповнити припоєм, наприклад, оловом, як це показано на рис. 10, то резонансні явища зникають, а значення КСХН практично не змінюється (рис. 11).

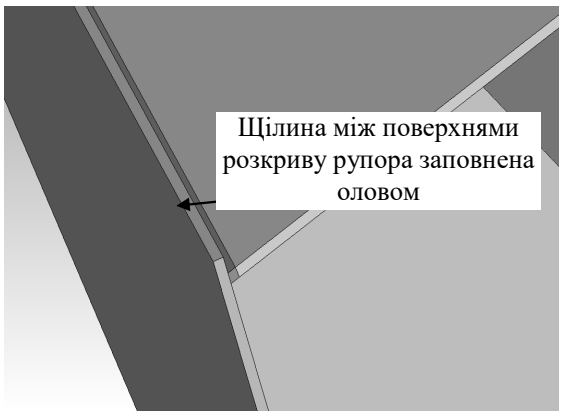


Рис. 10. Зовнішній вигляд щілини заповненої оловом

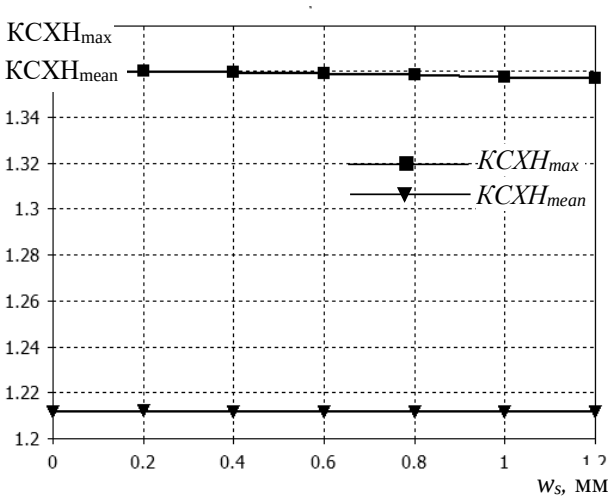


Рис. 11. Залежності середнього та максимального КСХН у смузі робочих частот від ширини щілини, заповненої оловом

Дослідження впливу похибок висоти та ширини розкриву рупора на КСХН показали, що похибки в межах 10% не призводять до його критичного зростання, а максимальне значення КСХН змінюється не більше ніж на 0,17, що відповідає, згідно з виразами (1) та (2), втратам менше ніж 2% енергії сигналу або зниженню коефіцієнта підсилення менше ніж на 0,08 дБ [12]:

$$PL(\%) = \left(\frac{VSWR-1}{VSWR+1}\right)^2 \cdot 100\,; \tag{1}$$

$$ML = -10\log\left(1-\left(\frac{VSWR-1}{VSWR+1}\right)^2\right), \tag{2}$$

де *VSWR* – КСХН;

PL (*%*) – втрати потужності сигналу у відсотках;

ML – втрати потужності сигналу в децибелах.

Враховуючи отримані результати, можна зробити висновок, що для забезпечення заданих параметрів та характеристик антени під час її виготовлення необхідно дотримуватися встановлених розмірів, а допуски не повинні перевищувати таких показників:

розміри розкриву рупора – 5 мм (5%);

ширина, довжина та висота хвилеводу живлення – 1 мм (6%);

відстань розміщення провідника збудження – 0,1 мм (6%);

відстань між гребенями – 0,1 мм (9%);

діаметр провідника збудження – 0,05 мм (7%);

діелектрична проникність ізолювального матеріалу – 0,2 (10%);

ширина щілини між поверхнями рупора – 0,3 мм.

Висновки. У разі однакової точності виготовлення елементів широкосмугової рупорної антени розглянуті варіанти компонування забезпечують близькі за значенням

технічні характеристики. Дослідження похибок виготовлення елементів антени показали, що найбільший вплив на її характеристики мають поздовжні розміри хвилеводу, відстань між гребенями, місце розміщення та діаметр провідника живлення, діелектричні характеристики ізолювального матеріалу. Так, збільшення зміщення провідника живлення вздовж широкої стінки хвилеводу на 0,5 мм та похибка встановлення гребенів 0,2 мм призводять до збільшення КСХН на 30%. Ширина щілин між поверхнями розкриву рупора до 0,3 мм суттєво не впливає на його КСХН, однак у разі більшого її значення виникають резонансні явища, а максимальне значення КСХН перевищує 14, середнє ж значення КП падає. Якщо вказані щілини заповнити металом, наприклад, оловом, то резонансні частоти зникають, а значення КСХН практично не змінюється. Обґрунтовано систему допусків на розміри основних елементів двогребеневої рупорної антени, дотримання яких забезпечить відповідність характеристик виготовленої антени отриманим у процесі моделювання та оптимізації з використанням спеціалізованих програмних засобів. Подальші роботи в даному напрямку доцільно спрямувати на дослідження впливу конструкцій систем живлення рупорної антени та способів кріплення гребенів усередині хвилеводу на технічні характеристики антени.

СПИСОК ЛІТЕРАТУРИ

1. Манойлов В. П., Павлюк В. В., Ставісюк Р. Л. Широкосмугові рупорні антени зі складною формою поперечного перерізу : монографія. Житомир, 2016. 212 с.
2. Jacobs D., Odendaal J. W., Joubert J. An Improved Design for a 1–18 GHz Double-Ridged Guide Horn Antenna. Pretoria, 2009. 9 p.
3. Куроптев П. Д., Левяков В. В, Фатеев А. В. Широкополосная рупорная антенна диапазона 0,8–30 ГГц // Электроника, измерительная техника, радиотехника и связь. Доклады ТУСУРа. 2016. Т. 19, № 2. С. 23–27.
4. Bruns C. Analysis and Simulation of a 1–18 GHz Broadband Double-Ridged Horn Antenna // IEEE TRANS. ON EC. 2003. Vol. 45, №. 1. P. 55-60.
5. Galvan-Tejada G. M., Peyrot-Solis M. A., Aguliar H. J. Ultra Wideband Antennas: Design, Methodologies, and Performance. CRC Press, 2015. 295 p.
6. Azimi M. A., Arazm F., Mohassel J. R. Design and optimization of a new 1–18 GHz double ridged guide horn antenna // Journal of Electromagnetic Wave and Applications. 2007. Vol. 21, № 4. P. 501–506.
7. Jarvis D. A., Rao T. C. Design of double-ridged rectangular wave guide of arbitrary aspect ratio and ridge height. Microw. Antenna Propagat // IEE Proc. 2000. Vol. 147. P. 31–34.
8. Ultra wideband double ridged horn with rectangular aperture / F. F. Dubrovka, G. A. Yena, P. Y. Stepanenko, V. M. Tereschenko // International Conference on Antenna Theory and Techniques. Seuastopol, 2003. P. 590–593.
9. Дубровка Ф. Ф., Сушко О. Ю. Ультраширокосмугова рупорна антена діапазону частот 1−20 ГГц з низьким рівнем бічного випромінювання // Вісник Нац. техн. ун-ту України "КПІ". Серія – Радіотехніка. Радіоапаратобудування. Київ, 2010. № 41. С. 68−73.
10. Additive manufacturing of a dual-ridged horn antenna / B. Majumdar, D. Baer, S. Chakraborty and other // Progress in electromagnetics research letters. Sydney, 2016. Vol. 9. P. 109–114.
11. CST STUDIO SUITE Electromagnetic and Multiphysics Simulation Software. URL: https://www.cst.com/products/csts2 (last accessed: 21.11.2019).

12. Antenna Magus. The leading antenna design tool. URL: www.antennamagus.com (last accessed: 21.11.2019).

Подано 30.12.2019

А. А. Нагорнюк, Ю. А. Колос

ВЛИЯНИЕ КОНСТРУКТИВНЫХ РЕШЕНИЙ КОМПОНОВКИ И ПОГРЕШНОСТЕЙ ИЗГОТОВЛЕНИЯ ЭЛЕМЕНТОВ ШИРОКОПОЛОСНОЙ РУПОРНОЙ АНТЕННЫ НА ЕЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

В статье представлены результаты исследования основных вариантов компоновки рупорной антенны с двумя гребнями, которые отличаются способами крепления элементов: болтовое соединение (заклепки) и пайка (сварка). Проанализировано влияние неточностей изготовления отдельных элементов антенны (погрешности геометрических размеров волновода и апертуры рупора, погрешности размещения проводника питания, различия диэлектрической проницаемости изолирующего материала от рассчитанной и другие) и в их соединении между собой (ширина щелей между пластинами апертуры рупора, расстояние между гребнями в точке возбуждения) на основные характеристики антенны (коэффициент стоячей волны по напряжению, коэффициент усиления, диаграмма направленности). Исследования проводились с использованием программных сред автоматизированного проектирования, моделирования и оптимизации трехмерных электромагнитных систем ANTENNA MAGUS и CST STUDIO SUITE. Установлено, что при одинаковой точности изготовления составляющих элементов широкополосной рупорной антенны рассмотренные варианты компоновки обеспечивают близкие по значению технические характеристики. Исследование погрешностей изготовления элементов антенны и их соединения между собой показали, что наибольшее влияние на характеристики антенны имеют продольные размеры волновода, расстояние между гребнями в точке возбуждения, место размещения и диаметр проводника питания, а также диэлектрические характеристики изолирующего материала. Установлено, что изменение отдельных размеров антенны на 10% может приводить к существенному ухудшению ее согласованности. Обоснована система допусков на размеры и соединения элементов антенны, соблюдение которых обеспечит соответствие характеристик изготовленного образца полученным в процессе моделирования и оптимизации с использованием специализированных программных средств.

Ключевые слова: *рупорная антенна; широкополосность; моделирование; компоновка; погрешности; волновод; характеристика; параметр; допуск.*

O. A. Nahorniuk, Y. O. Kolos

INFLUENCE OF CONSTRUCTIVE ARRANGEMENT DECISIONS AND MANUFACTURING ERRORS OF ELEMENTS OF THE WIDEBAND HORN ANTENNA ON ITS TECHNICAL CHARACTERISTICS

The results of the research of the main releases of arrangement of horn antenna with two ridges, which differ in the ways of fixing the elements: bolt connection (rivets) and soldering (welding), are presented in the article. The influence of inaccuracies in the manufacture of particular antenna elements (errors in the geometric dimensions of the waveguide and the horn aperture, errors in the location of the feed pin, differences in the relative permittivity of the

insulating material from the calculated one and others) and their interconnections (the width of the slots between the horn aperture plates, the distance between the ridges at the feeding point) on the main antenna characteristics (voltage standing-wave ratio, gain, radiation pattern). The researches were carried out using software environments for computer-aided designing, modeling and optimizing three-dimensional electromagnetic systems ANTENNA MAGUS and CST STUDIO SUITE. It has been found that with the same accuracy of manufacturing the constituent elements of a wideband horn antenna, the considered releases of arrangement provide similar technical characteristics. The research of manufacturing errors of the antenna elements and their interconnections showed that the longitudinal waveguide dimensions, the distance between the ridges at the point of excitation, the location and diameter of the feed pin, and also the dielectric characteristics of the insulating material have the greatest influence on the characteristics of the antenna. It has been established that a change in particular antenna sizes by 10% can lead to a significant deterioration in its matching.

The system of tolerances for the sizes and connections of antenna elements, the adherence of which will ensure the conformity of the characteristics of the manufactured example to those obtained in the process of modeling and optimization using specialized software, is justified.

Keywords: *horn antenna; wideband; modeling; arrangement; inaccuracies; waveguide; characteristic; parameter; tolerance***.**

ISSN 2076-1546

УДК 004.912 DOI: 10.46972/2076-1546.2019.17.10

О. В. Манько, О. М. Наумчак

ПІДХІД ДО ОРГАНІЗАЦІЇ ЗАХИСТУ ВІЙСЬКОВОСЛУЖБОВЦІВ ВІД НЕГАТИВНОГО ІНФОРМАЦІЙНОГО ВПЛИВУ

Упровадження інформаційно-комунікаційних технологій у всі сфери діяльності людини, зокрема й у військову, зумовлює появу широкого спектра загроз інформаційній безпеці. Серед них особливе місце займають загрози інформаційно-психологічного характеру, які проявляються у вигляді негативних інформаційних впливів на психологічний стан. Такі впливи реалізуються за допомогою інформаційних повідомлень, що сприймаються особою, та після опрацювання їх свідомістю корегують її світогляд: стверджують або змінюють переконання, погляди, принципи. Особливо небезпечними є подібні зміни у військовослужбовців, які виконують обов'язки у складі Об'єднаних сил на сході України. Постійний доступ особового складу до засобів масової інформації створює умови для реалізації таких загроз. Сукупність деструктивних повідомлень може зумовлювати тривалі відхилення від нормального психологічного стану військовослужбовця і, як наслідок, перешкоджати виконанню функціональних обов'язків. Актуальним є завдання з розробки підходу до організації захисту від такого впливу.

У роботі проаналізовано досвід, отриманий у ході моніторингу інформаційного простору, та описано основні способи створення й розповсюдження матеріалів із негативним інформаційним впливом на особовий склад Збройних Сил. Запропоновано підхід до визначення рівня негативного інформаційного впливу в засобах масової інформації, що дозволяє кількісно оцінювати аспекти інформаційного протиборства та створює теоретичну основу для розробки автоматизованих комплексів підтримки і прийняття рішень, що стосуються захисту особового складу від негативного інформаційного впливу. Наведено рекомендації для забезпечення захисту військовослужбовців від деструктивного впливу та сформовано загальний підхід до його організації.

Отже, для досягнення поставленої мети у даній роботі вирішуються завдання щодо: аналізу способів та методів здійснення негативних інформаційних впливів Російською Федерацією через засоби масової інформації; вивчення досвіду з протидії такому впливу з боку Міністерства оборони України та Збройних Сил України; розробки підходів до підвищення ефективності такої діяльності; вироблення рекомендацій щодо організації захисту особового складу, який бере участь у стримуванні агресії Росії. Отримані результати можуть бути використані в ході інформаційних операцій для реалізації заходів захисту інформаційного простору.

Ключові слова: *негативний інформаційно-психологічний вплив; інформаційні та психологічні загрози; особовий склад; інформаційні операції; організація захисту.*

Постановка проблеми в загальному вигляді. Упровадження інформаційно-комунікаційних технологій у всі сфери діяльності людини, зокрема й у військову, зумовлює появу широкого спектра загроз інформаційній безпеці. Серед них особливе місце займають загрози інформаційно-психологічного характеру. Вони проявляються у вигляді негативних

інформаційних впливів на психологічний стан людини, які реалізуються через інформаційні повідомлення. Результатом обробки таких повідомлень свідомістю особи є трансформація її світогляду: підтвердження або зміна переконань, поглядів, принципів та, як результат, поведінки.

В умовах агресії Російської Федерації (РФ), проведення операції Об'єднаних сил на сході нашої держави деструктивний інформаційно-психологічний вплив на військово-політичне керівництво, військовослужбовців Збройних Сил (ЗС) та цивільне населення України здійснюється в основному через електронні засоби масової інформації (ЗМІ). Через широкі можливості щодо розповсюдження повідомлень в інформаційному просторі, державну монополію РФ на ЗМІ та відсутність дієвих механізмів виявлення і нейтралізації негативних інформаційних впливів, в Україні існує суттєва загроза національним інтересам держави в цілому і її ЗС зокрема. Вільний доступ особового складу до ЗМІ створює потенційно сприятливі умови для реалізації інформаційно-психологічних загроз.

Отже, організація захисту військовослужбовців від негативного інформаційного впливу, що розповсюджуються в ЗМІ, є важливим та актуальним науково-практичним завданням.

Аналіз останніх досліджень та публікацій. Сьогодні в наукових виданнях значна увага приділяється розробці методів та способів ведення інформаційної боротьби (ІБ). У роботах [1–4] автори досліджують види та сфери ведення ІБ, визначають її мету та основні напрямки. При цьому в [4] не наведено класифікації методів та способів ведення ІБ, що ускладнює виявлення її технологічних аспектів. Подана в [5, 6] класифікація має дещо суб'єктивний характер, оскільки не дозволяє в повній мірі врахувати роль офіційних друкованих ЗМІ та телебачення в ІБ. Матеріали публікацій [1, 2] більше спрямовані на встановлення тенденцій створення та розвитку інтернет-спільнот, способів розповсюдження інформації визначеного контенту.

Суб'єктами ІБ РФ є в основному політичне і військове керівництво. Тому цілком очевидно, що негативний інформаційний вплив спрямований насамперед на: створення та нагнітання конфліктної обстановки всередині України; провокацію політичної напруги та хаосу; дискредитацію органів державної влади, військово-політичного керівництва, військовослужбовців ЗС та представників інших силових структур; ініціювання масових протестних акцій та заворушень; дестабілізацію у відносинах між політичними партіями; спробу розв'язання в державі громадянської війни тощо.

Аналіз змісту негативного інформаційного впливу, закладеного в інформаційні повідомлення, у [7, 8] дозволив виділити основні його спрямування на: прийняття політичних рішень; формування громадської думки; формування суспільної свідомості (книги, фільми, телевізійні програми, друковані ЗМІ); психологічний стан окремих осіб, що приймають рішення (дискредитація командирів, начальників). А електронні ЗМІ, які застосовуються як на підготовчому, основному, так і на завершальному етапах ІБ [9], залишаються найбільш потужним інструментом реалізації таких впливів.

Формулювання завдання дослідження. Інформаційне протиборство є постійно діючим елементом зовнішньої політики усіх держав світу. Це очевидний факт сьогодення, який загострився з переходом людства на нову стадію розвитку – створення інформаційного суспільства. Аналіз сутності конфліктів у світі підкреслює домінуючу

роль інформаційного протиборства в ході їх перебігу. РФ має значний потенціал для ведення інформаційної боротьби. Кілька останніх століть дії нашого північно-східного сусіда спрямовані на недопущення української державності, а з її виникненням – на її знищення. Конфлікт, що триває, ґрунтується на багаторічній експансії інформаційного простору з метою витіснення української ідентифікації. За таких умов особливо небезпечний негативний інформаційний вплив на військовослужбовців, які виконують обов'язки у складі Об'єднаних сил на сході України. Тому питання створення системи протидії агресивним діям в інформаційному просторі є завжди достатньо актуальним аспектом системи національної безпеки. Відповідно, метою статті є розробка підходу до організації захисту військовослужбовців від негативного інформаційного впливу.

Виклад основного матеріалу. Організація захисту військовослужбовців від негативного інформаційного впливу передбачає наявність трьох складових:

моніторингу інформаційного простору;

аналізу та прогнозування інформаційних загроз, вироблення стратегій та планів щодо забезпечення захисту особового складу ЗС;

нейтралізації таких впливів та здійснення адекватних контр- та превентивних заходів.

Ці складові є основою для функціювання системи інформаційно-психологічної безпеки військовослужбовців. Узагальнена модель формування морально-психологічного стану військовослужбовця зображена на рис. 1.

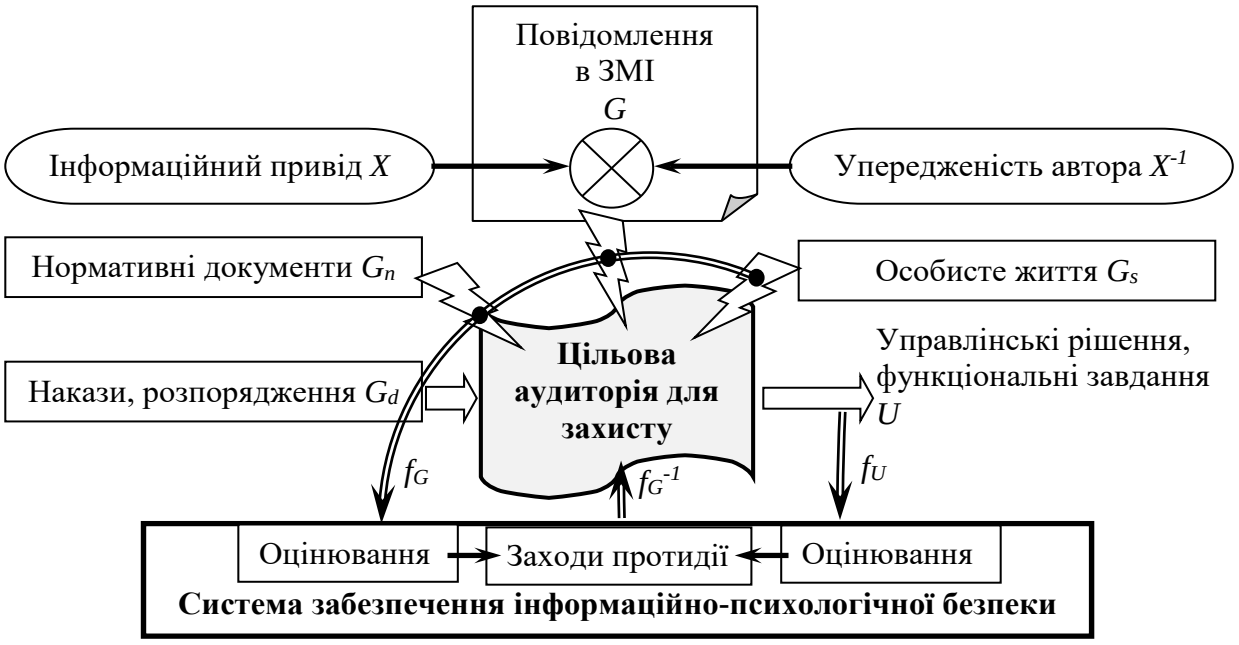


Рис. 1. Модель формування морально-психологічного стану військовослужбовця

Цілком очевидно, що велика кількість інформаційних ресурсів та каналів доступу до них потребують автоматизації такої діяльності. Це дозволить збільшити ймовірність завчасного виявлення наявних носіїв негативного впливу та розробки ефективних заходів для їх нейтралізації. Крім того, зазначене сприятиме більш якісному прогнозуванню можливого розвитку інформаційних та психологічних акцій (дій) противника, зокрема визначенню тематик та спрямування інформаційних повідомлень. Оперативність такої роботи (моніторингу) є доволі важливим аспектом у забезпеченні переваги

в інформаційному просторі. Якісне її виконання дозволить покращити стан захищеності особового складу від негативних впливів.

Загальна база результатів моніторингу дозволяє організовувати обробку даних для виявлення тенденцій, предметно обґрунтовувати прогнози розвитку ситуації. Це дозволить більш об'єктивно оцінювати обстановку, що склалася, а також виявляти ознаки ведення РФ інформаційних (психологічних) операцій, їх цілей та можливого розвитку в подальшому.

Суть роботи системи забезпечення інформаційно-психологічної безпеки полягає в:

постійному спостереженні за психологічним станом особового складу;

моніторингу інформаційного простору з метою виявлення загроз інформаційній безпеці, при цьому особлива увага приділяється негативним психологічним впливам, що розповсюджуються через ЗМІ;

підготовці та провадженні заходів, спрямованих на нейтралізацію загроз інформаційній безпеці та підтримання належного стану інформаційно-психологічної безпеки.

Як було зазначено вище, інформаційні повідомлення ЗМІ є основним носієм негативних інформаційних впливів. Аналіз таких повідомлень дозволить визначити рівень реалізованих у них деструктивних загроз для особового складу ЗС України.

Аналіз продукції, що розробляється противником для реалізації негативних інформаційних впливів і розповсюджується в ЗМІ, дозволяє виділити основні способи виявлення та протидії негативним інформаційним впливам. Для цього необхідно розробити підходи, які б дозволили виявляти негативні впливи в інформаційних повідомленнях та прогнозувати їх наслідки. Відповідно, необхідно вирішити низку часткових завдань, а саме:

оцінювання рівня деструктивності негативних інформаційних впливів;

визначення цілей такого випливу (спрямування та цільова аудиторія);

виявлення каналів впливу;

отримання вихідних даних для організації;

здійснення заходів протидії.

Оцінювання рівня негативних інформаційних впливів має здійснюватися на основі комплексного показника. З одного боку, він зважує потенційний негативний інформаційний вплив, зумовлений повідомленнями в ЗМІ. З іншого – враховує потенційну можливість ураження цільової аудиторії, що залежить від наявних каналів доступу до ЗМІ, а також від особистісних характеристик окремих складових цільової аудиторії (соціальних груп).

Рівень деструктивності інформаційного повідомлення $K_{пов}$ пропонуємо визначати на основі двох його складових: коефіцієнтів об'єктивності $\left(K_{об}\right)$ та негативної тональності $\left(K_{нт}\right)$. Для отримання оцінки рівня деструктивності повідомлення коефіцієнти об'єктивності та негативної тональності узагальнюються за мультиплікативною згорткою, оскільки мають однакову важливість:

$$K_{пов} = K_{об} \cdot K_{нт}. \qquad (1)$$

Коефіцієнт об'єктивності $K_{об}$ показує рівень достовірності повідомлення та є кількісною оцінкою наявних у наведених матеріалах аргументів, щоб визнати його таким, що відображає дійсність. Коефіцієнт негативної тональності $K_{нт}$ показує кількісну оцінку відхилення наведених фактів у повідомленні від офіційної позиції військово-політичного керівництва держави, загальноприйнятих норм: етичних, релігійних, ділових, культурних тощо.

Визначення рівня загроз кожного повідомлення $\left(K_{пов}\right)$ здійснюється методом експертного оцінювання. Значення коефіцієнтів об'єктивності та негативної тональності аналітик обирає, спираючись на власний досвід, у ході оцінювання кожного окремого повідомлення в діапазоні від 0 до 1 з кроком 0,01. Значення коефіцієнта об'єктивності повідомлення пропонуємо обирати з діапазонів, наведених у табл. 1, а негативну тональність – з використанням значень, наведених у табл. 2. Зауважимо, що діапазони було визначено в ході безпосереднього моніторингу інформаційних повідомлень за емпіричним підходом [10].

Таблиця 1

Значення коефіцієнта об'єктивності повідомлень

Джерело повідомлення	Діапазон значення коефіцієнта
Офіційне джерело (пряма мова без перекладу та скорочень)	0,80–1,0
Цитування офіційних джерел (використання перекладу та (або) редагування контексту)	0,60–0,79
Коментар компетентних за даним напрямком осіб	0,30–0,59
Інші коментарі	0,01–0,29

Таблиця 2

Значення коефіцієнта негативної тональності повідомлення

Показник негативної тональності	Діапазон значення коефіцієнта
Небезпечний	0,80–1,0
Високий	0,50–0,79
Середній	0,20–0,49
Низький (нейтральний)	0,01–0,19

Значення коефіцієнта також може залежати від тематики повідомлення $\left(\tau\right)$ – спрямування його на формування відчуття (переконань) загрози щодо реалізації потреб людини, зміни (руйнування) сформованих особистих цінностей. Варіанти тематик наведено в табл. 3. Коефіцієнт τ_i характеризує відносний вплив *i*-ї тематики на підвищення рівня деструктивного впливу ЗМІ. Значення коефіцієнта для кожної тематики пропонуємо обирати в діапазоні $\tau_i \in \left[1...7\right]$ з урахуванням теорії мотивацій, розробленої А. Маслоу [11]. Особливістю даних коефіцієнтів є те, що вони можуть мати однакові значення, за умови однакового відносного впливу *i*-ї тематики.

Таблиця 3

Значення коефіцієнта тематики інформаційних повідомлень

Суть тематики інформаційних повідомлень	Позначення	Важливість тематики
Загроза фізіологічним потребам	τ_1	7
Загроза життю (здоров'ю) власному (близьких)	τ_2	7
Загроза втрати можливості спілкування з близькими	τ_3	6
Загроза втрати джерела фінансування	τ_4	6
Загроза задоволенню інформаційних потреб	τ_5	3
Загроза перешкоджання особистому розвитку	τ_6	2
Загроза реалізації естетичних потреб	τ_7	1

Рівень деструктивного впливу за тематикою розраховується через рівні деструктивного впливу всіх повідомлень з даної тематики з використанням згортки за нелінійною схемою компромісів [12]:

$$K_{\tau} = 1 - \left(\sum_{i=j}^{n} a_j \left(1 - K_{пов_j} - \delta \right)^{-1} \right)^{-1}, \qquad (2)$$

де K_{τ} – рівень деструктивного впливу за тематикою;

n – кількість повідомлень з даної тематики;

$a_j = 1n$ – вагові коефіцієнти, які характеризують ступінь впливу *j*-го повідомлення на рівень деструктивного впливу за тематикою, беруться однаковими для всіх повідомлень;

$\delta = 0,001$ – константа, яка дозволяє уникнути ділення на нуль.

Отже, застосування даної згортки дозволяє з більшою чутливістю враховувати наявність деструктивних повідомлень за вибраною тематикою.

Для визначення результуючого рівня деструктивного негативного інформаційного впливу на конкретну особу $(K_{ос})$, реалізованого в повідомленнях певної тематики, використовуємо згортку за нелінійною схемою компромісів:

$$K_{ос} = 1 - \left(\sum_{i=1}^{m} \left(\frac{\tau_i}{\sum_{k \in m} \tau_k} \left(1 - K_{\tau_i} - \delta \right)^{-1} \right) \right)^{-1}, \qquad (3)$$

де $m \in M$ – підмножина тематик, які висвітлюються в ЗМІ та переглядаються особою, що їх оцінює.

Показник (3) дає змогу оцінити рівень негативного інформаційного впливу з використанням оберненої нормованої шкали, наведеної в табл. 4 [6].

Оцінку рівня негативного інформаційного впливу, який потенційно може бути здійснений на особовий склад (цільову аудиторію), у цілому доцільно розрахувати за допомогою виразу (4), використовуючи табл. 4:

$$K_{ЦА} = 1 - \left(\sum_{i=1}^{z} d_i \left(1 - K_{ос_i} - \delta \right)^{-1} \right)^{-1}, \qquad (4)$$

де z – кількість осіб у підрозділі;

d_i – вагові коефіцієнти, які дозволяють враховувати посадові обов'язки особи, що оцінюється.

