МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ ІМЕНІ С. П. КОРОЛЬОВА

ПРОБЛЕМИ СТВОРЕННЯ, ВИПРОБУВАННЯ, ЗАСТОСУВАННЯ ТА ЕКСПЛУАТАЦІЇ СКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

16

Житомир
2019

Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : збірник наукових праць. Вип. 16 / Житомирський військовий інститут імені С. П. Корольова. – Житомир : ЖВІ, 2019. – 180 с. – ISSN 2076-1546. https://doi.org/10.46972/2076-1546.2019.16.

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 № 01 від 12.09.2019.

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 629.7:355.45 DOI: 10.46972/2076-1546.2019.16.01

Ф. М. Андреєв, І. А. Беспалко, Д. М. Випорханюк, С. В. Ковбасюк

ОСНОВНІ ТЕНДЕНЦІЇ СВІТОВОЇ КОСМІЧНОЇ ДІЯЛЬНОСТІ В ІНТЕРЕСАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ

Останні десятиліття космос, як і суходіл, море, повітря та кіберпростір, став ареною суперництва потужних світових держав, що призвело до зміни природи дій у навколоземному космічному просторі низки країн. Наслідком космічної діяльності стало те, що географічне розташування перестало бути домінантою міжнародних відносин. Вітчизняна космічна діяльність, на жаль, не стала дієвим інструментом для досягнення геополітичних цілей України та забезпечення виконання завдань в інтересах національної безпеки й оборони. У зв'язку з цим актуальним є проведення аналізу сучасних тенденцій розвитку космічної діяльності у світі в безпековому секторі, результати якого повинні стати основою запровадження у вітчизняну практику її передового світового досвіду.

У статті авторами проаналізовано напрямки використання космічного простору, космічних продуктів і послуг провідними країнами в інтересах безпеки й оборони. Визначено основні тенденції розвитку космічної діяльності: глобалізація у зв'язку зі збільшенням кількості космічних держав; розширення партнерства з одночасним прагненням до автономії в цій сфері; поява технологій інспектування орбітальних засобів тощо. Розглянуто космічні спроможності в інтересах національної безпеки та оборони, зокрема використання військових і цивільних, розвідувальних і комерційних космічних систем та інфраструктури для підтримання безпекових стратегій, досягнення національних цілей та захисту державних інтересів. Запропоновано подальші напрями удосконалення вітчизняної космічної діяльності у сфері національної безпеки та оборони, а саме: покращення її нормативно-правового забезпечення; уточнення мети, визначення основних завдань та пріоритетних напрямів її модернізації; формування системи управління; організація і розвиток міжвідомчої координації, взаємодії та спільного вирішення завдань.

Ключові слова: *космічна діяльність; космічні продукти та послуги; засоби космічної інспекції; національна безпека й оборона.*

Постановка проблеми в загальному вигляді. Характерною рисою сучасного суспільства є його інформатизація – активна розробка та впровадження у всі сфери людської діяльності передових технологій та засобів. Однією зі складових загального інформаційного простору є відомості, отримані за результатами космічної діяльності, нинішній рівень якої є результатом науково-технічного прогресу та основою нового етапу якісних змін і масштабів діяльності людства. Космічна діяльність трансформувала зміст геополітики, змінила пріоритети умов і чинників, що визначають безпеку та впливовість держави. Широке впровадження та використання її результатів у всіх сферах зумовило те, що географічне розташування країни перестало бути домінантою міжнародних відносин.

На сьогоднішній день вітчизняна космічна діяльність не стала дієвим інструментом для досягнення геополітичних цілей держави, не забезпечується оперативне надання

незалежних геопросторових даних, навігаційної інформації та супутникового зв'язку [1]. Недосконаліть нормативно-правової бази космічної діяльності, органів державного та військового управління щодо її організації та здійснення, відомча розпорошеність сил і засобів, недостатній рівень і відсутність взаємодії та міжвідомчої координації унеможливлюють підвищення ефективності виконання завдань у сфері національної безпеки та оборони України за рахунок використання космічної техніки. Проблема загострюється довгостроковим характером російської гібридної війни проти нашої держави, вагомим чинником якої є космічна складова, що забезпечується ракетно-космічною галуззю та космічними військами Російської Федерації (РФ).