Таблиця 4

Обернена нормована шкала

Категорія рівня деструктивного впливу повідомлень	Значення $K_{ос}$
Критичний	0,81 – 1,0
Небезпечний	0,61 – 0,8
Високий	0,41 – 0, 6
Середній	0,21 – 0,4
Низький	0,01 – 0,2

Щодобове оцінювання в ході здійснення моніторингу повідомлень у ЗМІ дозволяє відслідковувати динаміку розповсюдження негативних впливів. Отримані результати моніторингу надають можливість корегувати психологічний стан військовослужбовців.

Для забезпечення захисту військовослужбовців від негативного інформаційного впливу, окрім оцінювання рівня деструктивності повідомлень, також необхідно:

удосконалити нормативно-правову базу, щоб надати основу для проведення спеціальних дій щодо виявлення, оцінювання інформаційних загроз та протидії їм відповідними органами;

розвивати систему підготовки та навчання як рядового й сержантського складу, так і офіцерського складу з метою вироблення компетенцій для особистого захисту, а також запобігання та нейтралізації негативних інформаційних впливів противника на підлеглих;

підтримувати та розвивати національну ідею, створювати і популяризувати всебічні ціннісні настанови, спрямовані на власну національну ідентичність;

збільшувати присутність та якість контенту українських телевізійних каналів, радіомовлення, електронних ресурсів в інформаційному просторі.

Крім того, слід виділити і такі підходи для запобігання деструктивної дії негативного інформаційного впливу на цільову аудиторію: завчасне попереджання про підготовку противником здійснення впливу; заохочення особового складу до зберігання вірності своїм патріотичним переконанням; оволодіння ним знаннями для об'єктивності оцінювання ситуації; проведення тренінгів щодо аналізу інформації, яка надходить зі ЗМІ.

Важливу роль для забезпечення реалізації зазначених вище підходів відіграє моніторинг інформаційних ресурсів. Його результати дозволяють узагальнювати інформацію щодо виявлених прийомів маніпулювання серед негативних інформаційних впливів та своєчасно вдосконалювати систему протидії.

Оперативність виявлення негативного впливу та його нейтралізацію можна забезпечити, автоматизувавши процес моніторингу інформаційного простору, використавши описаний вище підхід до його оцінювання. Для цього пропонуємо на першому етапі сформувати перелік інформаційних джерел для моніторингу (шляхом опитування особового складу щодо того, з яких інформаційних ресурсів вони отримують інформацію про події у світі, Україні), визначити формат та періодичність опрацювання

результатів моніторингу, сформувати перелік тематик, за якими необхідно проводити спостереження. На другому етапі потрібно проводити безпосередньо моніторинг інформаційного простору. Оцінювання рівня негативного інформаційного впливу варто здійснювати за розглянутим вище підходом. Отримані кількісні характеристики дадуть змогу робити ретроспективний аналіз. Це сприятиме розробленню підходів для нейтралізації або попередження негативного інформаційного впливу.

Висновки. У статті розглянуто підходи до оцінювання рівня негативного інформаційного впливу у ЗМІ, розрахунку потенційних можливостей противника щодо негативного інформаційного впливу на особовий склад ЗС України. Розроблений математичний апарат дозволяє кількісно оцінювати відповідні аспекти інформаційного протиборства, що дає можливість систематизувати та формалізувати таку діяльність. Це створює теоретичну основу для розроблення автоматизованих комплексів підтримки і прийняття рішень.

Запропоновані підходи до організації захисту особового складу від негативного інформаційного впливу дозволять покращити стан інформаційно-психологічної безпеки за рахунок завчасного надання відповідним органам інформації для реалізації превентивних заходів та формування стратегії здійснення корегування психологічного стану. Окрім того, отримані результати забезпечують можливість здійснення індивідуального підходу до корекції психологічного стану особового складу, що бере участь проведенні операції Об'єднаних сил.

Наукова новизна наведених результатів полягає в розробленні підходу до організації захисту військовослужбовців від негативного інформаційного впливу на основі визначення рівня його деструктивності, а також в обґрунтуванні показників для оцінювання рівня негативних впливів в електронних ЗМІ, що дозволяє кількісно їх оцінювати. Практичне значення одержаних результатів полягає в забезпеченні підвищення ефективності заходів захисту військовослужбовців від негативного психологічного впливу в ЗМІ.

Подальші дослідження доцільно спрямувати на вдосконалення програмного комплексу, а також на визначення часткових показників, які дають кількісну оцінку таким показникам: наявному рівню негативного інформаційного впливу в ЗМІ; інформаційній інфраструктурі в районах розміщення військ (сил) – окремих груп цільових аудиторій; морально-психологічному стану цільової аудиторії (з огляду її залежності від рівня негативного інформаційного впливу).

СПИСОК ЛІТЕРАТУРИ

1. Військовий стандарт ВСТ 01.004.004 – 2014 (01). Інформаційна безпека держави у воєнній сфері. Терміни та визначення. Київ, 2014. 32 с.
2. Левченко О. В. Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату // Наука і оборона. 2013. № 3. С. 21–26.
3. Информационные войны в интернете. URL: http://emirr.ru/emirr_articles/232-informacionnye-vojny-v-internete.html (дата обращения: 20.02.2019).
4. Гриненко І., Прокоф'єва Д. Вплив віртуальних спільнот на інформаційну безпеку: сучасний стан та тенденції розвитку // Правове, нормативне та метрологічне забезпечення

системи захисту інформації в Україні. 2012. Вип. 1 (23). С. 18–23.
5. Спосіб поширення інформації та запобігання поширенню інформації в комп'ютерній мережі. URL: http://findpatent.com.ua/patent/240/2408145.html (дата звернення: 17.03.2019).
6. Корнієнко С. Путін веде в Україні гібридну війну – генерал Каппен. URL: https://www.radiosvoboda.org/a/25363591.html (дата звернення: 20.09.2019).
7. Технология мониторинга новостей. URL: http://infostream.ua/ (дата обращения: 20.02.2019).
8. Грищук Р. В., Манько О. В., Орищук І. О. Особливості організації та ведення моніторингу електронних засобів масової інформації комунікації // Інформаційна безпека : наук. журнал. Луганськ, 2014. Вип. 3 (15). С. 10–15. ISSN 2224-9613.
9. Кучеренко С. М. Психічна стійкість як фактор організації ефективної діяльності фахівця в екстремальних умовах // Проблеми екстремальної та кризової психології : зб. наук. праць. Харків : НУЦЗУ, 2015 . Вип. 17 . С. 165.
10. Ландэ Д. В. Стабильность источников как один из параметров информационных потоков // Компьютерная лингвистика и интеллектуальные технологи: по материалам ежегодной Междунар. конф. "Диалог". Вып. 7 (14). Москва : РГГУ. 2008. С. 332-334.
11. Рассел Джесси. Пирамида потребностей по Маслоу. Москва : Книга по требованию, 2016. 496 с.
12. Корпорация в системе общественного производства : монография / [Л. И. Дмитриченко, Т. С. Чунихина, Л. А. Дмитриченко, А. Н. Химченко]. Донецк : ООО «Східний видавничий дім», 2010. 220 с.
13. FM 3-05.301 Psychological Operations Process Tactics, Techniques and Procedures. URL: https://info.publicintelligence.net/USArmy-PsyOpsTactics.pdf (дата звернення: 18.03.2019).
14. Почепцов Г. Г. Сучасні інформаційні війни. Вид. 3-тє, доповн. та переробл. Київ : Вид. дім "Києво-Могилянська академія", 2016. 504 с.

Подано 30.12.2019

О. В. Манько, Е. М. Наумчак

ПОДХОД К ОРГАНИЗАЦИИ ЗАЩИТЫ ВОЕННОСЛУЖАЩИХ ОТ НЕГАТИВНОГО ИНФОРМАЦИОННОГО ВЛИЯНИЯ

Внедрение информационно-коммуникационных технологий во все сферы деятельности человека, в том числе и в военную, приводит к появлению широкого спектра угроз информационной безопасности. Среди них особое место занимают угрозы информационно-психологического характера, которые проявляются в виде негативных информационных воздействий на психологическое состояние. Такие воздействия реализуются с помощью информационных сообщений, которые воспринимаются человеком, и после обработки их сознанием корректируют его мировоззрение: утверждают или меняют убеждения, взгляды, принципы. Особенно опасны подобные изменения у военнослужащих, выполняющих обязанности в составе Объединенных сил на востоке Украины. Постоянный доступ личного состава к средствам массовой информации создает условия для реализации таких угроз. Совокупность деструктивных сообщений может вызывать длительные отклонения от нормального психологического

состояния военнослужащих и, как следствие, препятствовать выполнению функциональных обязанностей. Актуальной является задача по разработке подхода к организации защиты от такого воздействия.

В работе проанализирован опыт, полученный в ходе мониторинга информационного пространства, и описаны основные способы создания и распространения материалов с негативным информационным влиянием на личный состав Вооруженных Сил. Предложен подход к определению уровня негативного информационного воздействия в средствах массовой информации, позволяющий количественно оценивать аспекты информационного противоборства и создающий теоретическую основу для разработки автоматизированных комплексов поддержки и принятия решений, касающихся защиты личного состава от негативного информационного воздействия. Приведены рекомендации для обеспечения защиты военнослужащих от деструктивного влияния и сформирован общий подход к ее организации.

Следовательно, для достижения поставленной цели в данной работе решаются задачи по: анализу способов и методов осуществления негативных информационных воздействий Российской Федерацией через средства массовой информации; изучению опыта по противодействию такому влиянию со стороны Министерства обороны Украины и Вооруженных Сил Украины; разработке подходов к повышению эффективности такой деятельности; выработке рекомендаций по организации защиты личного состава, участвующего в сдерживании агрессии России. Полученные результаты могут быть использованы в ходе информационных операций для реализации мер защиты информационного пространства.

Ключевые слова: *негативное информационно-психологическое воздействие; информационные и психологические угрозы; личный состав; информационные операции; организация защиты.*

O. V. Manko, O. M. Naumchak

APPROACH FOR THE ORGANIZATION OF PROTECTION OF MILITARY PERSONNEL FROM NEGATIVE PSYCHOLOGICAL INFLUENCE

The introduction of information and communication technologies in all spheres of human activity, including in the military, causes the emergence of a wide range of threats to information security. Among them, special place is occupied by threats of information and psychological character, which manifest themselves in the form of negative information influences on the psychological state. Such influences are realized with the help of information messages that are perceived by the person, and after processing their consciousness, they adjust their worldview: affirm or change beliefs, attitudes, principles. Particularly dangerous are the changes in the military serving in the Allied Forces in eastern Ukraine. The constant access of the personnel to the media creates the conditions for the realization of such threats. A set of destructive messages can lead to prolonged deviations from the normal psychological state of the serviceman and, as a consequence, impede the performance of functional duties. The urgent task is to develop an approach to the organization of protection against such influence.

This paper analyzes the experience gained during the monitoring of the information space and describes the main methods for creating and disseminating materials with a negative

information impact on the Armed Forces personnel. An approach to determining the level of negative information influence in the media is offered, which allows to quantify aspects of information confrontation and creates a theoretical basis for the development of automated complexes of support and decision making regarding the protection of personnel from negative information influence. Recommendations are given to ensure the protection of military personnel from destructive influence and formulate a general approach to its organization.

Therefore, in order to achieve this goal, the tasks are solved in the following: analysis of ways and methods of implementation of negative information influences by the Russian Federation through mass media; study of experience in counteracting such influence by the Ministry of Defense of Ukraine and the Armed Forces of Ukraine; developing approaches to increase the effectiveness of such activities; making recommendations on the organization of protection of personnel involved in deterring Russia's aggression. The results obtained can be used in information operations to implement information space security measures.

Keywords: *negative informational and psychological impact; informational and psychological threats; personnel; informational operations; organization of defense.*

УДК 621.396 DOI: 10.46972/2076-1546.2019.17.11

О. Л. Сидорчук, С. П. Фриз, В. Й. Залевський, Л. М. Марищук

ЧИСЛОВИЙ МЕТОД ВИЗНАЧЕННЯ ЕЛЕКТРОМАГНІТНОГО ПОЛЯ В ОБЛАСТІ ФОКУСА ПАРАБОЛОЇДА ОБЕРТАННЯ ДЗЕРКАЛЬНОЇ АНТЕННОЇ СИСТЕМИ

У ході аналізу антен та розробки їх нових зразків, зокрема й дзеркальних, необхідно визначити (розрахувати) їх основні характеристики (параметри). Для цього потрібно дослідити електромагнітне поле, яке збуджується в області фокуса параболоїда обертання, що опромінюється рупорним опромінювачем.

На даний час такі розрахунки проводяться за допомогою сучасних програмних продуктів моделювання. Вони ґрунтуються на загальних числових методах розв'язання рівнянь Максвелла та подаються як готовий продукт без розкриття внутрішнього змісту. Тому оцінювання похибки розрахунків за допомогою таких програм практично неможливе.

Унаслідок математичної складності навіть найпростіших задач розсіювання та дифракції рідко вдається отримати в замкнутому вигляді рішення, придатні для безпосереднього розрахунку практично корисних фізичних характеристик. Отже, доводиться допускати певний ступінь наближення для формування граничних умов, розв'язання рівнянь або на всіх етапах.

Отримані раніше алгоритми розрахунку мають недолік, оскільки можуть бути реалізовані лише числовими методами, тому що отримані інтеграли не є табличними і не підлягають приведенню до таких. Саме тому виникає необхідність у спрощенні виразів для розсіяного рупором поля шляхом апроксимації й отримання простих формул.

У статті запропоновано визначення електромагнітного поля в області фокуса параболоїда обертання дзеркальної антени та на осі дзеркала шляхом розв'язання інтегральних рівнянь числовим методом за нормальної поляризації падаючої хвилі.

Новизна отриманих результатів полягає в застосуванні нового числового методу визначення розсіяного електромагнітного поля, перевипроміненого рупорним опромінювачем, розташованим у фокусі параболоїда обертання антенної системи, з метою покращення тактико-технічних характеристик радіотехнічних станцій, на яких вона встановлена.

Отримано кінцеві наближені вирази, з яких зрозуміла фізика явища перевідбиття (розсіювання).

Ключові слова: *параболоїд обертання; дзеркальна антена; малогабаритний рупорний опромінювач.*

Постановка проблеми в загальному вигляді. Антена є одним із найважливіших елементів радіотехнічного пристрою, що випромінює та приймає електромагнітні хвилі. Від якості її роботи суттєво залежать його можливості в цілому: дальність радіозв'язку і радіолокації, пошукові й оглядові можливості радіолокаційних станцій (РЛС), розрізнювальна здатність, якість передачі сигналу, точність пеленга цілі, перешкодозахищеність тощо. Покращення таких характеристик є важливим завданням, що спонукає до дослідження наявних антенних систем та проєктування нових.

Значна частина сучасних РЛС оснащена дзеркальними антенами. Незважаючи на те, що вони досить добре досліджені, завдання їх удосконалення і на сьогодні є актуальним.

Під час аналізу антен, а особливо в ході розробки нових, зокрема й дзеркальних, виникає задача визначення (розрахунку) їх параметрів: опору випромінювання, вхідного опору, діаграми спрямованості тощо. На даний час такі обчислення проводять за допомогою сучасних програмних продуктів моделювання антен Вони ґрунтуються на загальних числових методах розв'язання рівнянь Максвелла без розкриття внутрішнього змісту. Оцінка похибки розрахунків за допомогою таких програм практично неможлива, а загальні алгоритми, побудовані на основі відомих обчислювальних методів, найчастіше можуть бути нестійкими [1].

Аналіз останніх досліджень і публікацій. Загалом задача суворого розрахунку параметрів будь-якої антени спочатку вирішується як внутрішня, а потім як зовнішня. Внутрішня задача полягає у визначенні електричних і магнітних струмів на деякій віртуальній поверхні – поверхні випромінювання. За знайденими струмами (зовнішня задача) на поверхні випромінювання знаходять електромагнітне поле в будь-якій точці простору [2–3].

На сьогодні розв'язок внутрішньої задачі за відомим розподіленням струмів для більшості випромінювачів не є проблемним. Майже всі труднощі, пов'язані з побудовою адекватних фізичних і математичних моделей випромінювальних систем, належать до внутрішньої задачі аналізу теорії антен.

Аналіз дзеркальної антени зводиться до розв'язання задачі дифракції її електромагнітної хвилі, збудженої випромінювачем на рефлекторі (дзеркалі). Як відомо, існує три основні методи розв'язання подібних задач: методи геометричної та фізичної оптики і метод інтегральних рівнянь [3].

Метод геометричної оптики, в основу якого покладено закон Снеліуса і принцип Ферма, застосовується лише для дзеркал великих геометричних розмірів [3]. Поле, відбите дзеркалом, у ближній зоні має усі шість компонент вектора, навіть якщо воно опромінене поляризованою хвилею. Проте метод геометричної оптики не враховує векторного характеру поля. Тому для його аналізу в ближній зоні застосування даного методу є неможливим. Його використання доцільне лише для дальньої зони, де хвиля є суто поперечною [3].

Метод фізичної оптики ґрунтується на визначенні електромагнітного поля випромінювання за відомим розподілом збуджувального поля на плоскій поверхні розкриву дзеркала (апертурі) відповідно до теореми еквівалентності. Вважають, що поверхнею випромінювання є тільки апертура, тому часто нехтують випромінюванням малих поверхневих струмів на тіньовій стороні дзеркала. Такий метод має багато недоліків, а головне – не враховує багаторазового розсіювання, тобто зворотного впливу рефлектора на опромінювач. Проте вважається, що він є більш точним за метод геометричної оптики [7].

Більшості з описаних вище недоліків позбавлений метод інтегральних рівнянь, який полягає у визначенні поля, розсіяного дзеркалом, за наведеними на ньому струмами. Функції їх розподілу на поверхні дзеркала визначають із розв'язку інтегрального рівняння, до якого зводиться крайова задача на поверхні параболоїда обертання. У науковій літературі методу інтегральних рівнянь приділяється дуже мало уваги, до того

ж він є значно складнішим, ніж методи фізичної та геометричної оптики [7]. У ході аналізу дзеркальних антен також виникають маловивчені гіперсингулярності [10, 11], які, крім того, є двовимірними, тому ще більш складними.

На даний час добре описані методи розв'язання інтегральних рівнянь із традиційними «слабкими» одновимірними сингулярностями: логарифмічними, Коші та Гільберта.

Зазвичай для розрахунку будь-якої антени (зокрема й дзеркальної) аналізують поле в її дальній зоні та, як правило, не звертають уваги на те, що традиційні методи не можуть застосовуватися для аналізу електромагнітного поля в ближній зоні антени [2, 12]. Більше того, відсутній граничний перехід електромагнітного поля до густини струму на поверхні антени. Це пояснюється тим, що поверхнева густина струму пов'язана з напруженістю магнітного поля співвідношенням, де вектор нормалі до поверхні, на якій знаходиться функція, як правило, визначають з інтегральних рівнянь першого роду, він містить у неявному вигляді особливості (сингулярності), коли точка джерела збігається з точкою спостереження.

У [14] запропоновано вдосконалений математичний апарат для дослідження електромагнітного поля, розсіяного антенною системою з рупорним опромінювачем пірамідальної форми. Удосконалення полягає в застосуванні нового методу визначення розсіяного електромагнітного поля, перевипроміненого рупорним опромінювачем, що розташований у фокусі параболоїда обертання антенної системи, за умов нормальної поляризації падаючої плоскої хвилі до площини її падіння та збігу їх поляризації [14–17].

Розрахунки за новим методом [14], що поєднує методи фізичної оптики та інтегральних рівнянь, дозволяють оцінювати вплив елементів, розміщених у площині фокуса, на розсіювання антенних систем у цілому. Проте для розробки дзеркальних антен, зокрема для покращення тактико-технічних характеристик об'єктів, на яких вони встановлені, необхідно мати вирази, нехай і наближені, з яких була б зрозуміла фізика явища перевідбиття (розсіювання).

Унаслідок математичної складності навіть найпростіших задач розсіювання та дифракції рідко вдається отримати в замкнутому вигляді розв'язки, зручні для безпосереднього розрахунку практично корисних фізичних характеристик. Тому доводиться допускати відомий ступінь наближення для формування граничних умов, розв'язання рівнянь або на обох етапах.

Важливою складовою теоретичних досліджень є виведення наближених формул, корисних в обмежених областях змінювання параметрів або змінних. Правильне розуміння їх фізичного сенсу, а також умов застосування становить важливий момент математичної теорії й експериментальної практики антен.

Наведений у [14] алгоритм розрахунку має недолік у тому, що може бути реалізований лише числовими методами, оскільки отримані інтеграли не є табличними та не підлягають приведенню до таких. Отже, виникає необхідність у спрощенні виразів, виведених у [14], для розсіяного рупором поля шляхом апроксимації й отримання простих формул, з яких було б зрозуміло фізичний процес явища перевідбиття.

У даній роботі обмежимося нормальною поляризацією падаючої хвилі до площини падіння як одним із випадків довільного падіння плоскої електромагнітної хвилі.

Формулювання завдання дослідження. Метою статті є визначення електромагнітного поля в області фокуса параболоїда обертання дзеркальної антени та на

осі дзеркала шляхом розв'язку інтегральних рівнянь числовим методом за нормальної поляризації падаючої хвилі.

Виклад основного матеріалу. Розглянемо випадок, коли електромагнітна хвилі, що падає, нормально поляризована до площини падіння (рис. 1). У такому разі електричну $\vec{E}_f^{\perp}$ і магнітну $\vec{H}_f^{\perp}$ складові вектора падіння хвилі можна записати в такий спосіб [13]:

$$\begin{cases} \vec{E}_f^{\perp} = \vec{e}_x E_0 e^{ikR^{\perp}}; \\ \vec{H}_f^{\perp} = -\left(\vec{e}_z \sin\theta_f + \vec{e}_y \cos\theta_f\right) e^{ikR^{\perp}} \dfrac{E_0}{Z_0}, \end{cases} \tag{1}$$

де E_0 – амплітуда електричної складової електромагнітної хвилі;

k – хвильове число;

θ_f – кут падіння плоскої електромагнітної хвилі;

$\vec{e}_x$, $\vec{e}_y$, $\vec{e}_z$ – одиничні вектори;

Z_0 – хвильовий імпеданс вільного простору;

$R^{\perp}$ – відстань від лінії фронту падаючої хвилі до поверхні дзеркала:

$$R^{\perp} = ftg\frac{\psi}{2}\left(tg\frac{\psi}{2} + 2tg\theta_f \sin\varphi\right)\cos\theta_f, \tag{2}$$

де ψ – кут, утворений між віссю z і відстанню R від фокуса до параболоїда;

φ – азимутальний кут, відрахований від осі x (рис. 1).

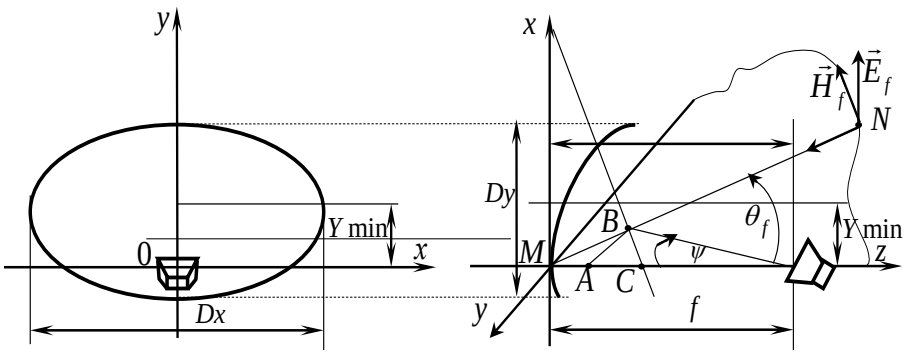


Рис. 1. Схема дзеркальної антени з несиметричним рефлектором. Випадок падіння плоскої електромагнітної хвилі, нормально поляризованої до площини падіння

Вектор щільності поверхневого струму на дзеркалі в наближенні фізичної оптики можна визначити за відомою формулою

$$\vec{j} = 2\left[\vec{n}, \vec{H}_f^{\perp}\right], \tag{3}$$

де $\vec{n}$ – одиничний орт до поверхні параболоїда обертання, що дорівнює

$$\vec{n} = \vec{e}_z \cos\frac{\psi}{2} - \vec{e}_x \sin\frac{\psi}{2}\cos\varphi - \vec{e}_y \sin\frac{\psi}{2}\sin\varphi. \tag{4}$$

Після підстановки (1), (4) у (3) отримаємо

$$j^{\perp} = 2\frac{E_0}{Z_0} e^{ikR^{\perp}} \left(\vec{e}_x \, a_x^{\perp} + \vec{e}_y \, a_y^{\perp} + \vec{e}_z \, a_z^{\perp} \right), \tag{5}$$

де

$$\begin{cases} a_x^{\perp} = \left(sin\frac{\psi}{2} sin\varphi \, sin\theta_f + cos\frac{\psi}{2} cos\,\theta_f \right); \\ a_y^{\perp} = -sin\frac{\psi}{2} cos\,\varphi \, sin\,\theta_f; \\ a_z^{\perp} = sin\frac{\psi}{2} cos\,\varphi \, sin\,\theta_f. \end{cases} \tag{6}$$

Електричну складову електромагнітного поля, що утворюється поверхневим струмом (3), можна розрахувати з виразу (5):

$$\vec{E}^{\perp} = \frac{1}{i\omega\varepsilon} \left[grad \; div\vec{A}^{\perp} + k^2 \vec{A}^{\perp} \right], \tag{7}$$

а магнітну складову – у такий спосіб:

$$\vec{H}^{\perp} = \frac{i}{\omega\mu} rot\vec{E}, \tag{8}$$

де електричний потенціал $\vec{A}^{\perp}$, утворений струмами, що течуть по поверхні дзеркала, визначають з такого виразу:

$$\vec{A}^{\perp} = \frac{1}{4\pi} \int\limits_{(S)} \vec{j}^{\perp} \frac{e^{-ikr}}{r} ds, \tag{9}$$

де ds – елемент поверхні зі струмами:

$$ds = \frac{2f^2 sin\frac{\psi}{2}}{cos^4\frac{\psi}{2}} d\psi d\varphi, \tag{10}$$

r – відстань від точки спостереження $N\left|x_2, y_2, z_2\right|$ до точки інтегрування $M\left|x_1, y_1, z_1\right|$, розташованої на поверхні дзеркала, що дорівнює

$$r = \sqrt{\left(x_2 - x_1\right)^2 + \left(y_2 - y_1\right)^2 + \left(z_2 - z_1\right)^2}. \tag{11}$$

Координати точки інтегрування подамо в такому вигляді:

$$\begin{cases} x_1 = 2ftg\frac{\psi}{2} cos\,\varphi; \\ y_1 = 2ftg\frac{\psi}{2} sin\,\varphi; \\ z_1 = ftg^2\frac{\psi}{2}. \end{cases} \tag{12}$$

Вираз під інтегралом (9) з урахуванням (10)–(12) набуде такого вигляду:

$$\int\limits_{(S)} \vec{j}^{\perp} \frac{e^{-ikr}}{r} ds = \frac{4E_0 f^2}{Z_0} \iint\limits_{(\varphi)(\psi)} \left(\vec{e}_x a_x^{\perp} + \vec{e}_y a_y^{\perp} + \vec{e}_z a_z^{\perp} \right) \frac{e^{-ikr}}{r} \frac{\sin\frac{\psi}{2}}{\cos^4\frac{\psi}{2}} d\psi \, d\varphi. \tag{13}$$

Для визначення електричної складової електромагнітного поля необхідно у вираз (7) підставити (9) з урахуванням (13).

Відомо, що за умови $r >> \lambda$ виконується співвідношення $k^2 \vec{A} >> grad\ div \vec{A}^{\perp}$. З його урахуванням можна приблизно записати

$$\vec{E}^{\perp} \cong -i \frac{2E_0 f^2}{\lambda} \int\limits_0^{2\pi} \int\limits_0^{\psi_0} \left(\vec{e}_x a_x^{\perp} + \vec{e}_y a_y^{\perp} + \vec{e}_z a_z^{\perp} \right) \frac{e^{ik\left(R^{\perp} - r\right)}}{r \cos\frac{\psi}{2}} tg\frac{\psi}{2} \left(1 + tg^2\frac{\psi}{2} \right) d\psi d\varphi, \tag{14}$$

де коефіцієнти $a_{x,y,z}^{\perp}$ визначають за виразом (6).

Для зручності використання (14) подамо координати точки спостереження x_2, y_2, z_2 через відстань від неї, а також кути θ_f і θ_m (рис. 2):

$$\begin{cases} x_2 = f - a\cos\theta_m; \\ y_2 = a\sin\theta_f \sin\theta_m; \\ z_2 = a\sin\theta_f \cos\theta_m. \end{cases} \tag{15}$$

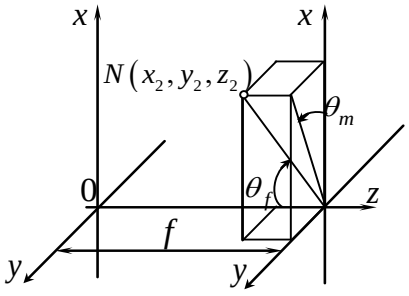


Рис. 2. Визначення координат точки спостереження

Після підстановки в (11) значень координат (12), (15) та незначних перетворень отримаємо

$$r = f\sqrt{\left(\frac{a}{f}\right)^2 + \left(1 + tg^2\frac{\psi}{2}\right)^2 + \frac{2a^2}{f}\left(tg^2\frac{\psi}{2}\cos\theta_f - \cos\theta_f - 2tg\frac{\psi}{2}\sin\theta_f \cos\left(\theta_f - \theta_m\right)\right)}. \tag{16}$$

З урахуванням того, що нас цікавить поле поблизу фокуса параболоїда обертання, де виконується умова $\frac{a}{f} << 1$, застосувавши до підкореневого виразу (16) формулу Маклорена

$$r = f\sqrt{\left(1+tg^2\frac{\psi}{2}+\frac{a}{f}cos^2\frac{\psi}{2}\left[tg^2\frac{\psi}{2}cos\,\theta_f - 2tg\frac{\psi}{2}sin\,\theta_f\,cos\left(\theta_f-\theta_m\right)-cos\,\theta_f\ldots\right]\right)} \qquad (17)$$

та обмеживши трьома членами в розкладанні (17), отримаємо

$$r = f\sqrt{\left(1+tg^2\frac{\psi}{2}-\frac{a}{f}\left(cos\,\theta_f\,cos\,\theta_m+sin\,\theta_f\,sin\,\theta_m\,cos\left(\theta_f-\theta_m\right)\right)\right)}. \qquad (18)$$

Враховуючи, що $\frac{a}{f}<<1$, і нехтуючи таким співвідношенням, у знаменнику виразу (14) після підстановки в нього формул (2), (4), (18) отримаємо

$$\vec{E}^{\perp} \approx -i\frac{2E_0 f}{\lambda}e^{-ikf}\int_0^{2\pi}\int_0^{\psi_0}\left\{\left(\vec{e}_x\left[sin\,\theta_f\,sin\,\varphi+\frac{cos\,\theta_f}{tg\frac{\psi}{2}}\right]-\vec{e}_y\,cos\,\varphi\,sin\,\theta_f+\vec{e}_z\,cos\,\varphi\,cos\,\theta_f\right)tg^2\frac{\psi}{2}\times\right.$$

$$\times exp\left[ik\left(\left(ftg^2\frac{\psi}{2}+2\,ftg\,\theta_f tg\frac{\psi}{2}sin\,\varphi\right)cos\,\theta_f - ftg^2\frac{\psi}{2}+\right.\right. \qquad (19)$$

$$\left.\left.\left.+a\left(cos\,\psi\,cos\,\theta+sin\,\theta\,sin\,\psi\left(cos\,\varphi\,cos\,\eta+sin\,\varphi\,sin\,\eta\right)\right)\right)\right]\right\}d\psi d\psi.$$

Для взяття інтеграла позначимо

$$W_1=\left(2ftg\frac{\psi}{2}sin\,\theta_f+2y_2\,sin\,\psi\right)k; \qquad W_2=kx_2\,sin\,\psi. \qquad (20)$$

З урахуванням позначень (20) вираз (19) подамо в такому вигляді:

$$\vec{E}^{\perp} \approx -i\frac{2E_0 f}{\lambda}e^{-ikf}\int_0^{\psi_0}\left\{\vec{e}_x\left(tg^2\frac{\psi}{2}sin\,\theta_f I_{1x\varphi}+tg\frac{\psi}{2}cos\,\theta_f I_{2x\varphi}\right)+\vec{e}_y tg^2\frac{\psi}{2}sin\,\theta_f I_{y\varphi}+\right.$$

$$\left.+\vec{e}_z tg^2\frac{\psi}{2}cos\,\theta_f I_{z\varphi}\right\}exp\left[ik\left(a\,cos\,\theta\,cos\,\psi+ftg^2\frac{\psi}{2}\left(cos\,\theta_f-1\right)\right)\right], \qquad (21)$$

де

$$\begin{cases} I_{1x\varphi}=\int_0^{2\pi}sin\,\varphi e^{i(W_1 sin\varphi+W_2 cos\varphi)}d\varphi; \\ I_{2x\varphi}=\int_0^{2\pi}e^{i(W_1 sin\varphi+W_2 cos\varphi)}d\varphi; \\ I_{y\varphi}=I_{y\varphi}=\int_0^{2\pi}cos\,\varphi e^{i(W_1 sin\varphi+W_2 cos\varphi)}d\varphi. \end{cases} \qquad (22)$$

Розглянемо інтеграли (22). Позначимо:

$$W_1 = A\sin\alpha; \qquad W_2 = A\cos\alpha; \qquad A = \sqrt{W_1^2 + W_2^2}\,. \tag{23}$$

Інтеграл $I_{1x\varphi}$ з (22) з урахуванням (23) набуде такого вигляду:

$$\begin{aligned} I_{1x\varphi} &= \int_0^{2\pi} \sin\varphi e^{iA\cos(\varphi-\alpha)} d\varphi = \\ &= \cos\alpha \int_0^{2\pi} \sin(\varphi-\alpha) e^{-iA\cos(\varphi-\alpha)} d\varphi + \sin\alpha \int_0^{2\pi} \cos(\varphi-\alpha) e^{iA\cos(\varphi-\alpha)} d\varphi. \end{aligned} \tag{24}$$

Позначимо $\gamma = \varphi - \alpha$, $d\gamma = d\varphi$, отримаємо

$$I_{1x\varphi} = \cos\alpha \int_{-\alpha}^{2\pi-\alpha} \sin\gamma e^{iA\cos\gamma} d\gamma + \sin\alpha \int_{-\alpha}^{2\pi-\alpha} \cos\gamma e^{iA\cos\gamma} d\gamma = \frac{i2\pi W_1}{\sqrt{W_1^2 + W_2^2}} I_1\left(\sqrt{W_1^2 + W_2^2}\right) = I_1 i\, 2\pi W_1 \cdot \tag{25}$$

Аналогічно отримаємо і для інших інтегралів (22):

$$\begin{cases} I_{2x\varphi} = 2\pi I_0\left(\sqrt{W_1^2 + W_2^2}\right); \\ I_{2y\varphi} = I_{z\varphi} = \dfrac{2\pi W_2}{\sqrt{W_1^2 + W_2^2}} I_1\left(\sqrt{W_1^2 + W_2^2}\right) = 2\pi W_2 I_1. \end{cases} \tag{26}$$

Поле в області фокуса з виразу (21) з урахуванням узятих інтегралів (25), (26) набуде такого вигляду:

$$\begin{aligned} \vec{E}^{\perp} \approx -i\frac{4\pi E_0 f}{\lambda} e^{-ikf} \int_0^{\psi_0} \Bigg\{ \vec{e}_x tg\frac{\psi}{2}\left(\cos\theta_f I_0\left(\sqrt{W_1^2 + W_2^2}\right)\right) + i\sin\theta_f I_1 W_1 tg\frac{\psi}{2} + \\ + \left(\vec{e}_y \sin\theta_f + \vec{e}_z \cos\theta_f\right) iW_2 tg^2\frac{\psi}{2} I_1 \Bigg\} exp\left[ik\left(a\cos\theta\cos\psi - 2f\sin^2\frac{\theta_f}{2} tg^2\frac{\psi}{2}\right)\right]. \end{aligned} \tag{27}$$

Для взяття інтеграла і з'ясування фізики процесу необхідно використати числові методи.

Розглянемо два окремі випадки за нормального падіння плоскої хвилі $\theta_f = 0$: поле в точці фокуса $a = 0$ і поле на осі дзеркала $\theta = 0$.

Поле в точці фокуса після взяття інтеграла (27) набуде вигляду

$$\vec{E}_F^{\perp} = E \approx \vec{e}_x i 8\pi E_0 \frac{f}{\lambda} e^{-ikf}\, ln\left|\cos\frac{\psi_0}{2}\right|. \tag{28}$$

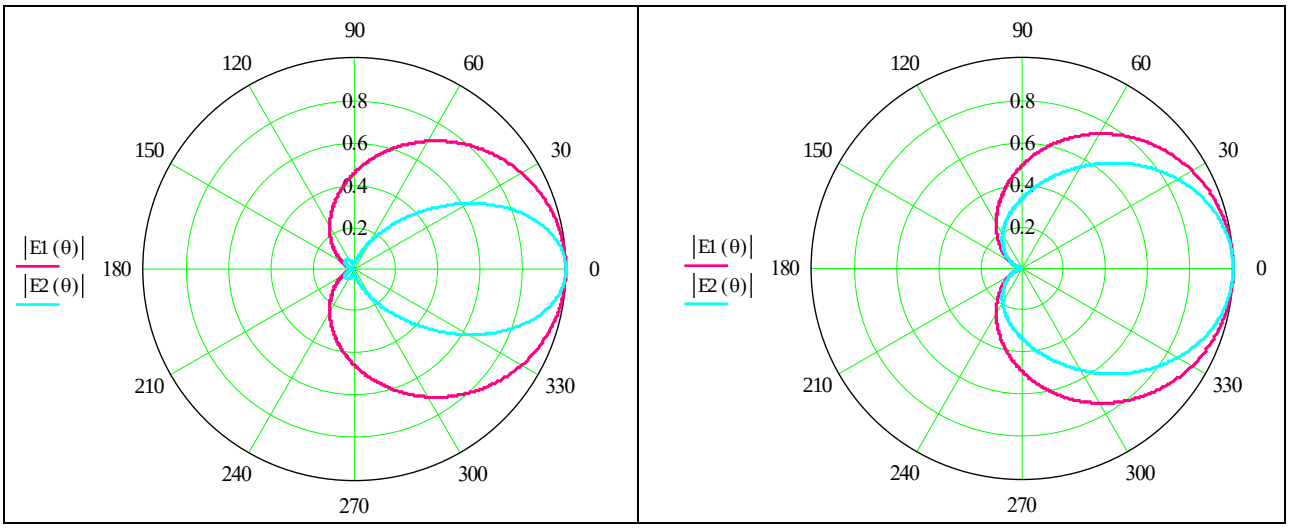
Працездатність (28) перевіримо на прикладі антенної системи РЛС 1РЛ133 «Кредо» [17] шляхом підстановки її параметрів у вираз для визначення поля, що випромінюється рупорним опромінювачем у площині H:

$$E_1^H(\theta) = \frac{1+\cos\theta}{2} \cdot \frac{\cos\left(\dfrac{a}{\lambda}\sin\theta\right)}{1 - \left(\dfrac{2a}{\lambda}\sin\theta \cdot \dfrac{1}{\pi}\right)^2}, \tag{29}$$

А також у площині E:

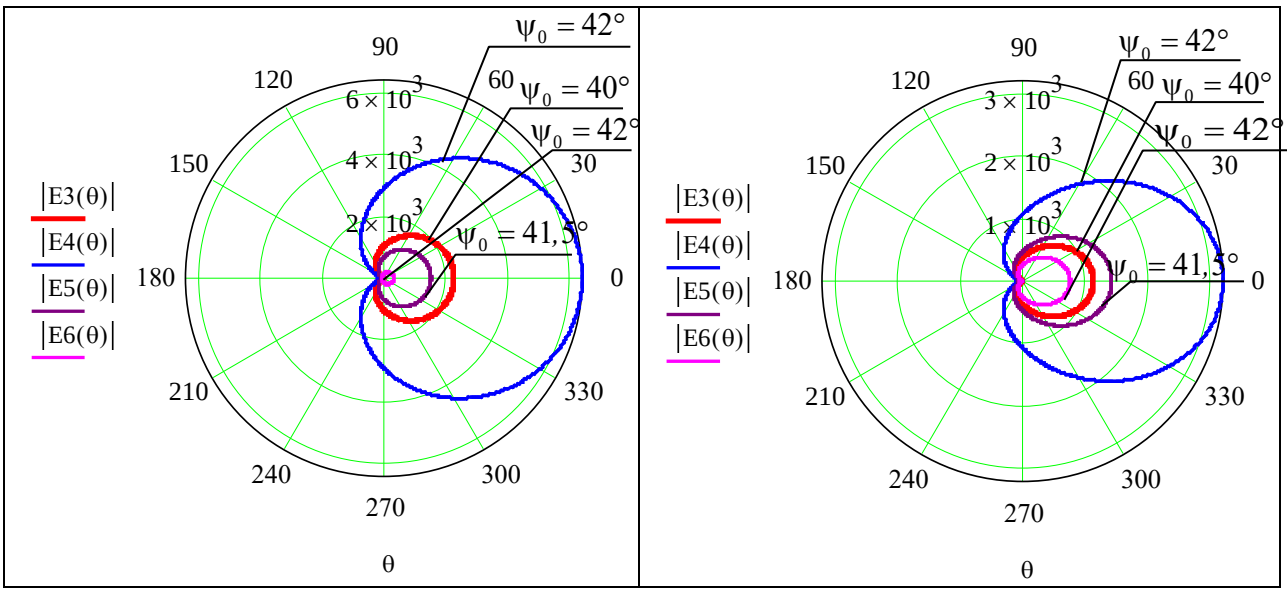
$$E_2^E(\theta)=\frac{1+\cos\theta}{2}\cdot\frac{\sin\left(\frac{b}{\lambda}\sin\theta\right)}{\frac{b}{\lambda}\sin\theta}. \qquad (30)$$

На рис. 3 наведено діаграми спрямованості, побудовані для рупорного опромінювача дзеркальної антени за параметрами РЛС 1РЛ133 «Кредо» в площині H за відомим наближеним виразом (29) – $\vec{E}_1(\theta)$ та в площині E (30) – $\vec{E}_2(\theta)$.



а) *б)*

Рис 3. Діаграма спрямованості рупорного опромінювача:
а) у площині H; б) у площині E



а) *б)*

Рис 4. Діаграма спрямованості антенної системи з урахуванням впливу рупорного опромінювача для кутів його нахилу ψ_0*:*

$E3(\theta)\ \psi_0=40°$*;* $E4(\theta)\ \psi_0=41°$*;* $E5(\theta)\ \psi_0=41{,}5°$ *та* $\psi_0=42°$ $E6(\theta)$

На рис. 4 наведено діаграми спрямованості електромагнітного поля за отриманим методом перевалу (28) для визначення поля в точці фокуса після взяття інтеграла (27), що випромінюється рупорним опромінювачем антенної системи РЛС 1РЛ133 «Кредо» [17] у площині H. Фокусна відстань $f = 0{,}27$ м. Кут нахилу опромінювача $\psi = 41°$.

З рис. 4 видно, що зміна кута нахилу опромінювача навіть на $0{,}5°$ зумовить зменшення електромагнітного поля майже втричі, що свідчить про суттєвий вплив будь-яких неоднорідностей, неточностей кріплення тощо на поле, що збуджується в області фокуса параболоїда обертання.

Отже, отриманий за числовим методом вираз для визначення електромагнітного поля в області фокуса параболоїда обертання дзеркальної антенної системи є хоча й наближеним, проте працездатним із досить прийнятною точністю. Похибки, що виникають, будуть розглянуті в подальших дослідженнях.

Поле на осі дзеркала за прямого падіння електромагнітної хвилі від рупорного опромінювача (21) з урахуванням узятих інтегралів (25), (26) після взяття інтеграла (27) набуде такого вигляду:

$$\vec{E}^{\perp}_{\substack{|\theta_f=0\\|\theta=0}} \approx \vec{e}_x i 8\pi E_0 \frac{f}{\lambda} e^{-ikf} \Big[I_0(ka) ln\left|cos\frac{\psi_0}{2}\right| - i_2 I_1(ka)\left(sin^2\left(\frac{\psi_0}{2}\right) + ln\left|cos\left(\frac{\psi_0}{2}\right)\right|\right) -$$

$$-2I_2(ka)\left(2\,sin^4\left(\frac{\psi_0}{2}\right) + ln\left|cos\left(\frac{\psi_0}{2}\right)\right|\right) + iI_3(ka)\left(-4\,sin^4\left(\frac{\psi_0}{2}\right) + \frac{16}{3} sin^6\left(\frac{\psi_0}{2}\right) + \right. \qquad (26)$$

$$\left. +2\left(sin^2\left(\frac{\psi_0}{2}\right) + ln\left|cos\left(\frac{\psi_0}{2}\right)\right|\right) - \ \ldots \ \Big].$$

Моделювання за виразом (26) буде проведено в подальших дослідженнях.

Висновки. У статті наведено спосіб визначення електромагнітного поля в області фокуса параболоїда обертання дзеркальної антени та на осі дзеркала шляхом розв’язання інтегральних рівнянь числовим методом за нормальної поляризації падаючої хвилі.

Запропонований порядок розрахунку має недолік у тому, що може бути реалізований лише числовими методами, оскільки отримані інтеграли не є табличними і не підлягають приведенню до таких. Цей недолік було усунуто шляхом визначення електромагнітного поля в області фокуса параболоїда обертання дзеркальної антени та на осі дзеркала розв’язком інтегральних рівнянь числовим методом. Працездатність отриманого розв’язку складного інтегрального рівняння доведено шляхом моделювання.

Розрахунки за новим методом дозволять оцінювати вплив різних елементів (неоднорідностей, неточностей кріплення тощо), розміщених у площині фокуса, на розсіяння антенних систем у цілому в разі будь-якого падіння хвилі на дзеркало.

Новизна отриманих результатів полягає в застосуванні нового числового методу визначення розсіяного електромагнітного поля, перевипроміненого рупорним опромінювачем, розташованим у фокусі параболоїда обертання антенної системи з метою покращення тактико-технічних характеристик радіотехнічних систем, на яких вони встановлені.

Розробка таких моделей і алгоритмів дозволить створювати принципово нові швидкодіючі системи автоматичного проєктування, що надасть можливість розраховувати

антени даного типу з точністю, яка значно перевищує максимально можливу в наявних системах проєктування [18–22]. Це сприятиме істотному зниженню матеріально-часових витрат на кінцеве доведення і налаштування розроблюваних антенних систем.

СПИСОК ЛІТЕРАТУРИ

1. Вуд П. Анализ и проектирование зеркальных антенн / Пер. с англ. под ред. О. П. Фролова. Москва : Радио и связь, 1984. 208 с.
2. Neganov V. A., Klyuev D. S., Sokolova J. V. A Method for Calculation of the Input Impedance of a Microstrip Electric Dipole // Radiophysics and Quantum Electronics. 2008. Vol. 51. № 12. P. 956–965.
3. Прохоров И. О., Кондратьева А. П. Зеркальная антенна с диаграммой направленности специальной формы // Антенны. 2009. Вып. 12 (151). С. 9–12.
4. Скулкин С. П., Турчин В. И. Импульсное поле офсетной параболической антенны в дальней зоне // Антенны. 2009. Вып. 6 (145). С. 3–7.
5. Будагян И. Ф., Щучкин Г. Г. Характеристики поля зеркальной антенны с корректирующим импедансом в ближней и дальней зонах при работе со сверхкороткими импульсами // Антенны. 2008. Вып. 4 (131). С. 20–26.
6. Кирьянов О. Е., Мартынов Н. А. Комбинированная итерационная методика расчета эффективной площади рассеяния зеркальных антенн // Антенны. 2009. Вып. 10 (149). С. 17–25.
7. Ильинский А. С., Кравцов В. В., Свешников А. Г. Математические модели электродинамики : учеб. пособ. для студентов вузов. Москва : Высшая школа, 1991. 224 с.
8. Галишникова Т. Н., Ильинский А. С. Численные методы в задачах дифракции. Москва : Изд-во МГУ, 1987. 208 с.
9. Лифанов И. К. Метод сингулярных интегральных уравнений и численный эксперимент. Москва : Янус, 1995. 520 с.
10. Вайникко Г. М., Лифанов И. К., Полтавский Л. Н. Численные методы в гиперсингулярных интегральных уравнениях и их приложения. Москва : Янус, 2001. 508 с.
11. Неганов В. А. Физическая регуляризация некорректных задач электродинамики. Москва : Сайнс-Пресс, 2008. 450 с.
12. Давыдов А. Г., Захаров Е. В., Пименов Ю. В. Метод численного решения задач дифракции электромагнитных волн на незамкнутых поверхностях произвольной формы // Доклады академии наук СССР. 1984. Т. 276. № 1. С. 96–100.
13. Лифанов И. К. Численные методы решения некоторых классов сингулярных интегральных уравнений и их приложение в аэродинамике : дис. док. физ.-мат. наук. Москва, 1981. 256 с.
14. Сидорчук О. Л. Метод визначення електромагнітного поля, розсіяного від рупорного опромінювача, розташованого у фокусі параболоїда обертання антенної системи станцій наземної розвідки // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць ЖВІ. Житомир : ЖВІ, 2019. Вип. 16. С. 80–93.
15. Сидорчук О. Л. Метод покращення поляризаційних характеристик антенних систем переносних станцій наземної розвідки // Проблеми створення, випробування, застосування

та експлуатації складних інформаційних систем : зб. наук. праць ЖВІ. Житомир : ЖВІ, 2018. Вип. 15. С. 78–93.
16. Сидорчук О. Л. Метод проектування радіолокаційних станцій наземної розвідки з антенною системою колової поляризації // Сучасні інформаційні технології у сфері безпеки і оборони. Київ : НУОУ, 2018. Вип. 3 (33) С. 25–35.
17. Methodology improvment of the electromagnetic field amplitude study related to the antenna system risk radio-solid station of land-development "Credo-M1" / O. Sidorchuk, O. Tofanchuk, O. Kritenko, Yu. Kalenchuk // Scientific works of Kharkiv National Air Force University. 2017. № 5 (54). С. 102–109.
18. Астахов В. Н. Дифракция на проводящем шаре в поле параболоида антенны // Изв. ЛЭТИ. Научн. труды. 1974. Вып. 155. С. 25–31.
19. Астахов В. Н., Степанов В. А. Определение ЭПР параболоида вращения с проводящим шаром в фокусе // Изв. ЛЭТИ. Научн. труды. 1975. Вып. 178. С. 28–37.
20. Астахов В. Н., Степанов В. А. Определение дифракционного поля в области фокуса параболоида вращения // Изв. ЛЭТИ. Научн. труды. 1979. Вып. 245. С. 25–30.
21. Залевский Г. С. Обзор методов расчета вторичного излучения радиолокационных объектов // Системи обробки інформації : зб. наук. праць. Харків : ХУПС, 2007. Вип. 7 (65). С. 16–24.
22. Сидорчук О. Л. Аналіз методів і способів зменшення ефективної поверхні розсіювання антенних систем // Вісник ЖДТУ. Технічні науки. Житомир, 2012. № 2 (61). С. 94–106.

Подано 30.12.2019

О. Л. Сидорчук, С. П. Фриз, В. И. Залевский, Л. М. Марищук

ЧИСЛЕННЫЙ МЕТОД ОПРЕДЕЛЕНИЯ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ В ОБЛАСТИ ФОКУСА ПАРАБОЛОИДА ВРАЩЕНИЯ ЗЕРКАЛЬНОЙ АНТЕННОЙ СИСТЕМЫ

В ходе анализа антенн и разработки их новых образцов, в том числе зеркальных, необходимо определить (рассчитать) их основные характеристики (параметры). Для этого нужно исследовать электромагнитное поле, которое возбуждается в области фокуса параболоида вращения, облучается рупорным облучателем.

В настоящее время такие расчеты проводятся с помощью современных программных продуктов моделирования. Они основываются на общих числовых методах решения уравнений Максвелла и подаются как готовый продукт без раскрытия внутреннего содержания. Поэтому оценка погрешности расчетов с помощью таких программ практически невозможна.

В результате математической сложности даже простейших задач рассеяния и дифракции редко удается получить в замкнутом виде решения, применимые для непосредственного расчета практически полезных физических характеристик. Таким образом, приходится допускать определенную степень приближения для формирования граничных условий, решения уравнений или на всех этапах.

Полученные ранее алгоритмы расчета имеют недостаток, поскольку могут быть реализованы только численными методами, так как полученные интегралы не являются табличными и не подлежат приведению к таковым. Именно поэтому возникает

необходимость в упрощении выражений для рассеянного рупором поля путем аппроксимации и получения простых формул.

В статье предложено определение электромагнитного поля в области фокуса параболоида вращения зеркальной антенны и на оси зеркала путем решения интегральных уравнений численным методом при поляризации падающей волны.

Новизна полученных результатов заключается в применении нового численного метода определения рассеянного электромагнитного поля, переизлучённого рупорным облучателем, расположенным в фокусе параболоида вращения антенной системы, с целью улучшения тактико-технических характеристик радиотехнических станций, на которых она установлена.

Получены конечные приближённые выражения, из которых понятна физика явления переотражения (рассеивания).

Ключевые слова: *параболоид вращения; зеркальная антенна; малогабаритный рупорный облучатель.*

O. L. Sidorchuk, S. P. Fryz, V. I. Zalevsky, L. M. Maryshchuk

NUMERICAL METHOD OF DETERMINATION OF THE ELECTROMAGNETIC FIELD, IN THE FIELD OF FOCUS OF THE PARABOLOID OF THE MIRROR OF THE MIRROR ANTENNA SYSTEM

When analyzing antennas, and especially when developing new ones, including mirrors, there is a problem of calculating their basic parameters. For this purpose it is necessary to study the electromagnetic field excited in the focus region of the paraboloid of rotation, which is irradiated by the horn irradiator.

At present, such calculations are made using modern computer simulation software. They are based on common numerical methods for solving Maxwell's equations and are presented as a finished product without disclosing internal content. So, estimating the error of calculations with the help of such programs is almost impossible.

Due to the mathematical complexity of even the simplest scattering and diffraction problems, it is rarely possible to obtain closed-form solutions that are convenient for the direct calculation of virtually useful physical characteristics. Thus it is necessary to allow a certain degree of approximation when forming boundary conditions, solving equations, or at all stages.

The previously obtained calculation algorithms have the disadvantage that they can be implemented only by numerical methods, since the integrals obtained are not tabular and cannot be reduced to such. There is a need to simplify the expressions for the field scattered by the horn by approximating and obtaining simple formulas.

The paper proposes to determine the electromagnetic field in the focus area of the paraboloid of the rotation of the mirror antenna and on the axis of the mirror by solving the integral equations by a numerical method with the normal polarization of the incident wave.

The novelty is the use of a new numerical method for determining the scattered electromagnetic field, irradiated by a horn irradiator, which is located in the focus of the antenna system's rotational paraboloid in order to improve the tactical and technical characteristics of the radio stations at which they are installed.

Finite expressions, albeit approximate ones, are obtained, from which the physics of the phenomenon of re-reflection is understood.

Keywords*: rotary paraboloid; mirror antenna; small-sized horn irradiator.*

УДК 629.7.01 DOI: 10.46972/2076-1546.2019.17.12

С. П. Фриз, В. А. Миклуха, Л. М. Марищук, Р. О. Авсієвич

МЕТОД ОПТИМІЗАЦІЇ МАРШРУТУ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА В ХОДІ ВИКОНАННЯ ЗАВДАНЬ НА ЗАДАНІЙ ВИСОТІ

Статтю присвячено актуальній тематиці, а саме оптимізації та вдосконаленню способів і методів планування маршруту безпілотного літального апарата.

Проаналізовано сучасний стан розвитку безпілотних літальних апаратів та завдання, які вони виконують. Визначено низку невирішених проблемних питань щодо побудови маршруту руху безпілотного літального апарата залежно від характеру поставлених завдань. Встановлено, які основні тактико-технічні характеристики безпілотного літального апарата та цільового навантаження впливають на планування маршруту.

Розглянуто підходи до побудови маршруту безпілотного літального апарата з використанням теорії графів, проаналізовано їх переваги та недоліки. Визначено можливості відомих способів оптимізації маршруту безпілотного літального апарата та обрано для подальшої реалізації один з проаналізованих алгоритмів пошуку найкоротшої траєкторії польоту. Проаналізовано методи багатокритерійної оптимізації, зокрема кластерного аналізу, та виділено ті, які підходять для заданих умов. Серед усіх алгоритмів кластеризації обрано актуальні для оптимізації польоту безпілотного літального апарата. Запропоновано вдосконалений метод, який поєднує кластеризацію (на основі алгоритмів FOREL-2, K-MEANS) і оптимізацію на графі (з використанням модифікованого алгоритму Літтла) та сприяє оптимізації маршруту безпілотного літального апарата за критерієм його найменшої протяжності.

Проведено практичний розрахунок за вдосконаленим методом для обраного безпілотного літального апарата та цільового навантаження і показано, як зміниться його маршрут порівняно з відомими методами.

Виділено основні отримані результати та напрямки подальших досліджень щодо оптимізації маршруту безпілотного літального апарата для виконання ним поставлених завдань.

Ключові слова: *безпілотний літальний апарат; маршрут; оптимізація; знімання; об'єкт знімання; кластеризація; алгоритм Літтла.*

Постановка проблеми в загальному вигляді. Розвиток сучасних технологій у галузі робототехніки значно розширив можливості безпілотних літальних апаратів (БпЛА). З появою БпЛА невеликих розмірів (І класу з вагою до 25 кг) спектр завдань, які вони здатні виконувати, значно розширився. На сьогодні їх використовують як у воєнних цілях, так і в цивільних. До основних завдань БпЛА І класу належать такі: ведення розвідки (оптична, хімічна, радіаційна тощо); моніторинг лісових масивів (в інтересах підрозділів Державної служби України з надзвичайних ситуацій); моніторинг прикордонної зони (в інтересах загонів Державної прикордонної служби України); спостереження за осередками масових заворушень (в інтересах Національної поліції) та багато інших.