У зв'язку з цим актуальним завданням є проведення аналізу сучасних тенденцій розвитку космічної діяльності у світі в безпековому секторі та основних чинників і умов, які визначають рівень знання космічної обстановки. Отримані результати повинні стати основою запровадження у вітчизняну практику передового світового досвіду, зокрема європейського та держав – членів Північноатлантичного альянсу (НАТО).

Аналіз останніх досліджень і публікацій. Використання космічних систем і засобів в інтересах національної безпеки й оборони, інформаційного забезпечення органів державного та військового управління, у ході дій угруповань військ (сил) Збройних Сил (ЗС) України розглядається в багатьох публікаціях, у яких вітчизняні фахівці досліджують різні аспекти створення та застосування космічної техніки і космічних технологій у сфері національної безпеки й оборони держави [2–5]. Проте вони носять переважно загальний, концептуальний або вузькоспеціалізований характер щодо застосування (використання) конкретних космічних систем і засобів – видової розвідки та дистанційного зондування Землі, глобальних навігаційних супутникових систем, супутникового зв'язку, системи контролю й аналізу космічної обстановки, космічного інформаційного забезпечення (підтримки) військ (сил).

Результати системного опрацювання, узагальнення та систематизації сучасного іноземного й вітчизняного досвіду космічної діяльності у сферах національної безпеки та оборони вперше в Україні висвітлено в монографії [6], у якій проаналізовано чинну нормативно-правову базу космічної діяльності, сили та засоби її провадження, акцентовано увагу на необхідності пріоритетного розвитку космічних систем і засобів забезпечення національної безпеки та захисту державних інтересів.

Формулювання завдання дослідження. Отже, існує актуальна необхідність визначення основних тенденцій світової космічної діяльності в інтересах національної безпеки та оборони з урахуванням методологічних підходів до формування космічної стратегії України, викладених у [7], що і є метою статті.

Виклад основного матеріалу. Космічна політика, як ключова складова геополітики, істотно вирізняється космічними спроможностями, зокрема здатністю використання військових і цивільних, розвідувальних і комерційних космічних систем та інфраструктури для підтримання стратегій національної безпеки. Завдяки інформації, отриманій із космосу, планують операції, забезпечують безпеку національних військ, розгорнутих на всіх театрах воєнних дій. З космосу ведуть спостереження за противником, його укриттями, логістикою, діями та переміщеннями, завдяки чому можна зрозуміти його задум і наміри.

Ключова роль такої діяльності визначається екстериторіальністю космічного простору та унікальними можливостями сучасних космічних систем: їх глобальністю дії, високими інформативністю та достовірністю даних, комплексністю застосування, всепогодністю, значними обсягами та швидкостями передавання інформації.

У світовій практиці нині переважають два основні підходи до застосування космічних спроможностей в інтересах національної безпеки та оборони: космос як ресурс, що дозволяє забезпечити інформаційну підтримку вирішення безпекових й оборонних завдань, або як місце розміщення бойових космічних засобів [7].

Наприклад, державами – членами НАТО космічний простір розглядається як зона життєво важливих інтересів, а використання його у військових цілях – неодмінною умовою забезпечення їх національної безпеки та досягнення успіху у війнах і збройних конфліктах. Важливе місце в досягненні спільних оборонних спроможностей має союзна військово-космічна діяльність НАТО, що організована та розвивається під впливом досвіду потужних космічних держав – членів Альянсу, зокрема, США, Великобританії, Федеративної Республіки Німеччини (ФРН), Франції [6]. Зупинимося на цьому більш детально.