Але стрімкий розвиток БпЛА І класу обумовлює низку проблемних питань щодо способів та методів їх застосування. Найпоширенішими з них є прокладання маршрутів і визначення почерговості проходження їх точок залежно від специфіки поставлених завдань та умов застосування БпЛА. Щодо завдання побудови маршруту, то можна зазначити, що на сьогодні відсутні чіткі алгоритми та способи побудови траєкторії руху БпЛА для того чи іншого цільового призначення. При цьому не враховують специфіки поставленого завдання: необхідної висоти польоту, наявного цільового навантаження та його характеристик, можливого зменшення протяжності маршруту, почерговості проходження точок маршруту тощо. Програмне забезпечення (Mission Planner, Intel Mission Control, Pix4D capture, UgCS та інше), яке використовують для прокладання маршрутів БпЛА й управління ними в польоті, не вирішують зазначених завдань. Тому питання щодо оптимізації маршруту БпЛА за рахунок зменшення його протяжності для тих чи інших завдань є актуальним.

Аналіз останніх досліджень і публікацій. Питаннями, пов'язаними з дослідженнями щодо вдосконалення та підвищення ефективності застосування БпЛА для виконання завдань спостереження й розвідки заданих районів, займалися такі вітчизняні вчені: О. В. Харченко, С. П. Мосов, В. Б. Толубко, І. В. Матала, В. В. Руснак, С. А. Станкевич тощо.

Плануванню та застосуванню БпЛА в різних умовах для виконання різноманітних цільових завдань також присвячено багато наукових робіт. У [1, 6] розглянуто питання, які стосуються побудови їх маршрутів руху за будь-яких обставин. Робота [2] присвячена саме плануванню застосування БпЛА, у ній проаналізовано основні програмні засоби планування маршрутів, алгоритми та способи планування застосування БпЛА для різних специфічних завдань. В [11, 12] розкрито загальні питання та основні підходи до застосування БпЛА І класу для різних завдань. Але досі не приділено достатньої уваги поетапній побудові маршруту руху БпЛА, правильності вибору почерговості проходження заданих об'єктів, не розглянуто питання оптимізації прокладеного маршруту з метою зменшення його протяжності.

Слід зазначити, що оптимізація побудови маршрутів на етапі їх планування є актуальним науковим завданням. Про це свідчать численні роботи (українські та закордонні публікації), присвячені саме цій проблематиці. У [4, 5, 14] розглянуто питання побудови та оптимізації маршрутів з використанням методів оптимізації на графах (розв'язання класичної задачі комівояжера). У роботах [9, 14] запропоновано оптимізацію на графах з використанням алгоритму Літтла, який виділено як один із точних розв'язків задачі комівояжера. Але в цих роботах не враховано специфіки застосування та можливостей оптимізації маршруту безпосередньо для БпЛА. У публікаціях [3, 7] розглянуто питання щодо можливостей кластеризації об'єктів з подібними ознаками. Проаналізовано основні підходи до їх вирішення, виділено переваги та недоліки різних алгоритмів кластеризації, проте не враховано характеристик польоту БпЛА, а саме висоти польоту та її впливу на формування вибірок і подальшу кластеризацію загального маршруту.

Метою статті є розробка методу оптимізації маршруту БпЛА за критерієм найменшої протяжності, який буде враховувати параметри виконання поставлених завдань.

Формулювання завдання дослідження. Нехай є заданий район знімання з певною кількістю об'єктів n, які необхідно зняти. Їх можна подати у вигляді матриці відстаней $\left[s_{ij}\right]$, де s_{ij} – відстань між об'єктами i та j. Відомі тип БпЛА та характеристики

цільового навантаження (кут поля зору камери φ). БпЛА здійснює політ на фіксованій висоті $H_з = const$.

Необхідно прокласти такий оптимальний маршрут руху БпЛА, щоб забезпечити дослідження всіх заданих об'єктів за найменшої його протяжності L:

$$L = \sum_{i=1}^{n} \sum_{j=1}^{n} s_{ij} \to min. \quad (1)$$

Виклад основного матеріалу. З розширенням кола завдань, які здатні виконувати БпЛА (моніторинг місцевості, екологічна й технічна розвідка тощо), виникає низка невирішених питань [11, 12], які потребують доопрацювання та вдосконалення. Одним із них є прокладання маршруту руху БпЛА після отримання завдання [6].

За великої кількості об'єктів дослідження (більше 40) є висока ймовірність того, що в ході знімання з БпЛА в кадр буде потрапляти декілька об'єктів одночасно. Тому ми пропонуємо використати для оптимізації маршруту руху БпЛА кластеризацію об'єктів за шириною поля зору (рис. 1) БпЛА на визначеній висоті.

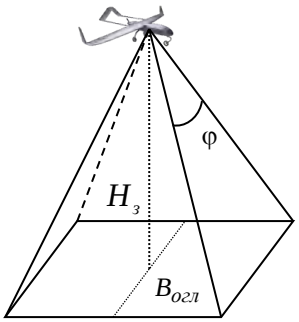


Рис. 1. Знімання з БпЛА

Ширину поля зору БпЛА $B_{огл}$ знаходимо за такою формулою:

$$B_{огл} = 2 \cdot H_з \cdot tg\left(\varphi / 2\right), \quad (2)$$

де $H_з$ – висота проведення знімання.

Для подальших розрахунків за допомогою програмного забезпечення, розробленого в рамках наукових досліджень [13, 14], змоделюємо польотне завдання (рис. 2).

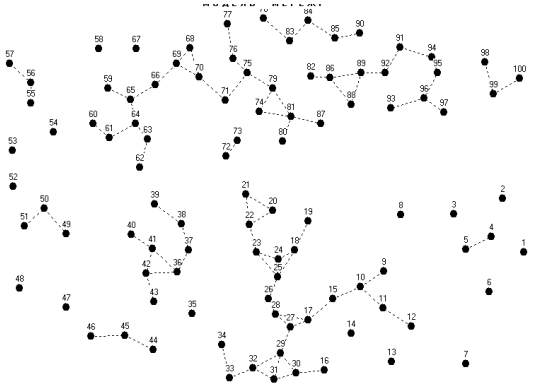


Рис. 2. Розміщення об'єктів, які необхідно дослідити

Далі запропонуємо метод кластеризації об'єктів дослідження за шириною зони огляду БпЛА на визначеній висоті.

Проведений аналіз [3, 7] показав, що серед розглянутих підходів до кластеризації об'єктів за подібними ознаками, а саме алгоритмів: STOLP, Fris-STOLP, NNDE, LVQ, FOREL, FOREL-2, K-MEANS – для вирішення поставленого завдання доцільно використати FOREL-2 та K-MEANS. Для даних алгоритмів кластеризації характерні певні недоліки: FOREL-2 має високу залежність від обрання першого об'єкта дослідження та може мати декілька рішень [7]; K-MEANS надає кращий результат за відомої кількості необхідних кластерів. Та дослідження [7] показали, що в разі поєднання даних алгоритмів зазначені вище недоліки зникають.

Тому для подальшої роботи пропонуємо провести кластеризацію об'єктів за шириною зони огляду БпЛА за допомогою модифікованого алгоритму кластеризації, який передбачає такі етапи:

на першому кроці обираємо множину об'єктів $\Im := Y$, з усієї вибірки виокремлюємо першу точку $y_0 \in \Im$;

на наступному кроці визначаємо кластер N з радіусом $\Re$ та центром у точці y_0:

$$\mathrm{N} := \left\{ y \in \Im \middle| \partial\left(y, y_0\right) \le \Re \right\}, \tag{3}$$

$$\partial\left(y, y_0\right) = \left(y - y_0\right)^2; \tag{4}$$

на третьому кроці обрана точка переміщається в центр мас кластера:

$$y_0' := \frac{1}{|\aleph|} \sum_{y \in \aleph} y; \tag{5}$$

четвертий крок: якщо $y_0 \neq y_0'$, то $y_0 := y_0'$ та повертаємося до другого кроку;

на п'ятому кроці позначаємо всі точки $\aleph$ як опрацьовані, а точку y_0 – як центр кластера;

шостий крок: якщо є неопрацьовані точки, то повторюємо кроки 2–5 доти, доки всі задані точки не будуть опрацьовані.

У результаті застосування алгоритму кластеризації за шириною зони огляду БпЛА на заданій висоті отримаємо новий план розміщення об'єктів (рис. 3).

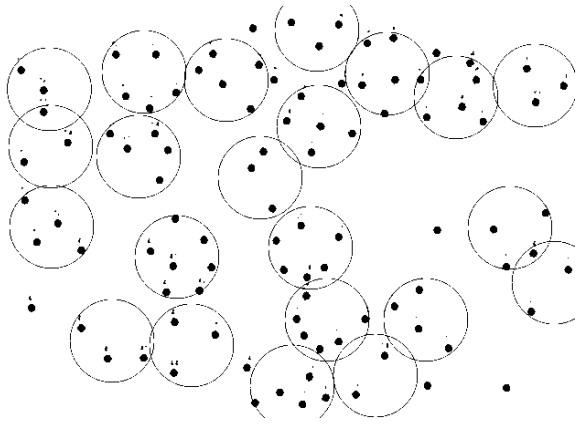


Рис. 3. Визначення кластерів за зоною огляду

Новими точками розрахунку маршруту будуть центри мас кластерів, визначених за запропонованим алгоритмом (рис. 4).

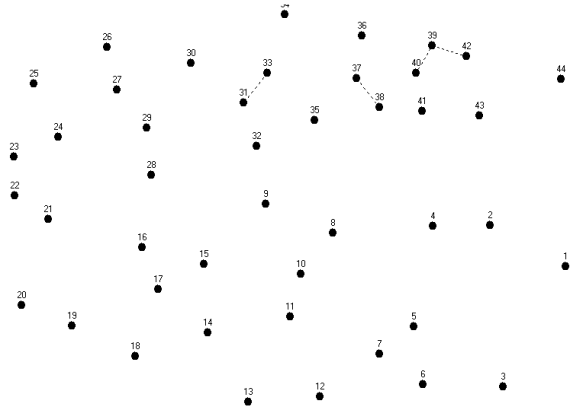


Рис. 4. Розміщення кластеризованих об'єктів

Надалі потрібно з'ясувати, яким же чином побудувати маршрут руху для БпЛА та в якій послідовності облітати об'єкти. Для вирішення даних питань застосуємо математичний апарат для розв'язання задачі комівояжера.

На сьогодні існує багато підходів до розв'язання задач даного типу [4, 5, 14]: метод найближчого сусіда, метод меж і гілок, алгоритм мурашиних колоній, метод поступок, алгоритм Літтла тощо. Дослідження основних підходів [6, 9, 13] та інтерпретація їх під умови поставленої задачі показали, що доцільно застосувати модифікований алгоритм Літтла. Як показали дослідження [13, 14], саме він у разі значного збільшення кількості точок маршруту (більше 50) надає найкращий наближений розв'язок задачі комівояжера. Ще однією перевагою даного алгоритму є швидкість обчислення. Отже, для проведення подальшої оптимізації маршруту БпЛА було обрано саме модифікований алгоритм Літтла. Розглянемо його сутність.

Маршрут БпЛА за визначеними об'єктами (точками маршруту) дослідження можна подати у вигляді зв'язного зваженого графа $G=(V,U)$ з множиною вершин V, $|V|=m$, та множиною ребер U, $\left[s_{ij}\right]$ – матриця відстаней (ваг ребер), де $s_{ij}\in R_0^+$, R_0^+ – множина дійсних невід'ємних чисел [13].

На першому кроці з матриці відстаней $\left[s_{ij}\right]$ формується зведена матриця $\left[s_{ij}\right]'$ шляхом зменшення кожного елемента рядка i матриці та елемента стовпця j матриці на найменший елемент рядка та стовпця h_i і H_j відповідно. У такий спосіб отримуємо зведену матрицю $\left[s_{ij}\right]'$, у кожному рядку та стовпці якої буде хоча б один нульовий елемент.

Наступним кроком проводимо оцінювання $\xi(Z)$ для множини Z можливих варіантів маршрутів БпЛА (кількість таких маршрутів буде $n!$). Оцінку визначаємо за формулою (6), яка включає в себе суми звідних констант h_i і H_j. Отже, жоден із можливих варіантів маршрутів не може мати оцінку, меншу за $\xi(Z)$:

$$\xi(Z) = \sum_i h_i + \sum_j H_j . \tag{6}$$

На третьому кроці множина Z розділяється на підмножину Z_1, яка включає в себе деяку пару вершин (r,t), та підмножину Z_2, що не включає пари (r,t).

Після цього визначаємо мінімальний елемент рядка та стовпця. Потім для кожного нульового елемента оцінюємо «штраф» за його невикористання за такою формулою [9]:

$$C_{pq} = \delta_p + \lambda_q . \tag{7}$$

За пару об'єктів обираємо ту, що має найбільше значення «штрафу» за невикористання в загальному маршруті $C_{sl} = \max\limits_{p,q}\{C_{pq}\}$.

Четвертий крок передбачає оцінювання підмножин Z_1 та Z_2. Оцінка підмножини Z_2 дорівнюватиме сумі оцінок множини Z та «штрафу» за невикористання (r,t). Для оцінювання підмножини Z_1 необхідно з матриці $\left[s_{ij}\right]$ виключити рядок r та стовпець t. Після чого потрібно замінити елементи (r,t) на знак (∞). Потім для отриманої матриці провести зведення та розрахувати оцінку підмножини Z_1, яка дорівнюватиме сумі оцінки множини Z та сумі звідних констант отриманої зведеної матриці:

$$\xi(Z_1) = \xi(Z) + \sum_i h_i' + \sum_j H_j' . \tag{8}$$

Для подальшої роботи обираємо ту з підмножин, яка має меншу оцінку. Після цього повертаємося до кроку 3.

Цикл повторюємо доти, доки зведена матриця не буде містити елементи, відмінні від (0) та (∞). У такий спосіб у підсумку отримуємо маршрут, який за протяжністю буде найкоротшим із можливих.

Отже, практично з моделюванням графів програмними засобами отримуємо результат з усіх об'єктів, які необхідно дослідити, та маємо траєкторію для руху БпЛА, найменшу за критерієм її протяжності.

Загальну протяжність такого маршруту визначаємо за виразом

$$L = \sum_{w=1}^{m}\sum_{u=1}^{m} z_{wu}, \tag{9}$$

де m – кількість отриманих кластерів та їх центрів мас відповідно;

z_{wu} – відстань між центрами мас отриманих кластерів.

Практична реалізація отриманих результатів проведена на прикладі розрахунку та оптимізації маршруту для БпЛА «PD-1» на висоті польоту $H_з = 1000$ м та для $n = 100$ об'єктів дослідження на певній площині. Початковий маршрут, визначений за допомогою відомих підходів до планування маршруту БпЛА [1, 6], наведено на рис. 5.

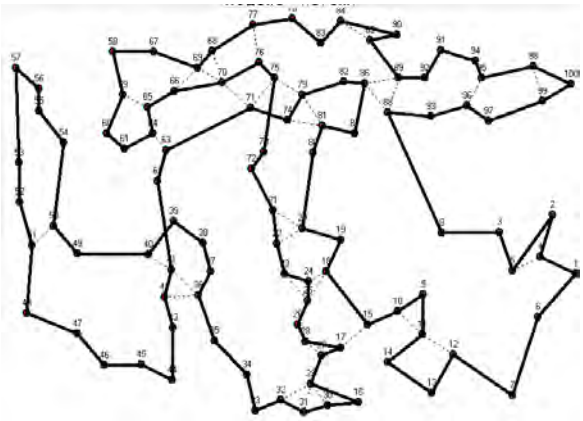


Рис. 5. Початковий маршрут для БпЛА «PD-1»

Після проведення кластеризації об’єктів (точок маршруту) запропонованим алгоритмом та оптимізації маршруту руху за допомогою пошуку найкоротшого варіанта з усіх можливих (оптимізація на графах із використанням вдосконаленого алгоритму Літтла) отримано маршрут, наведений на рис. 6.

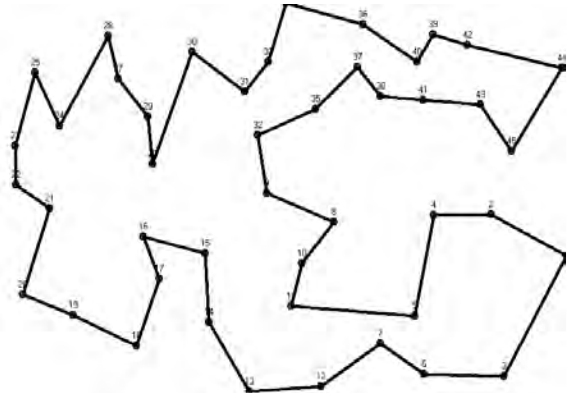


Рис. 6. Маршрут для БпЛА «PD-1», отриманий запропонованим методом

Отже, після опрацювання отриманих результатів маємо: зменшення кількості об’єктів на маршруті (точок маршруту) з $n_1 = 100$ до $n_2 = 44$, що становить 56%; скорочення загальної протяжності початкового маршруту на 42%, що зумовлює зменшення затрат ресурсів на політ (економічність польоту) та його тривалості (збільшення ймовірності успішного виконання поставлених завдань та зниження ймовірності поломки БпЛА в польоті). Крім того, головним досягнутим результатом є зменшення часу отримання необхідної інформації про стан досліджуваних об’єктів, що значно підвищить оперативність виконання поставлених завдань.

Висновки. У статті запропоновано новий підхід до оптимізації траєкторії польоту БпЛА в ході виконання завдань із дослідження певної кількості точкових об’єктів на заданій висоті. У результаті оптимізації були поєднані два підходи, а саме кластеризація маршруту за шириною зони огляду БпЛА на заданій висоті та модифікований алгоритм Літтла, для пошуку найкоротшого маршруту з усіх можливих комбінацій. Практична оцінка отриманих результатів показала доцільність та актуальність проведення досліджень, адже результатом стало зменшення протяжності вихідного маршруту БпЛА на 42%.

Перспектива подальших досліджень полягає в програмній реалізації запропонованого способу з урахуванням специфіки поставленого завдання. Надалі пропонуємо вдосконалювати отриманий результат, зважаючи на:

1) пріоритетність об'єктів (з урахуванням поставленого завдання та забезпечення необхідної оперативності отримання інформації);

2) можливості БпЛА щодо виконання польоту за прокладеним маршрутом (порівняння загальної протяжності отриманого маршруту та тактико-технічних характеристик наявних БпЛА);

3) врахування заборонених зон (небажаних, ймовірного ураження чи високої ймовірності поломки БпЛА).

СПИСОК ЛІТЕРАТУРИ

1. Dolinskaya I., Maggiar A. Time-optimal trajectories with bounded curvature in anisotropic medium // The International Journal of Robotics Research. 2012. Vol. 12-02. P. 1–48.
2. Walker A. Hard Real-Time Motion Planning for Autonomous Vehicles // PhD thesis, Swinburne University. 2011. P. 8–28.
3. Isaacs J. T., Hespanha J. P. Dubins Traveling Salesman Problem with Neighborhoods: A Graph-Based Approach // Algorithms. 2013. Vol. 6. P. 84–99.
4. Миклуха В. А., Хімчик Н. О. Оптимізація траєкторії польоту безпілотного літального апарата // Traektoria Nauki. 2017. Vol. 3, No. 9. P. 1009–1015. DOI: 10.22178/pos.26-5.
5. Puleko I., Myklukha V., Khimchyk N. Optimization trajectory of flight pilotless unmanned aerial vehicle is with the use theory of the graphs // Innovative solutions in modern science. 2017. № 10 (19). P. 5–13.
6. Kamil A. Alotaibi. Unmanned Aerial Vehicle Routing In The Presence Of Threats. Arlington : The University Of Texas At Arlington. 2014. P. 12–42.
7. Гуляницький Л. Ф., Мулеса О. Ю. Прикладні методи комбінаторної оптимізації. Київ : Видавничо-поліграфічний центр «Київський університет», 2016. 142 с.
8. The Strategic Research Agenda for Robotics in Europe // Robotic Visions to 2020 and beyond. European Robotics Technology Platform. 07/2009 (second edition). URL: http://www.robotics-platform.eu/cms/upload/SRA/2010-06_SRA_A3_low.pdf (last accessed: 12.12.2019).
9. Модификация метода Литтла для решения кольцевой задачи о сельском почтальоне / А. В. Морозов, А. В. Панишев, В. А. Скачков // Штучний інтелект. 2010. № 3. С. 103–115.
10. Харченко О. В., Кулєшин В. В., Коцуренко Ю. В. Класифікація та тенденції створення безпілотних літальних апаратів військового призначення // Наука і оборона. 2005. № 1. С. 47–54.
11. Guillaume Ducard. Fault-tolerant Flight Control and Guidance Systems: Practical Methods for Small Unmanned Aerial Vehicles. Publisher : Springer, 2009. P. 37–58. ISBN 1848825609.
12. Randal W. Beard, Timothy W. McLain. Small Unmanned Aircraft: Theory and Practice. Princeton University Press, 2012. P. 42–74. ISBN: 0691149216.
13. Левченко А. Ю., Морозов А. В., Панышев А. В. Быстрый алгоритм решения задачи о назначениях для нахождения нижней границы стоимости маршрута коммивояжера // Штучний інтелект. 2011. С. 406–416.
14. Левченко А. Ю., Морозов А. В., Панышев А. В. Механизм ускорения вычислений в методе Литтла для решения задач класса коммивояжера // Штучний інтелект. 2012. № 2. С. 95–110.

Подано 30.12.2019

С. П. Фриз, В. А. Миклуха, Л. М. Маришук, Р. А. Авсиевич

МЕТОД ОПТИМИЗАЦИИ МАРШРУТА БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА ПРИ ВЫПОЛНЕНИИ ЗАДАНИЙ НА ЗАДАННОЙ ВЫСОТЕ

Статья посвящена актуальной тематике, а именно оптимизации и усовершенствованию способов и методов планирования маршрута беспилотного летательного аппарата.

Проведён анализ современного состояния развития беспилотных летательных аппаратов и задач, которые на них возлагаются. Определен ряд проблемных вопросов по построению маршрута движения беспилотного летательного аппарата в зависимости от характера поставленных заданий. Установлено, какие основные тактико-технические характеристики беспилотного летательного аппарата и целевой нагрузки влияют на планирование маршрута.

Рассмотрены подходы к построению маршрута беспилотного летательного аппарата с использованием теории графов, проанализированы их преимущества и недостатки. Определены возможности известных способов оптимизации маршрута беспилотного летательного аппарата и выбран для дальнейшей реализации один из проанализированных алгоритмов поиска кратчайшей траектории полёта. Проанализированы методы многокритериальной оптимизации, а именно кластерного анализа, и выделены те, которые подходят для заданных условий. Среди всех алгоритмов кластеризации избраны актуальные для оптимизации полета беспилотного летательного аппарата. Предложен усовершенствованный метод, который сочетает кластеризацию (на основе алгоритмов FOREL-2, K-MEANS) и оптимизацию на графе (с использованием модифицированного алгоритма Литтла), а также способствует оптимизации маршрута беспилотного летательного аппарата по критерию его наименьшей протяженности.

Проведен практический расчет по усовершенствованному методу для выбранного беспилотного летательного аппарата и целевой нагрузки, показано, как изменится его маршрут по сравнению с известными методами.

Выделены основные полученные результаты и направления дальнейших исследований по оптимизации маршрута беспилотного летательного аппарата для решения поставленных заданий.

Ключевые слова: *беспилотный летательный аппарат, маршрут, оптимизация, съемка, объект съемки, кластеризация, алгоритм Литтла.*

S. P. Friz, V. A. Miklykha, L. M. Marishchyk, R. O. Avsievych

METHOD OF OPTIMIZATION THE ROUTE UNMANNED AERIAL VEHICLE DURING THE TASK AT THE HEIGHT

The article is devoted to the actual theme of the present, namely, optimization and improvement of methods and techniques of planning the route of an unmanned aerial vehicle.

In article the analysis of a modern condition of development of unmanned aerial vehicles and a circle of tasks which are assigned to them is spent. A number of unresolved tasks are

defined, to the construction of the unmanned aerial vehicle route depending on the nature of the tasks. It is analyzed, what main tactical and technical characteristics of the unmanned aerial vehicle and target load influence on the route planning.

The approaches to constructing the unmanned aerial vehicle route using graph theory were reviewed and their advantages and disadvantages were analyzed. The capabilities of known approaches to optimize the unmanned aerial vehicle route have been determined and one of the analyzed algorithms for finding the shortest route has been selected for further implementation. Multi-criteria optimization methods, namely cluster analysis, have been analyzed and those that are suitable for the given conditions have been highlighted. Among all clustering algorithms selected and proposed in the future work relevant to the optimization of unmanned aerial vehicle flight. Proposed an improved method that combines clustering (using the algorithm Forel-2 and K-MEANS) and optimization on the graph (using a modified algorithm Little`s), which optimizes the unmanned aerial vehicle flight route by the criterion of its minimum length.

A practical calculation of the improved method for the selected unmanned aerial vehicle and its target load has been performed and shows how the unmanned aerial vehicle route will change compared to the known methods.

The main results obtained and directions for further research on the optimization of the unmanned aerial vehicle route to solve the task

Keywords: *unmanned aerial vehicle, route, optimization, shooting, object of shooting, clustering, Little`s algorithm.*

ISSN 2076-1546

УДК 681.518 DOI: 10.46972/2076-1546.2019.17.13

В. В. Воротніков, І. В. Зімчук, Р. В. Нетребко

АЛГОРИТМ ЦИФРОВОГО УПРАВЛІННЯ ЕЛЕКТРОПРИВОДОМ АНТЕНИ НАЗЕМНОГО ПУНКТУ КЕРУВАННЯ БЕЗПІЛОТНОГО АВІАЦІЙНОГО КОМПЛЕКСУ

З кожним роком безпілотні авіаційні комплекси знаходять усе більше застосовують як у цивільній, так і військовій сфері. Стійкий зв'язок з безпілотним літальним апаратом забезпечується високоточним наведенням антени наземного пункту керування. У режимі автоматичного супроводження безпілотного літального апарата наведення антени здійснюється системою автоматичного супроводження за напрямком. Показано, що основною вимогою, яка висувається до системи автосупроводження за напрямком, є висока динамічна точність в умовах збурень та шумів різного характеру. Традиційна система автосупроводження за напрямком не спроможна забезпечити високу точність наведення антени. Покращити якість слідкувальної системи як у перехідному, так і сталому режимах роботи запропоновано за рахунок доповнення наявної аналогової системи підсистемою цифрової корекції. Роботу присвячено синтезу алгоритму цифрового управління електроприводом антени наземної приймально-передавальної станції безпілотного авіаційного комплексу. Алгоритм цифрового управління синтезовано як результат розв'язання різницевих рівнянь, що визначаються за дискретною передавальною функцією цифрового регулятора. На практиці перевага надається простим регуляторам, розмірність яких менша за розмірність об'єкта. Спрощення структури регулятора досягнуто використанням у процесі синтезу редукованої моделі системи управління антеною. Редукцію реалізовано методом, який ґрунтується на близькості перехідних характеристик математичних моделей початкового та редукованого об'єктів управління, охоплених одиничним негативним зворотним зв'язком. Для оцінювання ступеня близькості застосовано непрямі показники якості перехідного процесу. Безпосередній синтез регулятора виконано методом на основі теорії інваріантності, він передбачає компенсацію нулів та полюсів передавальної функції об'єкта управління. Відмінною рисою використаного методу є можливість урахування вимог до стійкості та заданої динамічної точності системи управління на етапі синтезу цифрового регулятора. Наведено результати моделювання, які підтверджують працездатність та ефективність синтезованого алгоритму управління.

Ключові слова: *безпілотний літальний апарат; система автосупроводження за напрямком; цифровий регулятор; алгоритм цифрового управління.*

Постановка проблеми в загальному вигляді. Останнє десятиріччя характеризується інтенсивним зростанням розробок у галузі безпілотної авіації. Безпілотні авіаційні комплекси (БпАК) знаходять широке застосування як у цивільній, так і військовій сфері [1, 2]. Незалежно від цього головними компонентами БпАК є безпілотний літальний апарат (БпЛА) та наземний пункт керування. Найважливішою характеристикою, яка визначає експлуатаційні можливості комплексу керування БпЛА, є спроможність забезпечення стійкого зв'язку.

Для забезпечення зв'язку на великі відстані та підвищення завадостійкості за рахунок просторової селекції в наземних пунктах керування широко використовують гостроспрямовані антенні системи [3]. Наведення головного максимуму діаграми спрямованості антени в задану точку простору та переміщення антени відповідно до реального руху БпЛА виконує система автосупроводження за напрямком (АСН). Більшість наявних систем АСН побудовані за принципом управління за відхиленням із використанням амплітудного пеленгатора як вимірювача кутового розузгодження та електропривода антени у складі: підсилювача потужності, виконавчого двигуна з редуктором [4, 5]. Однією з основних вимог до систем АСН є висока динамічна точність наведення антени в умовах збурень та шумів різного характеру. Оскільки основним режимом роботи системи АСН є стеження за кутовими координатами, які повільно змінюються, а аналоговому електроприводу властивий перший порядок астатизму, то традиційна система АСН не спроможна забезпечити високу точність наведення антени [5]. Покращити якість слідкувальної системи як у перехідному, так і сталому режимах роботи можливо за рахунок доповнення діючої аналогової системи підсистемою цифрової корекції.

Аналіз останніх досліджень і публікацій. Питання, пов'язані із синтезом алгоритмів цифрового управління, знайшли широке відображення у вітчизняній та зарубіжній літературі [4, 6–9], де достатньо глибоко викладено принципи побудови цифрових регуляторів за різними класифікаційними ознаками. Один з відомих методів [10], що ґрунтується на теорії інваріантності, передбачає синтез досить простих алгоритмів цифрового управління, стійкість та динамічну точність яких визначають на етапі синтезу. Однак спроектовані за зазначеним методом регулятори належать до класу компенсаційних, що не дозволяє використовувати їх для управління об'єктами високого порядку [7, 8]. Проте використання в процесі синтезу редукованої моделі об'єкта управління розширює можливості даного методу [10].

Формулювання завдання дослідження. Враховуючи викладене вище, метою даної роботи є підвищення точності наведення антени наземного пункту управління БпЛА за рахунок застосування у складі системи АСН алгоритму цифрового управління, який синтезовано компенсаційним методом із використанням редукованої моделі об'єкта управління.

Постановка завдання. Задача синтезу алгоритму цифрового управління ставиться для таких умов. Пеленгаційний пристрій, який складається з антенної системи, підсилювача радіочастоти та фазового детектора, структурно описують послідовним з'єднанням елемента порівняння і фільтра нижніх частот з передавальною функцією [4]:

$$W_{пп}(p) = \frac{k_{пп}}{1 + T_{пп} p},$$

де $k_{пп}$, $T_{пп}$ – коефіцієнт перетворення та постійна часу пеленгаційного пристрою;

p – оператор Лапласа.

Передавальні функції підсилювача $W_п(p)$ та двигуна $W_д(p)$ подаються в такому вигляді:

$$W_n(p)=\frac{k_n}{(1+T_n p)},$$

$$W_д(p)=\frac{K_д}{p(1+T_д p)},$$

де k_n, T_n – коефіцієнт перетворення та постійні часу підсилювача;

$k_д$, $T_д$ – коефіцієнт перетворення та постійна часу двигуна.

Припускається, що наведення головного максимуму діаграми спрямованості антени в задану точку простору відбувається поданням на систему автосупроводження вхідної дії, яку опишемо рівнянням

$$x(t)=x_0,$$

а в разі переміщення антени відповідно до реального руху БпЛА – рівнянням

$$x(t)=x_0+\dot{x}t,$$

де x, $\dot{x}$ – значення кутової координати та її похідна.

Необхідно синтезувати алгоритм цифрового управління електроприводом антени, параметри якого вважаються відомими. За критерій якості візьмемо відсутність динамічної помилки наведення антени в ході автосупроводження рухомого об'єкта:

$$\varepsilon_д=x(t)-y(t)=0,$$

де $y(t)$ – кутове положення максимуму діаграми спрямованості антени.

Виклад основного матеріалу. Для синтезу алгоритму управління використано метод, що ґрунтується на теорії інваріантності [10], відповідно до якого передавальну функцію цифрового регулятора визначаємо з такого виразу:

$$W_{цр}(z)=\frac{C(z)-A(z)}{A(z)W(z)}, \tag{1}$$

де

$$A(z)=\left(1-z^{-1}\right)^{N+1}, \tag{2}$$

$$C(z)=\prod_{i=1}^{N+1}\left(1+\Theta_i z^{-1}\right), \tag{3}$$

тут N – порядок вхідної дії;

$C(z)$ – характеристичний поліном замкненої системи, який визначає її стійкість;

$W(z)$ – дискретна передавальна функція об'єкта управління;

$A(z)$ – поліном, який визначає точність системи управління, розраховуємо з умови

$$A(z)x(z)=0.$$

Для синтезу обчислимо передавальну функцію розімкненої системи АСН:

$$W_c(p) = \frac{k_c}{p(1+T_{пп}p)(1+T_n p)(1+T_д p)},$$

$k_c = k_{пп}k_n k_д$.

На практиці перевагу надають простим регуляторам, розмірність яких менша за розмірність об'єкта. Саме тому вихідна передавальна функція $W_c(p)$ підлягає максимальному спрощенню. Відомі декілька способів редукції моделей об'єктів управління, наприклад [7, 11, 12]. У роботі застосовано метод, запропонований у [13]. Його ідея полягає в тому, що для побудови редукованої моделі об'єкта управління відповідності між початковою та редукованою передавальними функціями досягають шляхом використання непрямих показників якості перехідного процесу, які визначають за частотними характеристиками. За редуковану вибирають передавальну функцію

$$W(p) = \frac{k}{p(1+Tp)}, \tag{4}$$

якій відповідають такі амплітудно-частотна $W(\omega)$ та фазочастотна $\varphi(\omega)$ характеристики:

$$W(\omega) = \frac{k\sqrt{1+\omega^2T^2}}{\omega(1+\omega^2T^2)}, \tag{5}$$

$$\varphi(\omega) = arctg\left(\frac{1}{\omega T}\right). \tag{6}$$

При цьому значення коефіцієнта підсилення k та сталої часу T розраховані на частоті зрізу $\omega_{зр}$, яку визначено за логарифмічною амплітудно-частотною характеристикою вихідної моделі $W_c(p)$ [13].

Відповідно до (4) дискретна передавальна функція з урахуванням екстраполятора нульового порядку [4] матиме такий вигляд:

$$W(z) = \frac{c_1 z^{-1} + c_2 z^{-2}}{(1-z^{-1})(1-d_2 z^{-1})}, \tag{7}$$

де $c_1 = \frac{\alpha}{b^2}(bh - 1 + d_2)$;

$c_2 = \frac{\alpha}{b^2}(1 - d_2 - bhd_2)$;

$d_2 = e^{-bh}$;

$\alpha = \frac{k}{T}$;

$b = \frac{1}{T}$;

h – період дискретизації.

Для досягнення заданого показника якості системи з (2) та (3) запишемо поліноми:

$$A(z) = \left(1 - z^{-1}\right)^2, \tag{8}$$

$$C(z) = \left(1 - Q_1 z^{-1}\right)\left(1 - Q_2 z^{-1}\right). \tag{9}$$

Підстановкою рівнянь (7)–(9) до виразу (1) синтезуємо передавальну функцію цифрового регулятора

$$W_{цр}(z) = \frac{m_0 + m_1 z^{-1} + m_2 z^{-2}}{1 + n_1 z^{-1} + n_2 z^{-2}} \tag{10}$$

та визначимо відповідний йому алгоритм цифрового управління

$$u(n) = m_0 \varepsilon(n) + m_1 \varepsilon(n-1) + m_2 \varepsilon(n-2) - n_1 u(n-1) + n_2 u(n-2), \tag{11}$$

де ε – помилка автосупроводження БпЛА;

$$m_0 = \frac{2 - Q_1 - Q_2}{c_1};$$

$$m_1 = -\frac{2d_2 - d_2 Q_1 - d_2 Q_2 - Q_1 Q_2 + 1}{c_1};$$

$$m_2 = \frac{d_2\left(1 - Q_1 Q_2\right)}{c_1};$$

$$n_1 = \frac{c_2 - c_1}{c_1};$$

$$n_2 = -\frac{c_2}{c_1}.$$

Дослідження синтезованого алгоритму управління у складі системи АСН проводилося для таких значень вихідної моделі: $k_c = 20c^{-1}$, $T_{пп} = 0{,}02c$, $T_n = 0{,}03c$, $T_o = 0{,}08c$, – яким відповідає $\omega_{зр} = 15 рад/с$ та $\varphi_c\left(\omega_{зр}\right) = -171^\circ$. З виразів (5) та (6) коефіцієнти редукованої передавальної функції набули таких значень: $k = 87c^{-1}$, $T = 0{,}51$с. Коефіцієнти характеристичного рівняння розраховані методом розміщення нулів та полюсів [9]. Перерегулювання $\sigma \le 20\%$ задовольняють корені характеристичного рівняння $z_1 = 0{,}73$ та $z_2 = 0{,}75$, яким відповідають коефіцієнти $Q_1 = 0{,}73$ та $Q_2 = 0{,}75$.

Результати моделювання у вигляді перехідної характеристики за $x(n) = 1$ та графіки зміни помилки системи ε в разі лінійної вхідної дії $x(n) = nh$ наведено на рис. 1 та рис. 2.

Використання у складі замкнутої системи АСН синтезованого алгоритму цифрового управління зумовлює покращення її динамічних властивостей. Синтезований алгоритм надає системі астатизму другого порядку. У разі заданих вхідних дій у сталому режимі помилка дорівнює нулю.

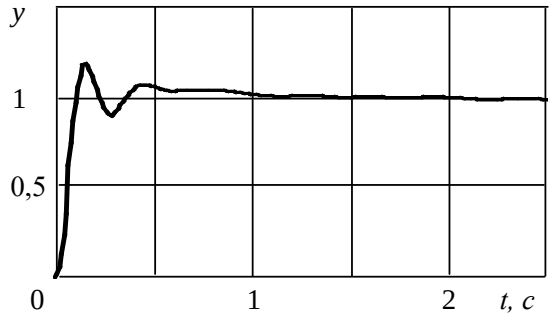


Рис. 1. Перехідна характеристика слідкувальної системи

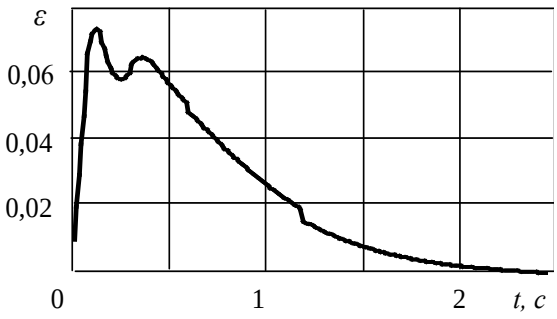


Рис. 2. Помилка слідкувальної системи в разі лінійної вхідної дії

Висновки. Виходячи з викладеного вище, можна стверджувати, що застосування синтезованого алгоритму цифрового управління електроприводом антени наземного пункту керування БпЛА дає змогу підвищити точність системи АСН і, як наслідок, покращити якість виконання завдань, що ставляться перед БпАК.

СПИСОК ЛІТЕРАТУРИ

1. Малкин В. А. Адаптивные фильтры сглаживания сигналов датчиков в системах микроавионики // Приборы и методы измерений. 2012. № 1 (4). С. 11–15.

2. Тимочко О. І., Голубничий Д. Ю., Третяк В. Ф., Рубан І. В. Класифікація безпілотних літальних апаратів // Системи озброєння і військова техніка. 2007. Вип. 1 (9). С. 61–66.

3. Авіоніка безпілотних літальних апаратів / В. П. Харченко, В. І. Чепіженко, А. А. Тунік та ін. ; за ред. В. П. Харченка. Київ : ТОВ «Абрис-принт», 2012. 464 с.

4. Гостев В. И., Стеклов В. И., Скляренко С. Н. Оптимальные системы управления с цифровыми регуляторами : справочник. Київ : КИРЦ «Сенс», 1995. 484 с.

5. Белянский П. В., Сергеев Б. Г. Управление наземными антенами и радиотелескопами. Москва : Сов. радио, 1980. 280 с.

6. Волгин Л. Н. Оптимальное дискретное управление динамическими системами. Москва : Наука, 1986. 239 с.

7. Изерман Р. Цифровые системы управления : пер. с англ. Москва : Мир, 1984. 541 с.

8. Куо Б. Теория и проектирование цифровых систем управления. Москва : Машиностроение, 1986. 448 с.

9. Поляков К. Ю. Основы теории цифровых систем управления : учеб. пособие. Санкт-Петербург : СПбГМТУ, 2006. 161 с.

10. Зімчук І. В., Іщенко В. І., Канкін І. О. Синтез алгоритмів цифрового управління для автоматичних слідкувальних систем // Системні дослідження та інформаційні технології. 2015. № 1. С. 32–38.

11. Некоторые методы синтеза регуляторов пониженного порядка и заданной структуры / Бойченко В. А., Курдюков А. П., Тимин В. Н. и др. // Управление большими системами : сб. трудов. Москва : ИПУ РАН, 2007. Вып. 19. С. 23–126.

12. Романова И. К. Современные методы редукции нелинейных систем и их применение для формирования моделей движущихся объектов // Вестник МГТУ им. Н. Э. Баумана. Сер. “Машиностроение”. 2012. С. 122–133.

13. Зімчук І. В. Синтез цифрових регуляторів пониженого порядку для замкнутих систем управління неперервними об’єктами // Радіоелектроніка, інформатика, управління. 2017. № 4. С. 187–192.

Подано 30.12.2019

В. В. Воротников, И. В. Зимчук, Р. В. Нетребко

АЛГОРИТМ ЦИФРОВОГО УПРАВЛЕНИЯ ЭЛЕКТРОПРИВОДОМ АНТЕННЫ НАЗЕМНОГО ПУНКТА УПРАВЛЕНИЯ БЕСПИЛОТНОГО АВИАЦИОННОГО КОМПЛЕКСА

С каждым годом беспилотные авиационные комплексы находят все большее применение как в гражданской, так и военной сфере. Устойчивая связь с беспилотным летательным аппаратом обеспечивается высокоточным наведением антенны наземного пункта управления. В режиме автоматического сопровождения беспилотного летательного аппарата наведения антенны осуществляется системой автоматического сопровождения по направлению. Показано, что основным требованием, которое выдвигается к системе автосопровождения по направлению, является высокая динамическая точность в условиях помех и шумов различного характера. Традиционная система автосопровождения по направлению не в состоянии обеспечить высокую точность наведения антенны. Улучшить качество следящей системы как в переходном, так и установившемся режимах работы предложено за счет дополнения существующей аналоговой системы подсистемой цифровой коррекции. Работа посвящена синтезу алгоритма цифрового управления электроприводом антенны наземной приемно-передающей станции беспилотного авиационного комплекса. Алгоритм цифрового управления синтезирован как результат решения разностных уравнений, определяемых по дискретной передаточной функции цифрового регулятора. На практике предпочтение отдается простым регуляторам, размерность которых меньше размерности объекта. Упрощение структуры регулятора достигнуто благодаря использованию в процессе синтеза редуцированной модели системы управления антенной. Редукция реализована методом, который основывается на близости переходных характеристик математических моделей начального и редуцированного объектов управления, охваченных единичной отрицательной обратной связью. Для оценки степени близости применены косвенные показатели качества переходного процесса. Непосредственный синтез регулятора выполнен методом на основе теории инвариантности, он предусматривает компенсацию нулей и полюсов передаточной функции объекта управления. Отличительной особенностью использованного метода является возможность учета требований к устойчивости и заданной динамической точности системы управления на этапе синтеза цифрового регулятора. Приведены результаты моделирования, подтверждающие работоспособность и эффективность синтезированного алгоритма управления.

Ключевые слова: *беспилотный летательный аппарат; система автосопровождения по направлению; цифровой регулятор; алгоритм цифрового управления.*

V. V. Vortnikov, I. V. Zimchuk, R. V. Netrebko

ALGORITHM FOR DIGITAL CONTROL OF THE ANTENNA OF THE GROUND CONTROL POINT OF THE UNMANNED AVIATION COMPLEX

Every year, unmanned aircraft systems are increasingly used in both the civilian and military spheres. Stable communication with an unmanned aerial vehicle is provided by high-precision pointing of the antenna of the ground control point. In the automatic tracking mode of an unmanned aerial vehicle, the antenna guidance is carried out by the automatic tracking system in the direction. It is shown that the main requirement that is put forward in the direction of the auto tracking system is high dynamic accuracy under conditions of disturbances and noises of various kinds. The traditional directional tracking system is not able to provide high precision antenna pointing. It is proposed to improve the quality of the tracking system in both transient and steady-state operating modes by supplementing the existing analog system with a digital correction subsystem. That is why the work is devoted to the synthesis of the digital control algorithm for the electric drive of the antenna of the ground receiving and transmitting station of an unmanned aircraft complex. The digital control algorithm is synthesized as a result of solving difference equations determined by the discrete transfer function of the digital controller. In practice, preference is given to simple controls, the dimension of which is less than the dimension of the object. A simplification of the controller structure was achieved by using a reduced model of the antenna control system in the synthesis process. The reduction is implemented by a method that is based on the proximity of the transition characteristics of mathematical models of initial and reduced control objects covered by a single negative feedback. To assess the degree of proximity, indirect indicators of the quality of the transition process are used. The direct synthesis of the controller is performed by a method that is based on the theory of invariance and provides for the compensation of zeros and poles of the transfer function of the control object. A distinctive feature of the method used is the ability to take into account the stability requirements and the given dynamic accuracy of the control system at the stage of synthesis of the digital controller. The simulation results confirming the efficiency and effectiveness of the synthesized control algorithm are presented.

Keywords: *unmanned aerial vehicle; directional tracking system; digital controller; digital control algorithm.*

УДК 681.518 DOI: 10.46972/2076-1546.2019.17.14

І. В. Зімчук, В. І. Іщенко, Т. М. Шапар

СИНТЕЗ МАТЕМАТИЧНОЇ МОДЕЛІ СИСТЕМИ АВТОМАТИЧНОГО КЕРУВАННЯ КУРСОМ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА

Безпілотні літальні апарати на сьогоднішній день є найбільш перспективними системами військового і цивільного призначення. Простежується тенденція до нарощування зусиль низки провідних країн щодо розробки безпілотних літальних апаратів та їх комплексів, тому в статті запропоновано синтез математичної моделі системи автоматичного керування курсом безпілотного літального апарата. Математична модель будь-якої системи відображає в тій або іншій мірі її реальні властивості, зокрема наявні обмеження. З'ясовано, що одним із найбільш сприятливих та ефективних методів побудови математичних моделей систем автоматичного управління є їх розробка з використанням передавальних функцій. Для вирішення поставленого завдання в статті розглянуто склад системи керування курсом безпілотного літального апарата. Синтезовано математичну модель, що складається із сумісного проєктування конструкції самого безпілотного літального апарата та системи автоматичного керування ним. Опис запропонованої математичної моделі системи ґрунтується на поданні лінійної неперервної системи різницевими рівняннями, які отримано з використанням співвідношення Тастіна. Запропонована в статті математична модель може бути використана для дослідження типових літальних апаратів, система управління курсом яких будується за розглянутою структурою.

Практичне значення одержаних результатів полягає в можливості застосування розробленої математичної моделі для дослідження динаміки зміни стану та налаштування системи автоматичного керування курсом безпілотного літального апарата шляхом комп'ютерного моделювання.

Перспективами подальших досліджень у цьому напрямку є проведення комп'ютерного моделювання системи автоматичного керування курсом безпілотного літального апарата та оцінювання точності розробленої математичної моделі.

Ключові слова *математична модель; передавальна функція; система автоматичного керування курсом; безпілотний літальний апарат.*

Постановка проблеми в загальному вигляді. За останні роки в усьому світі значно зріс інтерес до безпілотних літальних апаратів (БпЛА). Завдяки невеликим розмірам, надійним конструкціям, високій маневреності, простоті управління, їх використовують як в інтересах оборони держави, так і для виконання завдань цивільного призначення.

Високі показники якості систем БпЛА, оснащених повноцінним автопілотом, знижують експлуатаційні витрати і вимоги до персоналу. У процесі виконання польоту управління БпЛА здійснюють за допомогою бортового комплексу навігації та управління.

Дієвим підходом до підвищення точності, забезпечення стійкості, керованості й високої швидкодії систем автоматичного пілотування БпЛА є розробка методів їх математичного синтезу. Використання математичного моделювання дозволяє значно скоротити час проєктування, зменшити вартість розробки, підвищити якість створення.

Актуальність проблеми аналізу та синтезу математичної моделі БпЛА полягає в затребуваності нових математичних моделей цих об'єктів і алгоритмів керування, що забезпечують високу якість функціонування системи в цілому, з реалізацією їх числовими методами.

Аналіз останніх досліджень і публікацій. Питання, пов'язані із синтезом математичних моделей систем автоматичного управління, ґрунтовно досліджені в сучасній літературі [1, 3–5, 7, 8], де достатньо глибоко викладено принципи їх побудови за різними класифікаційними ознаками.

Вид математичної моделі та спосіб її розробки обирають на підставі апріорної інформації про об'єкт моделювання й цілі використання моделей [1, 4, 7].

До математичних моделей систем автоматики об'єктів управління ставлять низку вимог. Залежності, що описують модель, повинні бути справедливі для всього розрахункового інтервалу часу, на якому вирішується завдання управління. Модель повинна охоплювати всі вхідні змінні (керувальні та збурення), а також вихідні керовані величини.

Для побудови математичної моделі об'єкта можна використовувати різні методи: аналітичні, експериментальні та експериментально-аналітичні [7]. Аналітичний метод передбачає отримання математичного опису об'єкта у вигляді систем диференціальних рівнянь [1]. Такий підхід дає позитивний результат, якщо даний об'єкт досить простий за структурою і добре вивчений. В іншому разі вдаються до експериментальних методів, суть яких методів полягає в побудові непараметричних моделей у вигляді перехідної функції або частотної характеристики та параметричних моделей у вигляді системи диференціальних рівнянь або передавальних функцій. Параметричні методи отримання математичних моделей вимагають апріорного знання порядку моделей об'єкта та збурень [8].

Формулювання завдання дослідження. Метою статті є розробка математичної моделі для оцінювання ефективності функціонування системи автоматичного управління курсом БпЛА. Для цього необхідне вирішення таких завдань:

окреслити склад, структуру та зв'язки системи автоматичного управління курсом БпЛА;

визначити форму математичного опису її окремих частин;

розробити різницеві рівняння, придатні для комп'ютерного моделювання системи автоматичного управління курсом БпЛА.

Одним із найбільш сприятливих та ефективних методів розробки математичних моделей систем автоматичного управління є побудова з використанням передавальних функцій. Для синтезу рівнянь, які описують передавальні функції елементів системи управління, буде використано перетворення Тастіна [3].

Виклад основного матеріалу. Автопілот є одним із головних елементів загальної системи управління, що призначений для стабілізації кутових рухів літального апарата відносно центра маси та управління рухом самого центра маси відповідно до команд, що надходять з бортової радіоапаратури БпЛА.

Кожен автопілот має, як правило, три канали управління: тангаж, курс та крен. До складу кожного каналу входять чутливі елементи (гіроскопи) та рульовий привід [2, 5].

Стабілізація курсу автопілотом здійснюється за допомогою органів керування: рулем напрямку, елеронами, рулем напрямку й елеронами. Автопілот курсу виконує функцію стабілізації поздовжньої осі БпЛА і вектора швидкості за курсом. Поздовжня вісь у горизонтальній площині повертається під дією моментів відносно нормальної осі. Керувальний момент відносно нормальної осі створюється відхиленням руля напрямку. Розворот вектора швидкості за курсом відбувається під дією бічної сили, спричиненої кутом ковзання або за рахунок горизонтальної складової піднімальної сили, що виникає в разі при крені БпЛА [2, 9].

Функціональну схему системи автоматичного управління курсом БпЛА за допомогою руля напрямку наведено на рис. 1 [5, 9], де позначено:

П – підсилювач;

РМ – рульова машинка;

РН – руль напрямку;

ДК – датчик кута;

ДКШ – датчик кутової швидкості;

ЖЗЗ – жорсткий зворотній зв’язок;

$x(t), y(t)$ – вхідне та вихідне значення курсу;

$Мз$ – діюче збурення;

$\varepsilon(t)$ – помилка управління курсом.

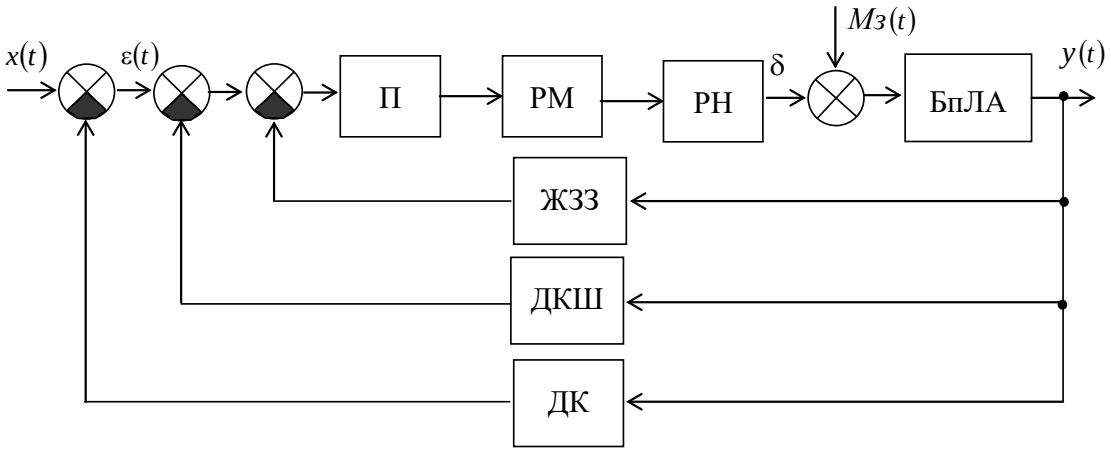


Рис. 1. Функціональна схема системи автоматичного управління курсом БпЛА

На вхід ланки БпЛА, що описує динаміку його руху, надходять впливи від руля напрямку та збурень. Виходом ланки є відхилення кута курсу та швидкість зміни курсу. Датчики кута та кутової швидкості виробляють сигнали, пропорційні значенням кута та кутової швидкості. Ці сигнали надходять на суматор, а потім через підсилювач на рульову машинку, яка переміщує руль напрямку.

У разі відхилення кута курсу від заданого, виникає помилка $\varepsilon = x - y$, яка після підсилення рульової машинки переміщує руль напрямку доти, доки помилка не стане дорівнювати нулю.

Отже, закон керування для стабілізації курсу за допомогою каналу руля напрямку має такий вигляд:

$$\delta = k_н(x - y) + k_v\dot{y}, \tag{1}$$

де $k_н, k_v$ – коефіцієнти перетворення.

Для покращення перехідного процесу БпЛА до автопілота вводять допоміжні сигнали: *U*, пропорційні кутовій швидкості обертання літака, та сигнал, пропорційний лінійним прискоренням. Тоді процес налаштування необхідного значення нормальних прискорень, заданих командою управління, буде проходити швидше, за відсутності цих допоміжних сигналів.

Знаючи передавальні функції рульового приводу і чутливих елементів, можна побудувати структурну схему системи автоматичного управління курсом БпЛА. Її наведено на рис. 2, де $K_p(p)$ умовно позначає передавальну функцію БпЛА [5].

Сигнали $U_{дк}$ і $U_{дкш}$, що знімаються з датчиків кута та кутової швидкості, відраховуються від сигналу команди управління U_k та надходять на рульовий привід. Руль курсу буде відхилятися таким чином, щоб компенсувати коливання й одночасно забезпечувати відповідність нормального прискорення величині команди управління U_k.

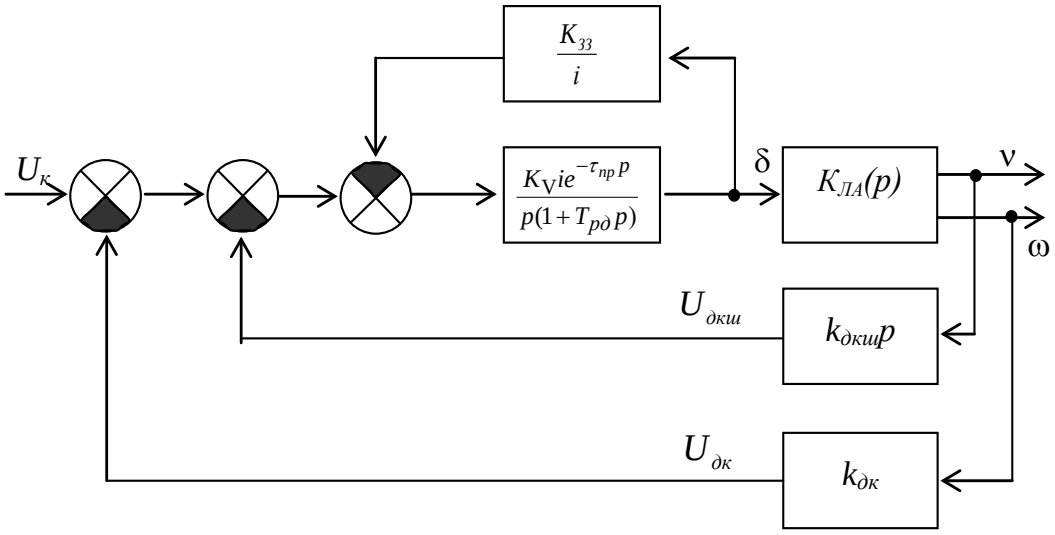


Рис. 2. Структурна схема системи автоматичного управління курсом БпЛА

Структурну схему рис. 2 можна спростити, якщо врахувати, що постійні часу рульового приводу ($\tau_{пр}$, $T_{рд}$) значно менші за постійну часу БпЛА *Тр*. Тоді передавальна функція замкненого рульового приводу матиме такий вигляд:

$$K_з(p) = \frac{\frac{k_v i}{p}}{1 + \frac{k_v i}{p}\frac{k_{зз}}{i}} = \frac{k_{пр} i}{1 + T_{пр} p}, \tag{2}$$

де $k_{пр} = 1/k_{зз}$ – коефіцієнт підсилення замкненого приводу;

$T_{пр} = 1/k_v\, k_{зз}$ – постійна часу.

Визначимо передавальну функцію БпЛА. Відомо, що вона за кутом атаки α є коливальною ланкою:

$$K_\alpha(p) = \frac{k_\alpha}{T_{ла}^2 p^2 + 2\xi_{ла} T_{ла} p + 1}, \tag{3}$$

де k_α – коефіцієнт підсилення за кутом атаки, який не має розмірності;

$T_{ла}$ – аеродинамічна стала часу;

$\xi_{ла}$ – коефіцієнт демпфування.

Отримаємо передавальну функцію за кутом курсу.

$$K_v(p)=\frac{k_\alpha}{T_{ла}^2 p^2+2\xi_{ла}T_{ла}p+1}\left(1+\frac{1}{T_\vartheta p}\right) \tag{4}$$

або після перетворення

$$K_v(p)=\frac{k_v(T_\vartheta p+1)}{p\left(T_{ла}^2 p^2+2\xi_{ла}T_{ла}p+1\right)}, \tag{5}$$

де $k_v=k_\alpha/T_\vartheta$ – коефіцієнт підсилення БпЛА за кутом курсу.