Відповідно до вимог доктринальних документів США щодо космічної діяльності значна залежність держави від використання космосу і космічних технологій є уразливою ланкою її системи безпеки. Тому будь-яке цілеспрямоване втручання в роботу космічних систем – військових, комерційних, союзницьких – розглядається як посягання на законні права. У разі потреби США готові застосовувати силу для їх захисту. Командуванню ЗС належить своєчасно виявляти та запобігати ворожим діям з боку будь-яких державних або недержавних структур інших країн, що намагаються перешкоджати доступу США та їх союзників до вільного використання космічного простору.

Військово-космічна політика Великобританії обґрунтовує необхідність подальшого розширення присутності НАТО в інтересах досягнення переваг у космосі, визначає ресурси та умови для вирішення цього завдання, національні спроможності й перспективи розвитку ситуації в повітряно-космічному просторі.

В основу національної космічної політики ФРН закладено принципи активного використання космічного простору в інтересах безпеки. Підкреслюється, що в сучасних умовах операції військового характеру значною мірою залежать від використання космічного потенціалу, а супутникові системи зв'язку, навігації, знімання земної поверхні є найважливішими елементами комплексної системи забезпечення національної безпеки.

На думку військово-політичного керівництва Франції щодо використання космосу для забезпечення національних інтересів в Європі та за її межами, процеси глобалізації визначають програму використання космічного простору однією з пріоритетних. Здатність досягти будь-якої точки світу в короткі часові інтервали за допомогою застосування орбітального угруповання посилює важливість подальшого розвитку воєнної теорії. За оцінками командування ЗС Франції, розміщення до 2025 року систем зброї на космічних платформах буде відігравати істотну роль у разі ураження об'єктів у стратегічній та оперативно-стратегічній глибині із застосуванням як звичайних засобів ураження, так і зброї масового ураження. Можливість вирішення цих завдань із залученням орбітального угруповання є важливою характеристикою сучасних космічних спроможностей. Крім того, ефективність бойового забезпечення, розвідувальної

діяльності, інформаційних операцій, транспортних перевезень, бойового застосування військово-повітряних сил і сухопутних військ у збройних конфліктах стратегічного масштабу багато в чому залежатиме від стану космічного угруповання.

З огляду на зазначене, основоположними складовими космічних спроможностей у НАТО є (рис. 1):

космічна ситуаційна обізнаність (Space Situational Awareness, SSA);

нарощування бойових спроможностей за рахунок використання космосу (Space Force Enhancement);

контроль космічного простору (Space Control).