За результатами отримання передавальних функцій елементів системи маємо спрощену структурну схему системи автоматичного управління курсом БпЛА, яку наведено на рис. 3.

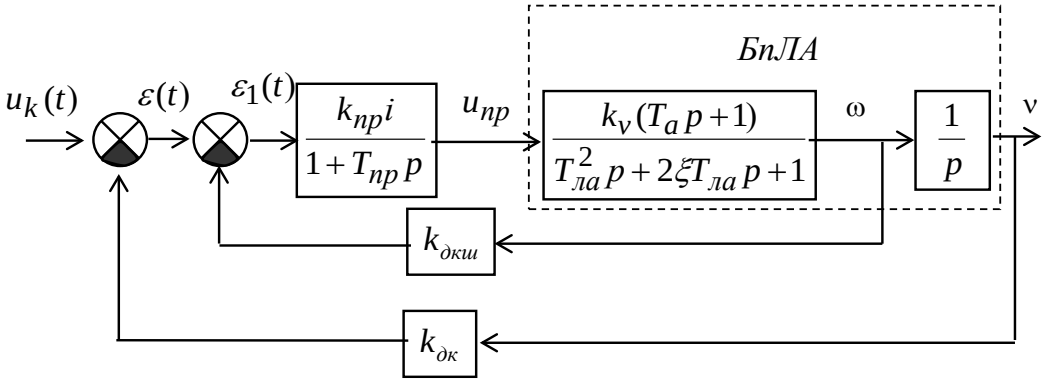


Рис. 3. Структурна схема системи управління БпЛА за каналом курсу

В основу математичної моделі системи управління БпЛА за каналом курсу покладено структурну схему, наведену на рис. 3. Для синтезу рівнянь, які описують передавальні функції елементів системи управління, використано так звану «підстановку Тастіна» [3]. Це перетворення дозволяє отримати дискретну передавальну функцію лінійного об'єкта з його вихідної безперервної передавальної функції.

Застосовуючи для опису передавальних функцій рекурентні формули для рульового приводу, маємо таке рівняння:

$$u_1(n)=\frac{2-T/T_{пр}}{2+T/T_{пр}}u_1(n-1)+\frac{T}{2+T/T_{пр}}\left(\varepsilon_1(n-1)+\varepsilon_1(n-1)\right), \tag{6}$$

$$u_{пр}(n)=k_{пр}iu_1(n), \tag{7}$$

де $u_{пр}(n)$ – вихідний сигнал приводу системи автоматичного управління курсом.

Літальний апарат опишемо такими рівняннями:

$$x_4(n)=\frac{k_v T_a}{T_{ла}^2}u_{пр}(n); \tag{8}$$

$$x_3(n)=\frac{4-2bT-aT^2}{4+2bT+aT^2}x_3(n-1)-\frac{4aT}{4+2bT+aT^2}x_2(n-1)+ \\ +\frac{2T}{4+2bT+aT^2}(x_4(n)+x_4(n-1)); \tag{9}$$

$$x_2(n)=x_2(n-1)+\frac{T}{2}(x_3(n)+x_3(n-1)); \tag{10}$$

$$w_1(n)=x_3(n)+dx_2(n); \tag{11}$$

$$w(n)=w(n-1)+\frac{T}{2}(w_1(n)+w_1(n-1)), \tag{12}$$

де $a=\frac{1}{T_{ла}}$; $b=\frac{2\xi_{ла}}{T_{ла}}$; $d=\frac{1}{T_a}$; $T-$ інтервал дискретизації.

Помилку управління визначимо з виразу

$$\varepsilon(k)=u_k(n)-k_{ок}w(n). \tag{13}$$

Сигнал із виходу другого елемента порівняння опишемо виразом

$$\varepsilon_1(n)=\varepsilon(n)-k_{окш}w_1(n). \tag{14}$$

Висновок. Отже, у результаті проведених досліджень запропоновано математичну модель системи керування курсом БпЛА, яка складається із сумісного проєктування конструкції самого БпЛА та системи автоматичного керування ним. Математична модель ґрунтується на поданні лінійної неперервної системи різницевими рівняннями завдяки використанню співвідношення Тастіна. Її можна застосовувати для дослідження типових літальних апаратів, система управління курсом яких будується за розглянутою структурою. Запропонована розробка може розглядатися як інструмент для дослідження моделей літальних апаратів.

Перспективами подальших досліджень у цьому напрямку є проведення комп'ютерного моделювання системи автоматичного керування курсом БпЛА та оцінювання точності розробленої математичної моделі.

СПИСОК ЛІТЕРАТУРИ

1. Васильев Е. М., Коломыцев В. Г. Теория автоматического управления. Дискретные системы : учеб. пособ. Пермь : Изд-во Перм. нац. исслед. политехн. ун-та, 2012. 152 с.

2. Управление и наведение беспилотных маневренных летательных аппаратов на основе современных информационных технологий / К. К. Веремеенко, А. Н. Головинский, В. В. Инсаров, М. Н. Красильщиков и др. Москва : Физматлит, 2003. 280 с.

3. Гостев В. И., Стеклов В. И. Системы автоматического регулирования с цифровыми регуляторами : справочник. Киев : “Радіоаматор”, 1998. 704 с.
4. Зімчук І. В., Іщенко В. І., Канкін І. О. Синтез алгоритмів цифрового управління для автоматичних слідкувальних систем // Системні дослідження та інформаційні технології. 2015. № 1. С. 32–38.
5. Іщенко В. І. Теорія автоматичного управління. Ч 1. Елементи та системи автоматичного управління : навч. посіб. Житомир : ЖВІ НАУ, 2007. 184 с.
6. Купріянова В. С., Матюшенко І. Ю. Стан та перспективи розвитку безпілотних літальних апаратів в Україні // Вісник економіки транспорту і промисловості. 2015. № 50. С. 334–340.
7. Методы классической и современной теории автоматического управления : учебник в 5 т. Т. 3. Синтез регуляторов систем автоматического управления / Под ред. К. А. Пупкова, Н. Д. Егупова. Москва : Изд-во МГТУ им. Н. Э. Баумана, 2004. 616 с.
8. Поляков К. Ю. Основы теории цифровых систем управления : учеб. пособ. Санкт-Петербург : СПб ГМТУ, 2006. 161 с.
9. Харченко В. П., Чепіженко В. І, Тунік А. А., Павлова С. В. Авіоніка безпілотних літальних апаратів : монографія / За ред. В. П. Харченка. Київ : ТОВ «Абрис-принт», 2012. 464 с.

Подано 30.12.2019

И. В. Зимчук, В. И. Ищенко, Т. Н. Шапар

СИНТЕЗ МАТЕМАТИЧЕСКОЙ МОДЕЛИ СИСТЕМЫ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ КУРСОМ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

Беспилотные летательные аппараты на сегодняшний день являются наиболее перспективными системами военного и гражданского назначения. Прослеживается тенденция к наращиванию усилий ряда ведущих стран по разработке беспилотных летательных аппаратов и их комплексов, поэтому в статье предложен синтез математической модели системы автоматического управления курсом беспилотного летательного аппарата. Математическая модель любой системы отражает в той или иной степени её реальные свойства, в частности имеющиеся ограничения. Установлено, что одним из самых благоприятных и эффективных методов построения математических моделей систем автоматического управления является их разработка с использованием передаточных функций. Для решения поставленной задачи в статье рассмотрен состав системы управления курсом беспилотного летательного аппарата. Синтезирована математическая модель, состоящая из совместного проектирования конструкции самого беспилотного летательного аппарата и системы автоматического управления им. Описание предлагаемой математической модели системы основано на представлении линейной непрерывной системы разностными уравнениями, полученными с использованием соотношения Тастина. Предложенная в статье математическая модель может быть использована для исследования типичных летательных аппаратов, система управления курсом которых строится по рассмотренной структуре.

Практическое значение полученных результатов заключается в возможности применения разработанной математической модели для исследования динамики

изменения состояния и настройки системы автоматического управления курсом беспилотного летательного аппарата путем компьютерного моделирования.

Перспективами дальнейших исследований в этом направлении является проведение компьютерного моделирования системы автоматического управления курсом беспилотного летательного аппарата и оценки точности разработанной математической модели.

***Ключевые слова**: математическая модель; передаточная функция; система автоматического управления курсом; беспилотный летательный аппарат.*

I. V. Zimchuk, V. I. Ishchenko, T. M. Shapar

SYNTHESIS OF THE MATHEMATICAL MODEL OF THE AUTOMATIC CONTROL SYSTEM OF THE UNMANNED AIRCRAFT COURSE

Unmanned aerial vehicles are by far the most promising military and civilian systems. There is a tendency to increase the efforts of a number of leading countries in the development of unmanned aerial vehicles and their complexes. The mathematical model of any system reflects in one way or another its real properties, including the existing limitations. It has been found that one of the most favorable and efficient methods for constructing mathematical models of automatic control systems is to develop them using transfer functions. In order to solve this problem, the article deals with the composition of the control system of a drone. A mathematical model consisting of the joint design of the unmanned aerial vehicle and its automatic control system has been synthesized. The description of the proposed mathematical model of the system is based on the representation of a linear continuous system by the difference equations obtained using the Tustin relation. The mathematical model proposed in the article can be used for the study of typical aircraft whose course management system is built according to the considered structure.

The practical significance of the obtained results is the possibility of applying the developed mathematical model to study the dynamics of the change of state and to set up the system of automatic control of the course of the unmanned aerial vehicle through computer simulation.

Prospects for further research in this area are computer simulation of an unmanned aerial vehicle control system and estimation of the accuracy of the mathematical model developed.

***Keywords:** mathematical model; transfer function; automatic course management system; unmanned aerial vehicle.*

УДК 355.40:004.82(477) DOI: 10.46972/2076-1546.2019.17.15

С. С. Гаценко, Є. М. Коутний, В. В. Шипітко, Д. О. Грибовський, О. М. Максименко

МЕТОДИКА РАЦІОНАЛЬНОГО РОЗПОДІЛУ СИЛ І ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ ЗА ЗАВДАННЯМИ, ОБ'ЄКТАМИ ТА ДЖЕРЕЛАМИ МОНІТОРИНГУ ОПЕРАТИВНО-ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ

Збройна агресія Російської Федерації проти України, втрата таких важливих промислових потенціалів, як Державна акціонерна холдингова компанія «Топаз», яка спеціалізувалася на розробці та виробництві складних радіотехнічних систем і комплексів, зокрема унікальних комплексів дальньої радіотехнічної розвідки та раннього попередження систем протиповітряної оборони, а саме станції радіотехнічної розвідки «Кольчуга», дали значний поштовх для розвитку радіоелектронної розвідки як одного з головних технічних видів воєнної розвідки України.

Радіоелектронна розвідка Збройних Сил України – це комплекс заходів і дій із добування розвідувальної інформації про збройні сили інших держав через викриття функціонування радіоелектронних засобів і радіотехнічних систем, які застосовуються для управління військами (силами) та зброєю, а також для збору, обробки, аналізу та доведення даної інформації визначеним споживачам у встановлені терміни.

Метою ведення радіоелектронної розвідки є своєчасне та гарантоване викриття на ранній стадії ознак виникнення безпосередньої загрози безпеці України з боку держав (блоків, коаліцій), що розвідуються, а також добування розвідувальної інформації для ефективної підготовки та застосування Збройних Сил України.

Для досягнення окресленої мети функціонує система радіоелектронної розвідки, яка є сукупністю взаємопов'язаних та узгоджених у своїх діях за завданнями, місцем і часом органів управління радіоелектронної розвідки усіх ланок, сил і засобів військових частин (підрозділів), які виконують визначені розвідувальні завдання за єдиним замислом і планом.

Розвідувальні завдання та об'єкти розвідки військовим частинам (підрозділам) радіоелектронної розвідки визначають з урахуванням їх призначення, наявності сил і засобів, а також їх можливостей.

Важливим елементом планування радіоелектронної розвідки як у мирний час, так і на оперативний період є раціональний (доцільний) розподіл відповідних сил і засобів у військовій частині радіоелектронної розвідки, що здійснюється за завданнями, об'єктами та джерелами моніторингу.

У статті на основі аналізу проблем розподілу ресурсу сил і засобів за завданнями, об'єктами та джерелами радіоелектронної розвідки як основного елемента планування на командних пунктах військових частин (підрозділів) радіоелектронної розвідки обґрунтовано структуру методики раціонального розподілу сил і засобів радіоелектронної розвідки для органів оперативно-тактичної ланки управління. В основі методики лежить системний підхід до організації розвідки з урахуванням вимог адекватності щодо структурного й функціонального образу в ході моделювання взаємозв'язків завдань, об'єктів і джерел розвідки. Головна мета методики – розробка

раціональних планів розподілу ресурсу для підвищення ефективності ведення радіоелектронної розвідки елементами системи й оцінювання їх можливостей.

Ключові слова: *система радіоелектронної розвідки; мета, об'єкти, джерела розвідки; ефективність; імовірність; план розвідки; розподіл сил і засобів.*

Постановка проблеми в загальному вигляді. На практиці розподіл сил і засобів (РСЗ) за завданнями, об'єктами та джерелами розвідки на командних пунктах (КП) військових частин радіоелектронної розвідки (РЕР) (Регіональних центрів РЕР), підрозділів РЕР (маневрених, окремих центрів РЕР) у повній мірі не здійснюється. Тобто для умов мирного часу традиційно використовують вироблений за довгий період ведення РЕР так званий "базовий варіант" (план розвідки (план бойового застосування сил і засобів)) розподілу ресурсу постів РЕР (радіоперехоплення, радіотехнічної розвідки) за екземплярами джерел радіовипромінювань (ДРВ) і мереж пеленгування, що знаходяться на спостереженні, а також постів і ресурсу мереж пеленгування для поточного пошуку як ДРВ, що спостерігатимуться, у разі зміни ними радіоданих, так і нових джерел, що не увійшли до плану розвідки.

Для інших умов, зміни оперативної обстановки, різких змін радіоелектронної обстановки (РЕО) в особливий період використовують режими посилення, пов'язані зі збільшенням загального ресурсу і нормативно розподіленого ресурсу щодо можливих джерел без детального розрахунку охоплення об'єктів і тим більше оцінки якості виконання розвідувальних завдань. Цілеспрямованість пошуку для цих умов з погляду процесу викриття РЕО низька передусім через відсутність робочих розвідувально-інформаційних моделей, еталонних моделей [1–5] і загальної, адекватної умовам методики розподілу ресурсу [6–8].

Питання формалізації, а тим більше автоматизації основних процесів розробки планів РСЗ для різних умов РЕО й окремих етапів ведення бойових дій не вирішені [9–12].

Причинами основних недоліків у практиці розподілу ресурсу є недоліки теорії [13–14]. Отже, **аналіз останніх досліджень і публікацій** вказує на недостатність вирішення завдань планування розподілу сил і засобів РЕР, що зумовлено [1–3]:

відсутністю методики розподілу ресурсу сил і засобів РЕР, придатної для використання в засобах автоматизації різних ланок управління, зокрема в його оперативно-тактичній ланці, що зв'язує завдання, об'єкти і джерела РЕР на основі використання сучасних розвідувально-інформаційних моделей для аналізу взаємозв'язків елементів розподілу та точної оцінки розвідувальної доступності джерел РЕР;

низькою критичністю до вирішуваних завдань показників ефективності розподілу, помилковою орієнтацією на організацію управління і зв'язку традиційних систем 80–90-х років, що не дозволяє сформувати оптимальний (раціональний) план розподілу ресурсу;

низькими показниками адекватності моделей, що застосовуються, особливо на перспективних системах зв'язку, для угруповань "модульних сил", їх систем управління на базі комплексних автоматизованих систем управління та комунікаційних систем загального користування з низькою структурною доступністю, що використовують самоорганізуючі мережі та супутникові системи зв'язку (WIN-T) [15–19]. Сучасна комунікаційна система відповідає концепції єдиного інформаційного простору Альянсу NNEC (NATO Network Enabled Capability), в основі якої – аналогічна американська

концепція мережецентричної війни NCW (Network-Centric Warfare), Концептуальна система управління збройних сил (ЗС) Російської Федерації для гарантованого управління військами (силами) і зброєю в єдиному інформаційному просторі [20–29]. Без вирішення зазначених проблем якість виконання завдань РСЗ у ході планування РЕР, а отже, завдань за призначенням, буде неухильно знижуватися.

Формулювання завдання дослідження. З урахуванням проблем розподілу ресурсу сил і засобів РЕР за завданнями, об'єктами і джерелами РЕР як основного елемента планування на КП військових частин (підрозділів) РЕР, **метою статті є:** обґрунтування структури методики раціонального плану (РП) РСЗ за завданнями, об'єктами і джерелами РЕР для органів оперативно-тактичної ланки управління, що дозволить запропонувати підхід до організації моніторингу з урахуванням вимог адекватності щодо структурного та функціонального образу в ході моделювання взаємозв'язків завдань, об'єктів і джерел РЕР тощо.

Виклад основного матеріалу. Методика РСЗ РЕР за завданнями, об'єктами та джерелами для військової частини (підрозділу) РЕР є елементом загальної методики РСЗ розвідки. Вона є сукупністю елементів (методів, операцій) традиційного та запропонованого науково-методичного апарату на основі поєднання методів нормативного планування й динамічного програмування, що застосовуються в певній логічній послідовності для формування РП розрахунку за завданнями, об'єктами розвідки (ОР), які адекватно їх відображають, а також ДРВ, що проявляються у функціонуванні ОР для різних умов обстановки (етапів бою або операції), з метою управління силами і засобами добування й обробки в інтересах ефективного вирішення завдань РЕР та оцінювання ступеня ефективності.

Основу розробленої авторами методики РП РСЗ РЕР складають структурно-просторові моделі взаємозв'язків завдань, об'єктів і джерел на базі розвідувально-інформаційних моделей (моделей управління силами та засобами добування й обробки в інтересах викриття джерел і об'єктів, їх складу, стану, положення, характеру діяльності) [30–32]. Вони описують для різних умов обстановки класи завдань, їх взаємозв'язки з об'єктами, характеристики об'єктів за інформаційними групами, розподілом за глибиною і проявом у ДРВ. Джерела описують за класами, діапазоном і розвідувальною (інформаційною) доступністю.

Структуру методики наведено на рис. 1, її важливими елементами є три методики:

РСЗ РЕР за завданнями й ОР у військовій частині (підрозділі) РЕР [32, 33];

розрахунку ОР та ДРВ у військовій частині (підрозділі) РЕР [32, 33];

розробки розвідувально-інформаційної моделі управління силами та засобами добування й обробки [32–34].

Вихідними даними для розподілу ресурсу є:

завдання РЕР, поставлені органами управління розвідки (для різних етапів розвитку оперативної обстановки);

розрахунок сил і засобів за завданнями й об'єктами військової частини (підрозділу) РЕР (оцінка важливості завдань у балах, їх конкретизація за часом і об'єктами, кількість об'єктів в інформаційних групах, за глибиною та напрямками, а також джерел – за групами, діапазоном, у тому числі доступним, ресурс постів перехоплення і пеленгування для резерву, пошуку та спостереження, пеленгаторних мереж);

розвідувально-інформаційна модель складу, стану, положення, характеру діяльності угруповання противника;

система управління, зв'язку і радіотехнічного забезпечення угруповання противника, викрите або надійно прогнозоване;

наявні сили і засоби РЕР, їх бойові можливості та бойові порядки підрозділів (комплексів РЕР).

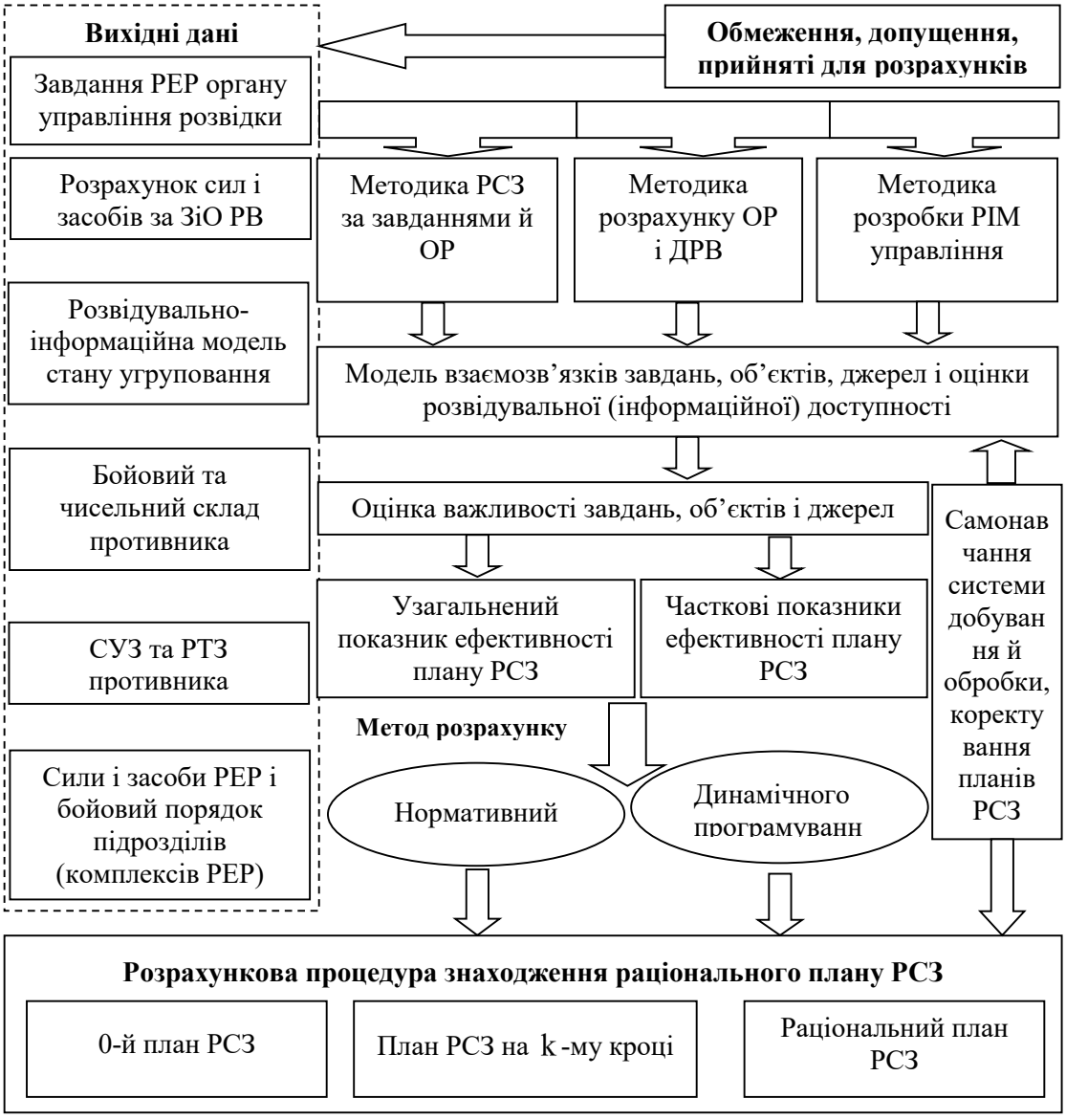


Рис. 1. Структура методики раціонального розподілу ресурсу

У даній методиці в ході вирішення завдань розподілу й оцінювання ефективності (якості) виконання розвідувальних завдань військовою частиною (підрозділом (комплексом РЕР)) введено такі обмеження і допущення:

визначення завдань РЕР, розрахунок сил і засобів на КП військових частин (підрозділів) РЕР здійснюється за відомими методиками (ручний режим);

ресурс розподіляється для всіх типів постів (елемент новизни) як наявних комплексів, так і перспективних, при цьому пости управління й обробки враховують під час розрахунку розвідувальної (ознакової) доступності;

модель організації пошуку та спостереження послідовна, пошук ведеться за частотою, напрямком, у просторі – за ознаками ДРВ.

За метод вирішення завдання розподілу, як показує аналіз його обсягу та проведене дослідження способів розрахунку, може бути використано комплексування методів нормативного планування і динамічного програмування [34, 35], що дозволяє ввести обмеження простору перебору на основі виявлених на практиці меж між різними ресурсами: резерв – 5–10%, пошук – залежно від ступеня розкриття РЕО (поточний – для звичайної обстановки 5–10%, посилений – для частково розкритої РЕО 30–40%, масований – для нерозкритої РЕО 70–80%). Середня розрахункова норма на пост під час ведення спостереження: для наявних комплексів – 3-4 джерела (як для періодичного спостереження), для нових та перспективних комплексів – 10–12.

Моделювання взаємозв'язку завдань, об'єктів, джерел і оцінки розвідувальної (інформаційної) доступності здійснюється такими методами: структурно-статистичним, логічним, зокрема статистичної обробки рішень експертів, через елементи РЕО і математичної логіки. Дана модель є новим елементом у відомих методиках.

Для оцінювання ефективності РП РСЗ РЕР введено загальні (узагальнені) та часткові показники, виходячи з таких міркувань.

Загальні показники повинні оцінювати якість плану в цілому, а часткові – окремо елементи розподілу: важливість завдань, об'єктів і джерел, його процеси. Ґрунтуючись на теорії подібності моделі й реальної системи РЕР, а також використовуючи такі основні вимоги до розвідки, як характеристики (повноту, своєчасність і достовірність), виберемо показники.

За загальний показник ефективності РП РСЗ РЕР на спостереження і пошук $D_{\text{П.С}}$ візьмемо ймовірність вирішення завдань РЕР $P_{\text{вириш}}(Z)$, яка відображає повноту виконання завдань РЕР за обмеження (виконання вимог) щодо своєчасності та достовірності.

Тоді за часткові показники ефективності РП РСЗ РЕР (для елементів розподілу) логічно вибрати:

коефіцієнт охоплення об'єктів у завданні $K_{\text{охопл О}}$:

$$K_{\text{охопл О}} = \frac{N_{\text{О викр}}}{N_{\text{О РІМ}}}, \tag{1}$$

де $N_{\text{О викр}}$ – кількість об'єктів у завданні, що входять до плану;

$N_{\text{О РІМ}}$ – кількість об'єктів завдання в розвідувально-інформаційній моделі;

$Д_{\text{вириш}}(Z)$ – достовірність вирішення завдання, що характеризується ймовірністю розпізнавання об'єктів у ньому, які входять до плану $P_{\text{розп О}}$;

$C_{\text{вириш}}(Z)$ – своєчасність виконання завдання, що залежить від імовірності своєчасного попередження викриття об'єктів розвідувального завдання, що входять до плану $P_{\text{випередж. викр О}}$.

Для розрахунку узагальненого показника застосовано статистичну модель і відповідний їй математичний апарат (теорію ймовірностей) та поетапно проведено обчислення.

На першому етапі оцінено важливість завдань, ОР і ДРВ.

За аналогією до оцінювання розвідувально-інформаційних документів та розподілу ОР відповідно до дальностей її ведення запропоновано три градації важливості завдань згідно з нормативними вимогами $B^u(Z)$ [32] (табл. 1).

Таблиця 1

Оцінка важливості розвідувальних завдань

Градація u	Важливість завдання $B^u(Z)$	Критерії оцінювання за вимогами до об'єктів, що відображають завдання		
		Повнота $K_{\text{охопл О}}$	Достовірність $P_{\text{розп О}}$	Своєчасність $P_{\text{випередж.викр О}}$
1	Особливої важливості	0,75	0,7	0,8
2	Важливі	0,65	0,6	0,7
3	Становлять інтерес	0,5	0,5	0,6

При цьому повнота охоплення ОР повинна бути (не менше): I категорія (органи й пункти управління РЯО, ЗМУ та ВТЗ) – 0,95; II категорія (найбільш важливі пункти управління) – 0,7; III категорія (інші об'єкти) – 0,5 [30, 32, 36].

Важливість ОР в загальному випадку можна визначити, виходячи з таких її складових (у порядку їх значущості):

ранг об'єкта (категорія), рівень (дивізія, бригада, батальйон, рота та їм рівні);

місце в бойовому порядку;

кількість завдань, у яких об'єкт проявляється, з урахуванням їх градацій важливості;

ступінь відображення через розвідувальні ознаки змісту завдань, у яких об'єкт проявляється, $P(X_j / Z_i)$ (знаходиться з розвідувально-інформаційної моделі).

Інформативність (важливість) джерела логічно визначити за такими показниками (у порядку їх значущості):

імовірністю розвідувальної доступності джерела $P_{\text{РД}}$; важливістю об'єктів, що входять до його складу;

кількістю об'єктів у мережі.

Імовірність $P_{\text{РД}}$ залежить від таких показників потенційної та реальної доступності, як: електромагнітна ($P_{\text{ЕМД}}$), апаратурна ($P_{\text{АД}}$), семантична ($P_{\text{СД}}$), ознакова доступність ($P_{\text{ОзД}}$). Її визначають як [15]

$$P_{\text{РД}} = P_{\text{ЕМД}}\left[1-\left(1-P_{\text{АД}}\right)\left(1-P_{\text{СД}}\right)\left(1-P_{\text{ПрД}}\right)\right]. \quad (2)$$

Імовірність розпізнавання об'єкта $P_{\text{розп О}}$ обчислюють з урахуванням розпізнаваності його через джерела радіорозвідки, у які об'єкт входить як головна ($P_{\text{розп.гол.р/ст.}}$) і підпорядковані станції ($P_{\text{розп.подч.р/ст.}}$), а також засоби РТЗ ($P_{\text{розп.РТР}}$):

$$P_{\text{розп О}} = 1-\left(1-P_{\text{розп.подч.р/ст.}}\right)\left(1-P_{\text{розп.гол.р/ст.}}\right)\left(1-P_{\text{розп.РТР}}\right). \quad (3)$$

Отже, у загальному випадку аналітичний вираз для розрахунку узагальненого показника k -го плану розподілу матиме такий вигляд:

$$P_{\text{вирiш}}(Z)=\sum_{u=1}^{3}\frac{N_{\text{вирiш}\,u}}{N_{\text{необх}\,u}}K_{\text{В}u}, \tag{4}$$

де $N_{\text{вирiш}\,u}$ – кількість розвідувальних завдань, що вирішуються за ступенем градації важливості;

$N_{\text{необх}\,u}$ – загальна кількість поставлених розвідувальних завдань, що потребують виконання;

$K_{\text{В}u}$ – коефіцієнт важливості завдання, що вирішується для кожної градації, визначений експертним шляхом за аналогією з оцінкою інформаційних документів: для завдань особливої важливості – 0,5; для важливих завдань – 0,3; для завдань, що становлять інтерес, – 0,2.

Розрахункова процедура знаходження РП базується на методі динамічного програмування, в основу якого закладено принцип оптимальності, сформульований Веллманом [37]. Опис моделі динамічного програмування схематично зображено на рис. 2.

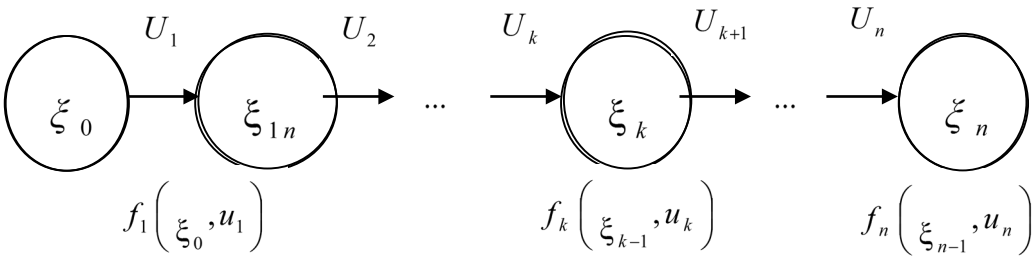


Рис. 2. Модель динамічного програмування

Наведено керовану систему (розподілу ресурсу), яка під впливом управління U_k переходить з початкового стану ξ_0 (вихідний або нульовий план розподілу $D_{\text{П П }0}$) у кінцевий ξ_n (РП розподілу). Передбачено, що весь процес управління системою може бути розбитий на n кроків. Причому $\xi_1, \xi_2, \ldots \xi_n$ – стани системи після першого, другого, ... n-го кроків. Стан системи на будь-якому кроці ξ_k характеризується параметрами $\xi_1, \xi_2, \ldots \xi_n$, так званими «фазовими координатами s-мірного простору» (перебір джерел плану розподілу для пошуку найменш інформативного та виключення його з плану). Послідовного (покрокового) перетворення системи досягають за допомогою дій $U_1 \ldots . U_n$, які становлять управління системою (характеризують показник ефективності на k-му кроці). Це спричиняє мінімальні втрати ймовірності вирішення завдань $\Delta P_{\text{вирiш}}(Z)$:

$$U=(U_1, U_2, \ldots . U_n), \tag{5}$$

де U_k – управління на k-му кроці, що переводить систему зі стану ξ_{k1} у ξ_k .

Управління полягає у виборі значень певних керівних змінних $U_{k1}, U_{k2}, ...U_{kr}$.

Для методики раціонального РСЗ РЕР доцільно застосовувати тільки зворотний хід виконання завдання.

Алгоритм розв'язання розрахункової задачі

Відповідно до моделі обчислювальна процедура пошуку РП розподілу має такий вигляд.

1. Формування нульового плану розподілу $D_{\text{ПП }0}$.

1.1. Розробка моделі взаємозв'язку завдань, ОР та ДРВ.

1.2. Оцінка розвідувальної (інформаційної) доступності ДРВ, включених у модель (2).

1.3. Вилучення з моделі неінформативних ДРВ з $P_{\text{РД}} < 0{,}5$.

1.4. Розрахунок імовірності розпізнавання кожного об'єкта $P_{\text{розп О}}$ (3).

1.5. Визначення узагальненого показника плану розподілу – імовірності вирішення завдань РЕР $P_{\text{вирiш}}(Z)$ (1, 4) (табл. 1).

1.6. Розрахунок потрібного ресурсу постів спостереження для охоплення періодичним наглядом усіх джерел плану за типами постів.

1.7. Визначення ресурсу постів резерву (5–10%) і пошуку (залежно від ступеня розкриття РЕО; для ведення розвідки в ході бойових дій – посилений пошук, як для частково викритої обстановки, – 30–40%).

1.8. Визначення загального необхідного ресурсу, зокрема за типами постів (діапазонами), і порівняння його з наявними.

1.9. Прийняття рішення про продовження або закінчення розрахункової процедури на основі порівняння необхідного і наявного ресурсів, у тому числі за типами постів. У разі перевищення необхідного ресурсу над наявним – продовження розрахунку (за окремими типами постів наявний ресурс може бути достатнім – немає в потрібній кількості інформативних джерел, у цьому разі розрахункова процедура для даних постів завершена).

2. Формування k-го ... n-го планів розподілу ($D_{\text{ПП}k}$ $D_{\text{ПП}n}$).

2.1. Послідовний перебір усіх ДРВ із розрахунком за пп. 1.4, 1.5 і виключення з плану розподілу одного найменш інформативного джерела (із найменшим показником ефективності).

2.2. Виконання пп. 1.5–1.9 для k+1 плану.

2.3. Повторення процедур пп. 2.1, 2.2 до збігу необхідного ресурсу і наявного, в останньому випадку визначається необхідний РП розподілу.

Визначений (розрахований) план раціонального РСЗ РЕР є основою для розподілу на конкретні пости з урахуванням нормативних вимог.

Для ведення спостереження необхідно виділити: 25% джерел – на безперервне спостереження (для об'єктів 1-ї категорії з урахуванням їх важливості), 25% – на періодичне спостереження (для об'єктів 1-ї категорії, що залишилися, та об'єктів 2-ї категорії з урахуванням їх важливості). Решту джерел слід поставити на контрольне спостереження.

На пошук потрібно виділяти пости з урахуванням їх функціональної спеціалізації.

Розрахунки, проведені за розробленою методикою на основі Microsoft Office Excel, дозволили оцінити розвідувальну (інформаційну) доступність перспективної системи зв'язку мотострілецької дивізії ЗС РФ. Показник розвідувальної (інформаційної) доступності основних джерел РЕР становив 0,7–0,8.

Висновки. Розроблена методика може бути застосована на КП військової частини (підрозділів) РЕР, що дозволить розробляти адекватні поставленим завданням плани розподілу ресурсу для підвищення ефективності організації та планування ведення РЕР елементами системи, а також оцінювання їх можливостей.

Використання даної методики із застосуванням спеціального програмного забезпечення дозволить підвищити оперативність розрахунку сил і засобів, знизити кількість залучених офіцерів КП військових частин (підрозділів) РЕР і забезпечити оперативне коректування планів РЕР у ході вирішення розвідувальних завдань особливо в оперативний період (з урахуванням втрат своїх сил і засобів під час бойових дій, а також ураження об'єктів противника).

Напрямками подальших досліджень автори вбачають удосконалення методологічного апарату розвитку системи РЕР, а саме методики розрахунку ОР і ДРВ в органах управління розвідки та військових частинах (підрозділах) РЕР, а також розробку розвідувально-інформаційної моделі управління силами і засобами добування й обробки розвідувальної інформації.

СПИСОК ЛІТЕРАТУРИ

1. Варламов І. Д., Гаценко С. С., Бучинський Ю. А. Особливості побудови та практичної реалізації автоматизованої системи управління розвідкою // Труди університету. Київ : НУО України, 2017. № 6 (145). С. 44–54. Інв. № 1923т. – ЖВІ.

2. Небога О. В., Кокорін В. О., Цвєтков Є. В. Розвідувальне забезпечення антитерористичної операції: інформаційно-аналітичний матеріал. Київ : НУО України, 2015. 17 с.

3. Автоматизована система підтримки прийняття рішення щодо визначення типів джерел радіовипромінювань / І. Д. Варламов, М. А. Роговець, С. С. Гаценко, Ю. А. Бучинський. // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2017. Вип. 14. С. 146–156.

4. Калашніков Є. М., Гаценко С. С., Шишацький А. В. Аналіз характеру сучасних воєнних конфліктів // International scientific and practical conference ("Challenges of hybrid war: information dimension" : conference proceedings, Vilnius, August 16–17, 2019). Vilnius : Izdevnieciba «Baltija Publishing». P. 24–27.

5. 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 наук.-практ. семінару "Основні напрямки застосування космічних систем та геоінформаційного забезпечення в інтересах національної безпеки і оборони". Київ : НУО України, 2015. С. 35–41.

6. Сницаренко П. М. Методические основы обоснования требований к военным системам дистанционного мониторинга окружающего пространства для выявления

и сопровождения подвижных объектов при условии ресурсных ограничений на их создание // Прикладная радиоэлектроника. 2010. Т. 9, № 2. С. 185–192.

7. Method of Immunity Minimization of the Free Platform ed Inertial Navigation System of Unmanned Aircrafts / R. Bieliakov, S. Hatsenko, O. Fesenko et al. // 2nd Ukraine Conference on Electrical and Computer Engineering (Lviv, Ukraine, July 2–6, 2019). P. 803–808.

8. Development of a method of fuzzy evaluation of information and analytical support of strategic management / I. Alieinykov, K. Thamer, Y. Zhuravskyi et al. // Eastern-European Journal of Enterprise Technologies. 2019. Vol. 6, No. 2 (102). P. 16–27. DOI: https://doi.org/10.15587/1729-4061.2019.184394.

9. Застосування інформаційних систем для аналізу радіоелекторонної обстановки / Ю. І. Радковець, В. А. Шуренок, М. А. Роговець, Р. В. Дзюбчук // Вісник військової розвідки. Київ : ОІР НУО України, 2008. № 17. С. 47–56. Інв. 656т – ЖВІ.

10. Шуренок В. А. Методика оцінки космічної обстановки на базі нечіткої логіки // Зб. наук. праць Військ. ін-ту Київськ. нац. ун-ту ім. Тараса Шевченка. Київ : ВІКНУ, 2003. Спецвип. С. 191–203.

11. Гаценко С. С. Методика оцінювання оперативної обстановки в автоматизованих системах управління військами в умовах невизначеності // Наука і техніка Повітряних Сил ЗС України. 2017. № 1 (26). С. 101–105.

12. Гаценко С. С. Інформаційна система оцінювання оперативної обстановки в умовах невизначеності // Труди університету. Київ : НУО України, 2017. № 1 (140). С. 157–165. Інв. № 47522т – НУО України.

13. Шишацький А. В., Бігун Н. С., Гаценко С. С. Проблеми забезпечення інформаційної безпеки держави в умовах ведення гібридних війн // Тези доповідей наук.-практ. конф. «Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн» (м. Житомир, 24–25 жовтня 2019 року). Житомир : ЖВІ, 2019. С. 155–159.

14. Гаценко С. С. Методика раціонального розподілу розвідувальної інформації за важливістю та кількістю розвідувальних ознак в умовах невизначеності // Зб. наук. праць НДІ ГУР Міністерства оборони України. Київ, 2017. № 43. С. 111–120. Інв. № 47703 – НУО України.

15. Молитвин А. О реализации концепции единого информационного пространства НАТО // Зарубеж. воен. обозрение. 2008. JVb 1. С. 39

16.Справочник по вооруженным силам иностранных государств. Минск : ГРУ ГШ, 2012.С. 79–98.

17. Бабуль В. Л., Гулич А. А. Оперативно-информационная подготовка. Система управления и РТО тактических соединений ВС США и ОВС НАТО. Силы, средства и боевые возможности по ведению Р и РЭБ дивизий США : учеб пособ. : в 5 ч. Минск : ВА РБ, 2007. Ч. IV. 124 с.

18. Field Manual № FM 6-02 53. Tactical Radio Operations. Washington, DC, 5 August 2009.

19. Field Manual № FM16-02.70 JNN. Washington, DC, 5 Expires, 5 September 2008.

20. Пермяков О. Ю., Варламов І. Д., Гаценко С. С., Панкратова О. С. Удосконалення автоматизованих систем управління військами на основі раціонального розподілу інформаційних потоків в інтегрованому командному середовищі // Тези доповідей XX Всеукр. наук.-практ. конф. «Проблеми створення, розвитку та застосування

високотехнологічних систем спеціального призначення» (28 листоп. 2014, м. Житомир). Житомир : ЖВІ, 2014. С. 49–50.
21. Гаценко С. С. Аналіз існуючого стану автоматизованих систем управління військами Збройних Сил України та шляхи їх удосконалення // Зб. наук. праць Центру воєн.-стратег. досліджень НУОУ ім. Івана Черняховського. Київ, 2015. № 2 (54). С. 85–90.
22. Гаценко С. С., Кальницький Ю. М., Гельвейчук О. М. Проблема розподілу інформаційних потоків в автоматизованих системах управління військами (силами) Збройних Сил України // Зб. наук. праць Центру воєн.-стратег. досліджень НУО України ім. Івана Черняховського. Київ, 2014. № 2 (51). С. 107–111.
23. Поколения: дистанционные и бесконтактные. Москва : ОЛМА-ПРЕСС образование, 2004. 382 с.
24. Сетецентрическая война. Дайджест по материалам открытых изданий и СМИ. Москва : ВАГШ ВС РФ, 2010. 100 с.
25. Савин Л. В. Сетецентричная и сетевая война. Введение в концепцию. Москва : Евразийское движение, 2011. 130 с.
26. Кондратьев А. Сетецентрический фронт. Боевые действия в едином информационном пространстве // Национальная оборона. 2011. № 2. С. 10–18.
27. Шеремет И. А. Концепция «сетецентричной войны» и особенности ее практической реализации // НВО. 2005 (11 ноября). URL: http://nvo.ng.ru/ concepts/2005-11-11/4_computers.html (дата обращения: 01.12.2019).
28. Трахтенгерц Э. А., Пащенко Ф. Ф. Сетецентрические методы управления в крупномасштабных сетях. Москва : ЛЕНАНД, 2016. 200 с.
29. Організація системи управління (пункти управління та вузли зв'язку) та зв'язку військ ЗС РФ, що беруть участь у збройному конфлікті на Сході України : довідник. Київ : ГУР МО України, 2019. 31 с.
30. Об'єкти розвідки та джерела розвідувальних відомостей : навч. посіб. / М. Ф. Пічугін та ін. Житомир : ЖВІ НАУ, 2009. 340 с.
31. Інструкція з організації та ведення радіоелектронної розвідки в Міністерстві оборони України та Збройних Силах України. Київ : ГУР МО України, 2016. 52 с. Інв. № 1515–ЖВІ.
32. Інструкція з ОІР у з'єднаннях (військових частинах) РЕР. Київ : ГУР МО України, 2004. 59 с. Інв. № 585т – ЖВІ.
33. Гончаров Ю. И. Теоретические основы радио и радиотехнической разведки. Ленинград : ВАС, 1989. 374 с.
34. Радіоелектронна розвідка: пошук та спостереження : навч. посіб. Київ : НУО України, 2017. 200 с.
35. Ивахненко А. Г., Юрачковский Ю. П. Моделирование сложных систем по экспериментальным данным. Москва : Радио и связь, 1987. 118 с.
36. Про затвердження Тимчасової настанови з оперативної розвідки : наказ нач-ка Генерального штабу – Головнокомандувача Збройних Сил України від 05.07.2016 № 09. Київ : МО України, 2016. 178 с. Інв. № 47264т – НУО України.
37. Тынкевич М. А. Экономико-математические методы (исследование операций). Кемерово : КГТУ, 2000. 200 с.

Подано 30.12.2019

С. С. Гаценко, Е. Н. Коутный, В. В. Шипитко, Д. О. Грибовский, А. Н. Максименко

МЕТОДИКА РАЦИОНАЛЬНОГО РАСПРЕДЕЛЕНИЯ СИЛ И СРЕДСТВ РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ ПО ЗАДАЧАМ, ОБЪЕКТАМ И ИСТОЧНИКАМ МОНИТОРИНГА ДЛЯ ОПЕРАТИВНО-ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ

Вооруженная агрессия Российской Федерации против Украины, потеря таких 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 радиоэлектронной разведки как одного из главных технических видов военной разведки Украина.

Радиоэлектронная разведка Вооруженных Сил Украины – это комплекс мер и действий по добыванию разведывательной информации о вооруженных силах других государств через выявление функционирования радиоэлектронных средств и систем, применяемых для управления войсками (силами) и оружием, а также для сбора, обработки, анализа и доведения этой разведывательной информации определенным потребителям в установленные сроки.

Целью ведения радиоэлектронной разведки является своевременное и гарантированное выявление на ранней стадии признаков возникновения непосредственной угрозы безопасности Украины со стороны разведываемых государств (блоков, коалиций), а также добывание разведывательной информации для эффективной подготовки и применения Вооружённых Сил Украины.

Для достижения изложенной цели функционирует система радиоэлектронной разведки, которая представляет собой совокупность взаимосвязанных и согласованных в своих действиях по задачам, месту и времени органов управления радиоэлектронной разведки всех звеньев, сил и средств воинских частей (подразделений) радиоэлектронной разведки, которые выполняют определенные разведывательные задания по единому замыслу и плану.

Разведывательные задачи и объекты разведки воинским частям (подразделениям) радиоэлектронной разведки определяют с учетом их назначения, наличия сил и средств, а также их возможностей.

Важным элементом планирования радиоэлектронной разведки как в мирное время, так и на оперативный период является рациональное (целесообразное) распределение сил и средств радиоэлектронной разведки в военной части радиоэлектронной разведки осуществляется по заданиям, объектами и источниками разведки.

В статье на основе анализа проблем распределения ресурса сил и средств по задачам, объектам и источникам радиоэлектронной разведки как основного элемента планирования на командных пунктах воинских частей (подразделений) радиоэлектронной разведки обоснована структура частичной методики рационального распределения сил и средств для органов оперативно-тактического звена управления. В основе методики лежит системный подход к организации разведки с учетом требований адекватности по структурному и функциональному образу при моделировании взаимосвязей задач,

объектов и источников разведки. Основное назначение методики – разработка планов распределения ресурса с целью повышения эффективности ведения радиоэлектронной разведки элементами системы и оценивания их возможностей.

Ключевые слова: *система радиоэлектронной разведки; цель, объекты, источники разведки; эффективность; вероятность; план разведки; распределение сил и средств.*

S. S. Hatsenko, Y. M. Koutnyi , V. V. Shypitko, D. O. Hrybovskyi, O. M. Maksymenko

METHODOLOGY OF THE RATIONAL DISTRIBUTION OF FORCES AND MEANS OF RADIOELECTRONIC INTELLIGENCE ON THE TASK, OBJECT AND RESEARCH SOURCES FOR THE OPERATIONAL AND TACTICAL CONTROL LINK

Armed aggression of the Russian Federation against Ukraine, loss of important industrial potentials, as Topaz State Joint Stock 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 anti-aircraft anti-aircraft systems Kolchuga radio intelligence provided a significant impetus for the development of radio electronic intelligence (EER) as one of the main, technical types of military intelligence Of Ukraine. Radio-electronic Intelligence of the Armed Forces of Ukraine is a set of measures and actions for obtaining intelligence on the armed forces of the reconnaissance states through exposing the functioning of radio-electronic means (PE3) and systems used for the control of troops (forces) and weapons, collection, processing, analysis and bringing this intelligence to specific consumers within the prescribed timeframe. The purpose of the EED is to expose early and guaranteed early warning signs of an imminent threat to the security of Ukraine by the reconnaissance states (blocs, coalitions), as well as to obtain intelligence for the effective preparation and use of the Armed Forces of Ukraine. To achieve the objective of the ERD, the ERD system is functioning, which is a set of interrelated and coordinated in their actions by the tasks, place and time of the ERD governing bodies of all units and forces and means of the military units (units) of the ERF OSF that perform certain intelligence tasks on a single purpose. and plan. Intelligence tasks and reconnaissance objects for the military units (units) of the EWP OSR are determined taking into account their purpose, availability of forces and capabilities and their capabilities. An important element of the planning of the EER, both in peacetime and in the operational period, is the rational (expedient) distribution of EER forces and resources in the military unit of the EOM in the tasks, objects and sources of intelligence. In the article, based on the analysis of problems of distribution of the resource of forces and means by tasks, objects and sources of radio-electronic intelligence, as the basic element of planning on command posts of military units (units) of the ER, the structure of partial distribution methodology for the organs of operational-tactical control unit is substantiated. The methodology is based on a systematic approach to the organization of intelligence, taking into account the requirements of adequacy in structural and functional image in modelling the relationship of tasks, objects and sources of intelligence. The main purpose of the methodology is to develop resource allocation plans to improve the efficiency of conducting electronic reconnaissance by system elements and to evaluate their capabilities.

Keywords: *electronic intelligence system; target, objects, sources of intelligence; efficiency; probability; intelligence plan; distribution of forces and means.*

УДК 004.056.5 DOI: 10.46972/2076-1546.2019.17.16

В. В. Охрімчук

МЕТОД ПОБУДОВИ ШАБЛОНІВ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ КІБЕРАТАК

На сьогодні у світі спостерігається суттєве збільшення кількості кібератак. При цьому пропорційно зростає їх технологічна складність. У найближчому майбутньому не виключається поява нових потенційно небезпечних кібератак, що, у свою чергу, може призвести до погіршення їх виявлення й нейтралізації та, як наслідок, негативно вплинути на рівень захищеності інформаційних та інформаційно-телекомунікаційних систем критичної інформаційної інфраструктури. З урахуванням зазначеного у статті вирішується актуальне завдання розроблення достовірного методу побудови шаблонів потенційно небезпечних кібератак, упровадження якого забезпечить усунення базового недоліку створення сигнатур шаблонів атак, а саме "ефекту запізнення" з вироблення потрібної сигнатури. В основу запропонованого методу покладено визначення ключових характеристик і параметрів потенційно небезпечної кібератаки, яке здійснюється на підставі аналізу стандартного функціонального профілю захищеності, реалізованого в комп'ютерній системі та мережі, а також джерел первинних даних, які використовуються для побудови шаблонів потенційно небезпечних кібератак. Результатом практичного застосування зазначеного методу є побудова двох шаблонів потенційно небезпечної кібератаки на комп'ютерну систему та мережу. Перший – диференційно-ігровий шаблон потенційно небезпечної кібератаки, що описує фізику процесів, які відбуваються в комп'ютерній системі та мережі під час проведення потенційно небезпечної кібератаки. Другий – фізичний шаблон, що містить у собі повний набір характеристик та параметрів, характерних цій атаці.

Ключові слова: *метод; вразливість; кібератака; кіберзагроза; комп'ютерна система та мережа; система інформаційної безпеки; сигнатура; стандартний функціональний профіль захищеності; шаблон потенційно небезпечної кібератаки.*

Постановка проблеми в загальному вигляді. Широке застосування комп'ютерних систем та мереж (КСМ) у різних сферах, наприклад, економічній, військовій, енергетичній, транспортній тощо, суттєво впливає на ефективність діяльності не тільки окремо взятої людини, але й суспільства та держави в цілому. Проте окрім усіх позитивних ефектів від впровадження КСМ у діяльність сучасного суспільства суттєво й не в кращий бік змінюється ситуація щодо їх безпеки [1, 2]. Так, сьогодні найбільшу небезпеку для них становлять кібератаки (КбА). Актуальність даної проблеми підтверджується статистичними даними за 2018–2019 рр. [1]. До того ж не тільки збільшується їх кількість, а й зростає технологічна складність таких атак. Це, у свою чергу, призводить до погіршення їх виявлення та нейтралізації, що негативно впливає на рівень захищеності КСМ. Відомі на даний час технології, покладені в основу функціонування систем інформаційної безпеки (СІБ) (антивірусних СІБ, систем виявлення КбА), ґрунтуються на використанні сигнатурного методу виявлення КбА. Це, відповідно, призводить до появи так званого "ефекту запізнення", який виникає через часові затримки,

зумовлені технологічною процедурою розроблення потрібного шаблону (сигнатури) КбА тільки після її виявлення та нейтралізації, що суттєво знижує захищеність КСМ від нових потенційно небезпечних атак, особливо тих, які мають високу технологічну складність.

Отже, завдання виявлення та нейтралізації потенційно небезпечних КбА на КСМ набуває особливої актуальності та може бути вирішене шляхом розроблення нових дієвих та модифікацією відомих методів побудови шаблонів КбА.

Аналіз останніх досліджень і публікацій [1–8] показав, що, незважаючи на значну кількість КСМ, проблема їх безпеки й надалі залишається актуальною, з нею також пов'язані питання технологічного [9], організаційного [10], дефініційного [11] характеру тощо.

У технологічному сенсі сьогодні відбувається комплексування відомих підходів до побудови сигнатур шаблонів атак. Кожен із провідних вендорів антивірусного програмного забезпечення, зокрема Kaspersky Lab, Panda Security, Intel Security-McAfee, ESET, Dr.Web Dr.Web тощо, тримає в комерційній таємниці способи побудови шаблонів атак. Інші відомі підходи, висвітлені в [12, 22], в кожному окремому випадку потребують адаптації.

Організаційна складова проблеми безпеки КСМ обумовлена суперечностями між усталеними у світовій практиці підходами до організації процесу забезпечення захищеності та їх повільною ратифікацією не тільки в межах України, а й усіх країн пострадянського простору.

Дефініційна проблема безпеки є відлунням організаційної. Навіть провідні вчені в галузі безпеки КСМ на сьогодні не мають єдиного бачення на вирішення питання забезпечення технічного захисту інформації на об'єктах інформаційної діяльності, безпеки інформаційних і комунікаційних систем, інформаційної та кібернетичної безпеки як окремої складової безпеки КСМ, так і безпеки системи в цілому.

Як показав критичний аналіз відомих публікацій за темою дослідження, означена вище проблема, незважаючи на її багатогранність, і досі залишається актуальною та потребує свого розв'язання.

Формулювання завдання дослідження. Метою статті є створення достовірного методу розроблення шаблону потенційно небезпечних КбА, що забезпечить відкриття нового дієвого механізму підвищення захищеності КСМ різного цільового призначення.

Виклад основного матеріалу. *Твердження*. Під потенційно небезпечною КбА будемо розуміти таку, яка призводить до порушення нормального функціонування КСМ та, як наслідок, ускладнює або унеможливлює виконання нею завдань за призначенням. При цьому вважається, що відомості про таку КбА в базах даних сигнатур СІБ відсутні.

Зазвичай будь-яка КбА характеризується наявністю невід'ємних складових, які необхідні для досягнення її мети, а саме [13]:

джерело (суб'єкт) атаки – зловмисник, шкідливе програмне забезпечення, за рахунок якого здійснюється КбА;

наявні в КСМ та її компонентах вразливості та варіанти їх використання;

об'єкт КбА, яким можуть бути ресурси КСМ та її компоненти.

Саме визначивши ці складові, можливо буде з високою ймовірністю стверджувати про проведення КбА на КСМ. Отже, метод розроблення шаблонів потенційно

небезпечних КбА повинен бути направлений на визначення їх ключових характеристик і параметрів та містити певні кроки.

Крок 1. Усебічне дослідження та аналіз КСМ

Для розроблення шаблону потенційно небезпечної КбА на першому етапі необхідно визначити її клас та всю множину ресурсів КСМ і її компонентів, які потенційно можуть бути атаковані. З цією метою слід проаналізувати стандартний функціональний профіль захищеності (СФПЗ), реалізований у КСМ. Це в першу чергу пов'язано з тим, що він реалізований для підтримання функціональних спроможностей КСМ, виведення з ладу яких призведе до неможливості використовувати її за призначенням. У результаті дослідження СФПЗ КСМ отримаємо ймовірний клас потенційно небезпечної КбА та множину ресурсів, які потенційно можуть бути атаковані.

Отже, як відомо з [14], СФПЗ – це перелік мінімально необхідних послуг, який повинен реалізовувати комплекс засобів СІБ КСМ, щоб відповідати визначеним вимогам щодо захищеності інформації, яка обробляється в даній КСМ. Таким чином, СФПЗ *A*, враховуючи зазначене припущення, можна подати в такому вигляді [15]:

$$A = \{a_1, a_2, ...a_\alpha\}, \tag{1}$$

де a_α – мінімально необхідна послуга безпеки, причому $6 \le |A| \le 24$.

Такий діапазон показників обумовлений кількістю мінімально необхідних послуг безпеки, що формують СФПЗ. Відповідно до [14] їх кількість варіюється від 6 до 24 для одного СФПЗ. Як відомо, послуга a_α може включати декілька рівнів. Чим вищий рівень послуги, тим більш повно вона забезпечує захист від певного класу кіберзагроз. Отже, на основі аналізу СФПЗ та його мінімальних необхідних послуг безпеки можливо визначити клас потенційно небезпечної КбА. Це пов'язано з тим, що виведення з ладу однієї з послуг СФПЗ може призвести до порушення функціонування КСМ, тобто до успішного проведення КбА. Якщо основною функцією КСМ є забезпечення доступності користувачів до її ресурсів, то і СФПЗ буде сформований таким чином, щоб її захистити, а отже, і клас потенційно небезпечної КбА повинен бути направлений на порушення цієї доступності.

Кожна послуга є набором функцій, що реалізуються певними ресурсами КСМ, метою яких є протидія визначеній множині загроз. Отже, як було зазначено вище, враховуючи невід'ємні характерні компоненти КбА, для успішного проведення потенційно небезпечної атаки необхідно порушити нормальне функціонування ресурсів КСМ, які забезпечують ту чи іншу мінімально необхідну послугу безпеки СФПЗ.