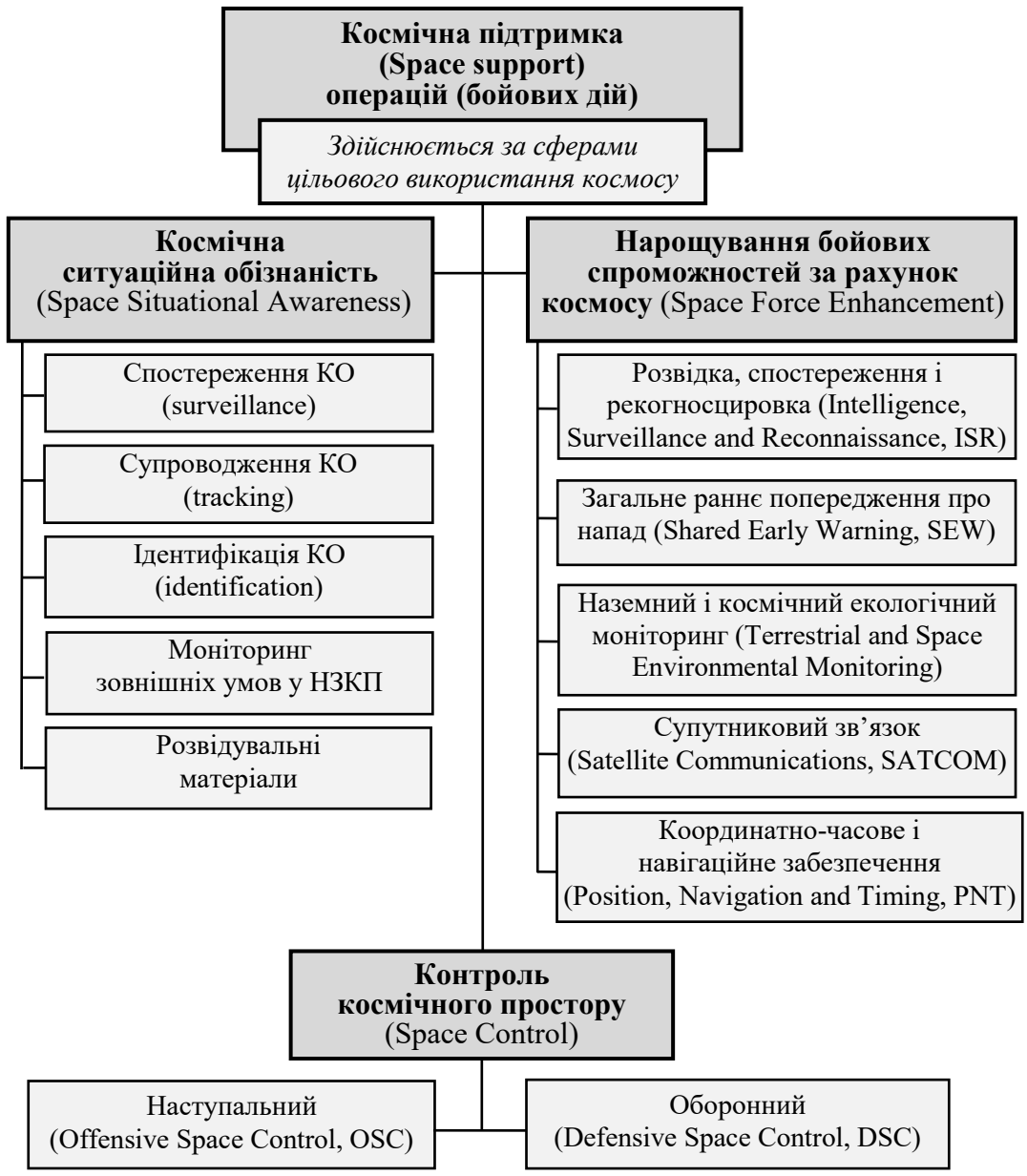


Рис. 1. Загальний зміст космічної підтримки операцій НАТО (КО – космічний об'єкт; НЗКП – навколоземний космічний простір)

На думку військово-політичного керівництва та військових фахівців РФ, істотне зростання ролі та значущості військ (сил) і засобів, що діють у повітряно-космічній сфері, є однією із найважливіших тенденцій зміни характеру збройної боротьби. Зокрема, воєнна доктрина РФ визначає наміри розміщення зброї в космосі як одну з основних зовнішніх

військових небезпек, а вплив на противника на всю глибину його території одночасно в глобальному інформаційному та повітряно-космічному просторі, на суші і морі – як характерну рису сучасних збройних конфліктів.

Сучасне космічне середовище, як і кіберсередовище, надає можливість комфортно діяти "в тіні" і залишатися без протидії, особливо якщо це стосується шпіонажу або втручання в роботу іноземних сервісів. Прикладом є космічний апарат (КА) РФ "Луч – Олімп", виведений на геостаціонарну орбіту 28.09.2014 у робочу орбітальну позицію 57° Е. Даних про нього у відкритих джерелах дуже обмаль, за час свого існування на орбіті супутник не менше 10 разів змінював орбітальну позицію. Так, 07.10.2014 КА досягнув орбітальної позиції, що становила 52° Е, зупинився біля КА системи стратегічної радіоелектронної розвідки Національного управління військово-космічної розвідки США, Агентства національної безпеки та Центрального розвідувального управління "NROL-15" та КА "WGS-5" широкосмугового стратегічного зв'язку Департаменту оборони США. Після трьох місяців перебування в орбітальній позиції 52° Е, КА "Луч – Олімп" почав передислокацію у східному напрямку й у березні – квітні 2015 року призупинився на довготах, що відповідали 95°–96° Е, у зоні проведення активних маневрів кораблів Тихоокеанського флоту РФ. У тій же орбітальній позиції у той самий час знаходився КА радіоелектронної розвідки США "Advanced Orion" (Mentor), який забезпечував даними Центральне розвідувальне управління та Агентство національної безпеки США. Так само з цієї орбітальної позиції постійно проводяться перехоплення урядової та дипломатичної інформації, яка надходить від китайських спецслужб.