Таким чином, враховуючи зазначене припущення, з усієї множини ресурсів КСМ $R = \{r_1, r_2, ..., r_k\}$, де k – кількість її ресурсів, можливо визначити підмножину ресурсів R', які можуть бути потенційно атаковані. Як було вказано в [16], будь-який k-й ресурс КСМ r_k можна описати кортежем як

$$r_k = \langle r_k, A_r, V_r, Ch_r \rangle, \tag{2}$$

де r_k – k-й ресурс КСМ;

A_r – множина мінімально необхідних послуг безпеки СФПЗ A, функціонування яких залежить від даного ресурсу, причому $A_r \subseteq A$ та $0 \le |A_r| \le 24$;

V_r – множина вразливостей даного ресурсу;

Ch_r – множина його параметрів та характеристик.

Отже, множина ресурсів R', які можуть бути потенційно атаковані, формується з ресурсів, у яких виконується така умова:

$$|A_r| \neq 0. \tag{3}$$

Тобто обраний ресурс повинен забезпечувати функціонування хоча б однієї мінімально необхідної послуги a_α СФПЗ A.

З урахуванням наведеного вище множина ресурсів КСМ, які можуть бути потенційно атаковані, набуває такого вигляду:

$$R' = \left\{ \left\langle r_k, A_r, V_r, Ch_r \right\rangle \mid r_k \in R, A_r \subseteq A, |A_r| \neq 0 \right\}. \tag{4}$$

У результаті виконання першого кроку методу розроблення шаблонів потенційно небезпечних КбА отримаємо необхідні вихідні дані, які будуть використані на наступних кроках.

Крок 2. Визначення джерел первинних даних для побудови шаблонів потенційно небезпечних КбА

Сьогодні у світі існує достатньо велика кількість вендорів СІБ, що займаються моніторингом, класифікацією та накопиченням відомостей про кіберзагрози. Кожна така організація надає, як правило, відкритий доступ до своїх власних баз кіберзагроз, які заповнюються різноманітною інформацією на свій розсуд. Це призводить до дисбалансу форматів подання первинних даних. Як наслідок, ускладнюються технології їх використання для створення шаблонів КбА. Крім того, дані від таких джерел не завжди комплексуються, що спричиняє нехтування низкою важливих інформативних характеристик, які описують КбА.

Детальний аналіз найбільш поширених баз первинних даних для побудови шаблонів потенційно небезпечних КбА наведено в [17]. Враховуючи ключові складові КбА [13, 16], усі відомі бази даних про них можна поділити на три великі категорії: ті, що характеризують середовище атаки; які описують об’єкт КбА та характеризують суб’єкт атаки.

Як показує практика, для опису середовища атаки найбільшого поширення набула база шаблонів атак KDD-99 [18], що містить $5 \cdot 10^6$ шаблонів мережевих з’єднань, які описують нормальну та аномальну поведінку трафіка в КСМ.

За бази даних, що характеризують суб’єкт атаки, доцільно використовувати ті, які містять у собі опис вразливостей ресурсів КСМ. Однією з найпоширеніших є база даних загальновідомих вразливостей інформаційної безпеки Common Vulnerabilities and Exposures (CVE) [19]. Вона містить множину відомих вразливостей програмних засобів КСМ та СІБ V_{CVE}.

Для опису суб'єкта атаки доцільно використовувати бази даних, які містять у собі шаблони дій зловмисника. Прикладом є база шаблонів КбА CAPEC (Common Attack Pattern Enumeration and Classification) компанії MITRE [20].

Для обрання з усієї множини відомих баз даних необхідно скористатися двома правилами: мінімальна кількість баз даних, які обираються як джерела первинних даних для розроблення шаблонів потенційно небезпечних КбА, має відповідати кількості її складових; обрані бази даних повинні мати максимальну інформативність про складові КбА.

Отже, у результаті виконання другого кроку отримаємо множину баз даних, які будуть використані як джерела первинних даних для розроблення шаблонів потенційно небезпечних КбА.

Крок 3. Оптимізація вихідних даних, необхідних для побудови шаблонів потенційно небезпечних КбА

Оптимізація вихідних даних здійснюється з метою відбору з усієї множини вхідних даних, необхідних для побудови шаблону потенційно небезпечної КбА, конкретних показників та характеристик, що однозначно будуть її визначати.

Оптимізації підлягає кожне джерело первинних даних, обране в ході виконання другого кроку.

Так, якщо для опису станів мережевого трафіка використовують базу KDD-99, то мережевий трафік є набором s вхідних інформативних параметрів, які підлягають контролю, $s=\overline{1,41}$ [21]. В умовах обмеженого часу на побудову шаблону потенційно небезпечної КбА використання визначеної кількості із s параметрів не є раціональним підходом. Доцільним у такому разі є оптимізувати кількість параметрів із s до s', де $s' \le s$. Дане припущення є справедливим, оскільки в [22] визначено найбільш інформативні параметри для усіх класів КбА та доведено, що кожен із відомих, а відповідно, і невідомих класів КбА може бути описаний своєю множиною з s' параметрів, які його чітко визначають.

Метою оптимізації множини ресурсів КСМ, які можуть бути потенційно атаковані R', є виокремлення тих, на які можуть бути спрямовані протиправні дії зловмисника.

Оскільки кожний ресурс $r_k \in R'$ можна подати у вигляді (2), то множина ресурсів, які потенційно можуть бути атакованими, являтиме собою відношення R'', задане на декартовому добутку множин ресурсів КСМ R', та відомих вразливостей V_{CVE} [23]. У формалізованому вигляді воно може бути представлене булевою матрицею суміжності:

R''	v_1	v_2	v_3	$\cdots$	v_n
r_1	1	0	1	$\cdots$	1
r_2	0	0	0	$\cdots$	1
r_3	0	0	1	$\cdots$	1
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$r_{\text{я}}$	1	1	0	$\cdots$	0

. (5)

Таким чином, множина R'' містить упорядковані пари (5). Першим елементом впорядкованої пари є ресурс r_k множини R', що має вразливість, а другим – відповідна цьому ресурсу вразливість $v_n \in V_{CVE}$, тобто

$$R'' \subseteq R' \times V_{CVE} = \{\langle r_k, v_n, Ch_r \rangle \mid r_k \in R', v_n \in V_{CVE}, r_k R'' v_n\}. \quad (6)$$

Така оптимізація дає змогу розглядати два можливі варіанти проведення потенційно небезпечної КбА: перший – атака зловмисника буде націлена на ресурс r_k, який матиме максимальну кількість вразливостей; другий – зловмисник для здійснення потенційно небезпечної КбА буде використовувати вразливість, притаманну максимально можливій множині ресурсів R''.

Оптимізацію параметрів множини вхідних даних, що описують суб'єкт атаки, здійснюють шляхом обрання параметрів, які характеризують дії зловмисника, потенційно можливі для експлуатації обраної вразливості чи здійснення КбА на визначений ресурс.

Отже, у результаті виконання третього кроку отримаємо усі необхідні дані для побудови шаблону потенційно небезпечної КбА.

Крок 4. Побудова шаблонів потенційно небезпечних КбА

На четвертому кроці безпосередньо створюють два шаблони потенційно небезпечної КбА на КСМ. Перший – диференційно-ігровий, він описує фізику процесів, що відбуваються в КСМ під час проведення потенційно небезпечної КбА. Другий – фізичний шаблон, що містить у собі повний набір характеристик та параметрів, притаманних цій атаці.

Для побудови першого шаблону потенційно небезперечної КбА застосуємо диференційно-ігровий метод, описаний у [12]. Для кожного ресурсу $r_k \in R''$ необхідно визначити множину станів, у яких вони можуть перебувати під час здійснення КбА, та проаналізувати переходи з одного стану в інший. За результатами аналізу необхідно побудувати диференційно-ігровий граф шаблону потенційно небезпечної КбА. Опис отриманого графа здійснюється за допомогою диференційних перетворень [24, 25]. Отже, практичне використання диференційно-ігрового шаблону потенційно небезпечної КбА дозволяє вивчати процеси кіберзахисту та кібернападу в КСМ за різних вхідних даних, не проводячи натурного експерименту через його потенційну небезпеку для об'єкта.

Фізичний шаблон потенційно небезпечної КбА формується на основі показників та параметрів, оптимізованих під час виконання кроків 1–3 цього методу, та моделі шаблону потенційно небезпечної КбА, описаної в [16].

У загальному вигляді запропонований метод побудови шаблонів потенційно небезпечної КбА можна подати у вигляді структурної схеми, зображеної на рис. 1. Виконання кроків 1–4 дає змогу встановити факт проведення потенційно небезпечної КбА. Для її виявлення та нейтралізації розроблений метод слід доповнити ще одним кроком (крок 5) (див. рис. 1), який виходить за межі даного дослідження. Метою даного кроку є класифікація потенційно небезпечної КбА.

На сьогодні відомо багато різних підходів до класифікації КбА [26–29]. Вважається, що найбільш повним та систематизованим варіантом, який застосовують на практиці для вирішення низки прикладних завдань, є узагальнена класифікація КбА, розроблена в [27] та подана у формалізованому вигляді в [30]. Перевагою обраного підходу є застосування ознакового принципу для опису різних класів КбА, який забезпечує опис не тільки відомих на сьогодні класів атак, а й дозволяє розширювати ознаковий простір для опису нових, невідомих і, відповідно, потенційно небезпечних класів.

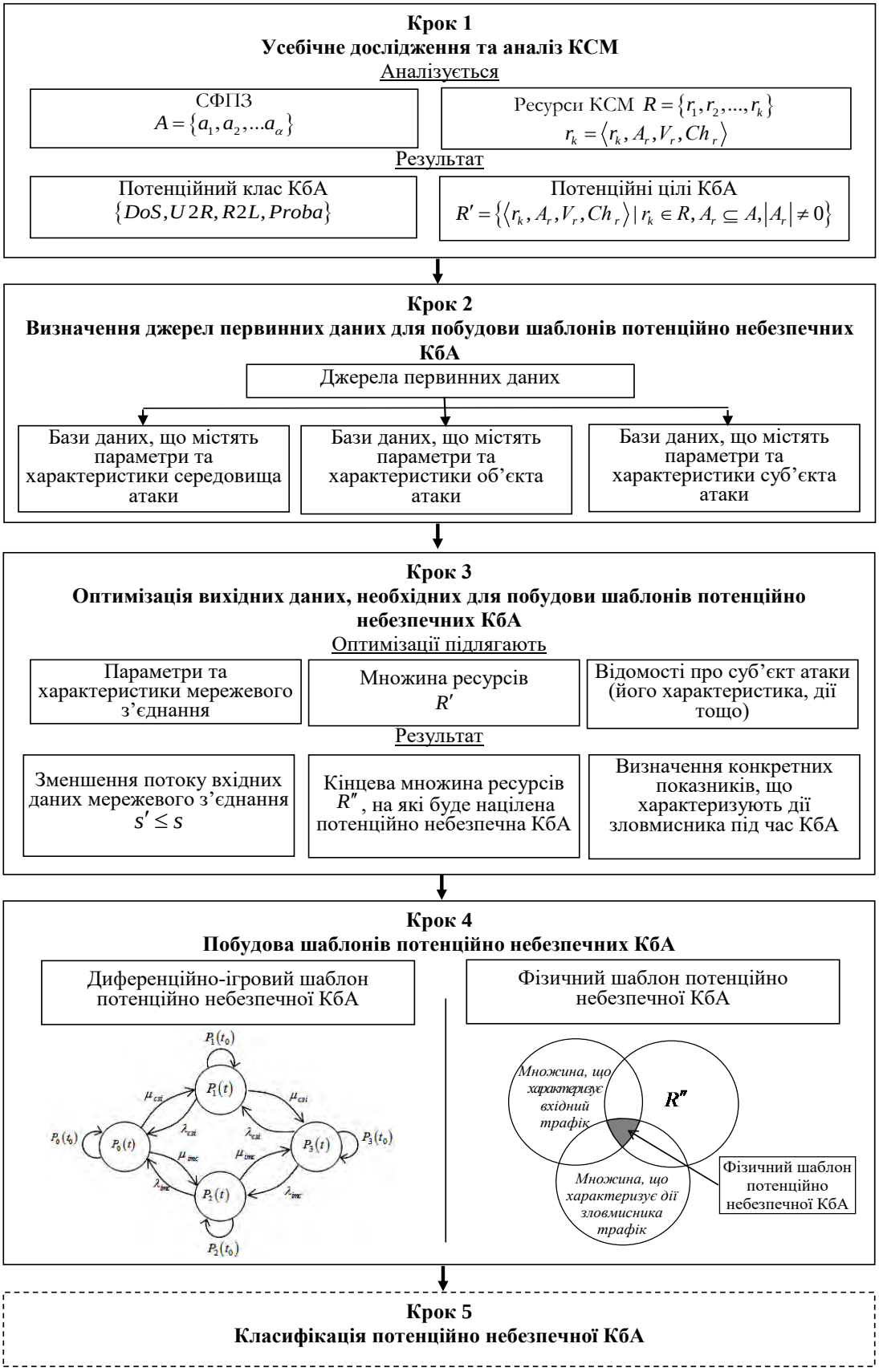


Рис 1. Структурна схема методу побудови шаблону потенційно небезпечної КбА

Висновки. Уперше запропоновано новий метод побудови шаблонів потенційно небезпечних КбА, який усуває базовий недолік відомих підходів – "ефект запізнення" в ході створення сигнатури. У його основу покладено визначення ключових характеристик

і параметрів потенційно небезпечної КбА, яке здійснюється на підставі аналізу стандартного функціонального профілю захищеності, реалізованого в КСМ, та джерел первинних даних, які використовуються для побудови шаблонів потенційно небезпечних КбА. У результаті практичного застосування зазначеного методу побудовано два шаблони потенційно небезпечної КбА на КСМ. Перший – диференційно-ігровий, який описує фізику процесів, що відбуваються в КСМ під час проведення потенційно небезпечної КбА. Другий – фізичний шаблон, який містить у собі повний набір характеристик та параметрів, властивих цій атаці.

Перспективним напрямом подальших досліджень є розроблення достовірної методики класифікації потенційно небезпечних КбА на КСМ.

СПИСОК ЛІТЕРАТУРИ

1. Geers K. Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn : CCDCOE, 2015. 176 c.
2. Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах // Сучасна спеціальна техніка. 2011. № 1 (24). С. 61–66.
3. Олифер В. Г., Олифер Н. А. Безопасность компьютерных сетей. Москва : Горячая линия – Телеком, 2015. 644 с.
4. Звіт CERT-UA за 2010–2013 роки. URL: http://cert.gov.ua/?p=316 (дата звернення: 10.12.2019).
5. Киберщит Украины: кто стоит на страже кибергранниц страны. URL: http://zillya.ua/ru/kibershchit-ukrainy-kto-stoit-na-strazhe-kibergranits-strany (дата обращения: 23.12.2019).
6. Ларина Л., Овчинский В. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. Москва : Книжный мир, 2014. 352 с.
7. Lewis T. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. 2014. 400 p.
8. Ten C.-W. , Manimaran G., Liu C.-C. Cybersecurity for criticalinfrastructures: Attack and defense modeling // IEEETrans. Syst., Man Cybern. A. 2010. Vol. 40, No. 4. P. 853–865.
9. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность. Киев : Арий, 2008. 344 с.
10. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення. Київ : НАУ, 2011. 640 с.
11. Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22–27.
12. Грищук Р. В. Диференціально-ігрова модель шаблону атаки на Web-сервер // Зб. наук. праць ВІКНУ ім. Т. Шевченка. 2010. № 21. С. 104–112.
13. Шабуров А. С. О разработке модели обнаружения компьютерных атак на объекты критической информационной инфраструктуры // Вестник ПНИПУ. 2018. № 26. С. 198–213.
14. НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу” [Затверджено наказом Адміністрації Держспецзв’язку від 15.10.2008 № 172]. 16 с.
15. Грищук Р., Охрімчук В. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак // Безпека інформації. 2015. № 21 (3). С. 276–282.

16. Охрімчук В. Модель шаблону потенційно небезпечної кібератаки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.-техніч. зб. 2018. № 1 (35). С. 30–39.
17. Грищук Р. В., Охрімчук В. В., Ахтирцева В. С. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак // Захист інформації. 2016. № 1 (18). С. 21–29.
18. Khubeb Siddiqui M., Naahid S. Analysis of KDD CUP 99 Dataset using Clustering based Data Mining // International Journal of Database Theory and Application. 2013. Vol. 6, No. 5. P. 23–34.
19. Common Vulnerabilities and Exposures (CVE). URL: http://cve.mitre.org (last accessed: 10.12.2019).
20. Common Attack Pattern Enumeration and Classification. URL: https://capec.mitre.org. (last accessed: 15.12.2019).
21. UCI Knowledge Discovery in Databases Archive. URL: http://kdd.ics.uci.edu. (last accessed: 18.12.2019).
22. Грищук Р. В., Мамарєв В. М. Метод скорочення розмірності потоку вхідних даних для мережних систем виявлення атак // Сучасний захист інформації. Київ : ДУІКТ, 2012. Спецвипуск. С. 16–19.
23. Михалін Г. О., Дюженкова Л. І. Елементи теорії множин і теорії чисел. Київ : НПУ ім. М. П. Драгоманова, 2003. 128 с.
24. Пухов Г. Дифференциальные преобразования и математическое моделирование физических процессов : монография. Киев : Наук. думка, 1986. 160 с.
25. Грищук Р. Метод диференціально-ігрового Р-моделювання процесів нападу на інформацію // Інформаційна безпека. 2009. № 2 (2). С. 128–132.
26. Классификация Ховарда. URL: http://helpiks.org/4-76231.html (дата обращения: 23.12.2019).
27. Корченко О. Г. Системи захисту інформації : монографія. Київ : НАУ, 2004. 264 с.
28. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения : монография. Киев : “МК-Пресс”, 2006. 320 с.
29. Классификация деструктивных информационных воздействий и кибератак. URL: http://antitentura.blogspot.com/2014/07/blog-post_11.html (дата обращения 23.12.2019).
30. Cyberattack classificator verification / V. Okhrimchuk, R. Hryshchuk, V. Mamarev et al. // Advances in Intelligent Systems and Computing. 2017. № 635. P. 402.

Подано 30.12.2019

В. В. Охримчук

МЕТОД ПОСТРОЕНИЯ ШАБЛОНОВ ПОТЕНЦИАЛЬНО ОПАСНЫХ КИБЕРАТАК

Сегодня в мире наблюдается существенное увеличение количества кибератак. При этом пропорционально возрастает их технологическая сложность. В ближайшем будущем не исключено появление новых потенциально опасных кибератак, что, в свою очередь, может привести к ухудшению их обнаружения и нейтрализации, а также, как следствие, негативно повлиять на уровень защищенности информационных и информационно-телекоммуникационных систем критической информационной инфраструктуры. С учетом изложенного в статье решается актуальная задача

разработки достоверного метода построения шаблонов потенциально опасных кибератак, внедрение которого обеспечит устранение базового недостатка создания сигнатур шаблонов атак, а именно "эффекта опоздания" по выработке нужной сигнатуры. В основу предложенного метода положено определение ключевых характеристик и параметров потенциально опасной кибератаки, которое осуществляется на базе анализа стандартного функционального профиля защищенности, реализованного в компьютерной системе и сети, а также источников первичных данных, которые используются для построения шаблонов потенциально опасных кибератак. Результатом практического применения данного метода является построение двух шаблонов потенциально опасной кибератаки на компьютерную систему и сеть. Первый – дифференциально-игровой шаблон потенциально опасной кибератаки, который описывает физику процессов, происходящих в компьютерной системе и сети во время проведения потенциально опасной кибератаки. Второй – физический шаблон, который включает в себя полный набор характеристик и параметров, характерных этой атаке.

Ключевые слова: *метод; уязвимость; кибератака; киберугроза; компьютерная система и сеть; система информационной безопасности; сигнатура; стандартный функциональный профиль защищенности; шаблон потенциально опасной кибератаки.*

V. V. Okhrimchuk

THE METHOD OF DEVELOPMENT A TEMPLATES OF POTENTIALLY DANGEROUS CYBER-ATTACKS

Today the world is experiencing a significant increase in the number of cyberattacks. At the same time, their technological complexity increases proportionally. In the near future, the emergence of new potentially dangerous cyberattacks is not ruled out, which in turn may lead to deterioration of their detection and neutralization and, consequently, negatively affect the level of security of information and information and telecommunications systems of critical information infrastructure. Based on this, the article solves the urgent problem of developing a reliable method of constructing patterns of potentially dangerous cyberattacks, the implementation of which eliminates the basic disadvantage of creating attack pattern signatures, namely the "delay effect" to produce the desired signature. The proposed method is based on the definition of key characteristics and parameters of a potentially dangerous cyber-attack. It is based on an analysis of the standard functional security profile implemented in the computer system and network and the primary data sources used to build the patterns of potentially dangerous cyberattacks. The practical application of this method will result in the construction of two patterns of potentially dangerous cyber-attack on a computer system and network. The first, a differential game template for a potentially dangerous cyberattack, will describe the physics of processes occurring in a computer system and network during a potentially dangerous cyberattack, and the second, a physical template, will contain the full set of characteristics and parameters inherent in that attack.

Keywords*: method; vulnerability; cyber-attack; cyber threat; computer system and network; information security system; signature; standard functional security profile; pattern of potentially dangerous cyber-attack.*

Авсієвич Роман Олексійович – ад'юнкт науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– космічні системи;
– оптимізаційні процеси планування.

Березіна Світлана Іванівна – кандидат технічних наук, старший науковий співробітник, старший науковий співробітник науково-дослідного відділу Наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба.
Наукові інтереси:
– обробка даних дистанційного зондування Землі;
– геоінформаційні технології.

Бродський Юрій Борисович – кандидат технічних наук, доцент, завідувач кафедри Житомирського національного агроекологічного університету.
Наукові інтереси:
– інформаційні системи;
– моделювання систем різної фізичної природи.

Бугайов Микола Вікторович – кандидат технічних наук, старший науковий співробітник науково-дослідної лабораторії наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– математичні методи й алгоритми оброблення сигналів.

Воротніков Володимир Володимирович – доктор технічних наук, доцент, начальник кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– управління сучасних інформаційно-керувальних систем.

Гаценко Сергій Станіславович – кандидат технічних наук, заступник начальника кафедри Національного університету оборони України імені Івана Черняховського.
Наукові інтереси:
– інформаційні технології у сфері безпеки та оборони;
– підвищення ефективності ведення воєнної розвідки.

Гордієнко Юрій Олексійович – кандидат технічних наук, провідний науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– обробка спеціальної інформації.

Гордійчук Валерій Валентинович – кандидат технічних наук, начальник науково-організаційного відділення Інституту Військово-Морських Сил Національного університету «Одеська морська академія».
Наукові інтереси:
– захист інформації в телекомунікаційних системах;
– форми і способи застосування Військово-Морських Сил;
– організація наукових досліджень.

Грибовський Дмитро Олегович – слухач Командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняховського.

Наукові інтереси:
– нові форми та способи обробки інформації.

Дзюбенко Олександр Володимирович – старший науковий співробітник військової частини А1906.
Наукові інтереси:
– системні дослідження та інформаційні технології;
– системи інформаційної підтримки та прийняття рішень.

Дудник Володимир Петрович – кандидат військових наук, професор кафедри Національної академії сухопутних військ імені гетьмана Петра Сагайдачного.
Наукові інтереси:
– нові форми та способи застосування військ (сил);
– підвищення ефективності прийняття рішень.

Завада Андрій Анатолійович – провідний науковий співробітник науково-дослідної лабораторії наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– автоматизована обробка інформації в складних інформаційних системах.

Залевський Віктор Йосипович – науковий співробітник науково-дослідної лабораторії наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– космічні системи;
– охорона державної таємниці та захист інформації.

Запорожець Сергій Анатолійович – кандидат політичних наук, офіцер військової частитни А0515.
Наукові інтереси:
– інформаційна безпека, інформаційно-психологічні операції;
– державна політика, гібридна війна.

Зімчук Ігор Валерійович – кандидат технічних наук, доцент, доцент кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– алгоритми оцінювання та управління для сучасних інформаційно-керувальних систем.

Іщенко Володимир Іванович – кандидат технічних наук, доцент, викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– алгоритми оцінювання та управління для сучасних інформаційно-керувальних систем.

Ковальчук Сергій Валерійович – науковий співробітник військової частитни А1906.
Наукові інтереси:
– статистична радіотехніка.

Ковтун Сергій Олександрович – кандидат технічних наук, старший науковий співробітник, провідний інженер ТОВ «Науково-впроваджувальна фірма “КРИПТОН”».
Наукові інтереси:
– статистична радіотехніка, системні дослідження.

Колос Юрій Олександрович – кандидат технічних наук, доцент, доцент кафедри Житомирського військового інституту імені С. П. Корольова.

Наукові інтереси:
– синтез та аналіз антенно-фідерних пристроїв і систем.

Коутний Євген Миколайович – слухач Командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняховського.
Наукові інтереси:
– нові форми та способи застосування військ (сил);
– підвищення ефективності прийняття рішень у сфері розвідки.

Ліщенко Олександр Миколайович – слухач Командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняховського.
Наукові інтереси:
– нові форми та способи обробки інформації;
– підвищення ефективності прийняття рішень.

Максименко Олександр Миколайович – слухач Командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняховського.
Наукові інтереси:
– нові форми та способи обробки інформації.

Манько Олег Віталійович – начальник наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційно-аналітичні системи;
– обробка великих масивів даних;
– системи прийняття рішень.

Марищук Людмила Мічеславівна – молодший науковий співробітник науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційно-психологічна безпека;
– організація наукових досліджень.

Марченков Сергій Миколайович – начальник кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційні та психологічні операції, інформаційно-аналітична робота;
– національна безпека.

Михайлюк Ігор Олегович – слухач Національного університету оборони України імені Івана Черняховського.
Наукові інтереси:
– розвідувальні інформаційні системи та комплекси.

Миклуха Василь Анатолійович – ад'юнкт науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– безпілотні авіаційні комплекси;
– планування застосування безпілотних авіаційних апаратів;
– оптимізаційні процеси планування.

Молодецький Богдан Валентинович – кандидат технічних наук, начальник науково-дослідного відділу в/ч А1906.
Наукові інтереси:
– розроблення спеціалізованих інформаційних систем;
– автоматизоване оброблення інформації.

Нагорнюк Олександр Анатолійович – кандидат технічних наук, провідний науковий співробітник науково-дослідної лабораторії наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– методи цифрової обробки та розпізнавання радіосигналів;
– методи радіопеленгації;
– методи проєктування та дослідження антен.

Наумчак Олена Михайлівна – молодший науковий співробітник науково-дослідної лабораторії наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційно-психологічна безпека;
– психологічна стійкість до інформаційно-психологічних впливів.

Нетребко Руслан Васильович – викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційні технології;
– управління сучасних інформаційно-керувальних систем.

Охрімчук Володимир Васильович – старший викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– кібербезпека;
– інформаційна безпека держави.

Павленко Михайло Михайлович – старший науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– обробка великих масивів даних;
– автоматизована обробка інформації в складних інформаційних системах.

Перегуда Олександр Михайлович – кандидат технічних наук, старший науковий співробітник, начальник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– проєктування, розробка та експлуатація автоматизованих систем військового призначення.

Піонтківський Петро Миколайович – кандидат технічних наук, провідний науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– системи прийняття рішень в інформаційних системах військового призначення.

Ратушний Сергій Анатолійович – начальник курсу Національного університету оборони України імені Івана Черняховського.
Наукові інтереси:
– інформаційні технології.

Сидорчук Ольга Леонідівна – кандидат технічних наук, старший викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– радіоелектронний захист складних антенних систем;
– теоретичні дослідження електромагнітного поля;
– дослідження у сфері радіоелектронної розвідки та радіоелектронної боротьби.

Солонець Олексій Іванович – кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник науково-дослідного відділу Наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба.
Наукові інтереси:
– космічні забезпечувальні системи;
– обробка спеціальної інформації.

Сотніченко Андрій Іванович – слухач Командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняховського.
Наукові інтереси:
– нові форми та способи обробки інформації;
– підвищення ефективності прийняття рішень.

Топольницький Павло Петрович – кандидат технічних наук, доцент, доцент кафедри Житомирського національного агроекологічного університету.
Наукові інтереси:
– обробка інформації в інформаційно-вимірювальних системах.

Фриз Сергій Петрович – доктор технічних наук, доцент, начальник кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– дослідження телекомунікаційних і радіотехнічних систем спеціального призначення наземного, повітряного та космічного базування.

Черкес Олена Петрівна – науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– реляційні системи управління базами даних;
– проєктування та розробка інформаційних систем.

Шапар Тетяна Миколаївна – викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– аналіз та синтез систем управління.

Шипітко Володимир Васильович – слухач Командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняховського.
Наукові інтереси:
– інформаційні технології у сфері безпеки та оборони.

Н А У К О В Е В И Д А Н Н Я

ПРОБЛЕМИ СТВОРЕННЯ, ВИПРОБУВАННЯ, ЗАСТОСУВАННЯ ТА ЕКСПЛУАТАЦІЇ СКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Збірник наукових праць

Випуск 17

Видавничий оригінал виготовлений
у науково-організаційному відділенні ЖВІ

Редактор: **Л. М. Марищук**
Комп'ютерна верстка та макетування **Л. М. Марищук**

Свідоцтво про реєстрацію № 877 від 21 жовтня 2013 року.
Підписано до друку 30.12.2019. Формат 60 × 84 / 8.
Ум. друк. арк. 21,85. Тираж 100 прим. Зам. 834 офс.

Безкоштовно
Друкарня ЖВІ

10004, м. Житомир, пр-т Миру, 22