Ці приклади підтверджують той факт, що зараз реальним є інспектування та перехоплення даних КА з боку іноземних супутників-шпіонів. Також можуть бути здійснені спроби вивести з ладу діючий КА або навіть змінити його траєкторію. У зв'язку з цим актуальним завданням є розроблення нових підходів до проведення космічних операцій з метою захисту країни та попередження агресії.

Усебічне забезпечення діяльності російських ЗС із космосу та гарантований доступ у космічний простір зі своєї території розглядається військово-політичним керівництвом держави як пріоритетна умова володіння необхідним військовим потенціалом, що забезпечує безпеку, незалежність і нормальний розвиток держави, збереження авторитету на арені світової політики. Воєнна доктрина РФ серед основних завдань ЗС визначає розгортання та підтримання в стратегічній космічній зоні орбітальних угруповань КА, що забезпечують діяльність ЗС РФ.

З урахуванням зростаючої значущості космічних сил і засобів у ході підготовки та ведення сучасних операцій, практики застосування космічних ресурсів державами в збройних конфліктах різної інтенсивності, у РФ визначено для використання такі терміни: космічний театр воєнних дій, повітряно-космічний театр воєнних дій, стратегічна космічна зона.

На даний час космічна діяльність провідних держав у сфері національної безпеки та оборони, залежно від її обсягу, повноти та завдань, провадиться спеціально створеними організаційними структурами – космічними військами (силами), які можуть бути в складі як ЗС, так і цивільних міністерств і відомств. Держави, які не мають або мають обмежені орбітальні сегменти космічної інфраструктури, здійснюють космічну діяльність переважно з використанням власного наземного інформаційного комплексу, космічних продуктів і космічних послуг союзників та комерційних партнерів. Для здійснення

космічної діяльності вони створили або створюють організаційні структури змішаного військово-цивільного типу. Тенденцією сучасної космонавтики є намагання досягти стратегічної космічної автономії провідними державами. Як перехідний етап розглядається співробітництво з іншими країнами, наприклад, франко-італійське в орбітальному угрупованні та франко-німецьке в галузі моніторингу НЗКП. Однак кінцевою метою є досягнення повної автономії щодо виконання завдань у космосі.

У сучасному світі практична космонавтика перестала бути монополією передових космічних держав, швидко розширюється коло тих, які мають космічні програми та відповідні технології. Найбільше вражає космічний ривок Китаю, що стрімко наближається до передових космічних держав, а за низкою показників, зокрема з кількості космічних запусків і надання пускових послуг, випереджає колишніх лідерів. Підтвердженням цього є аналіз динаміки кількості космічних запусків за 2010–2018 роки (табл. 1), що однозначно свідчить про перерозподіл світового ринку пускових послуг і втрату РФ лідерських позицій у цьому виді космічної діяльності.

Таблиця 1

Статистика космічних запусків за 2010–2018 роки

Рік		Кількість космічних запусків							
		Усього	В окремих державах						Решта
			РФ	США	КНР	ЄС	Японія	Індія	
2010	Усього	74	**31 (41,9%)**	15 (20,3%)	**15 (20,3%)**	6 (8,1%)	2 (2,7%)	3(4,0%)	2(2,7%)
	Успішних	70	30 (96,8%)	15 (100%)	15 (100%)	6 (100%)	2 (100%)	1 (33,3%)	1 (50,0%)
2011	Усього	84	33 (39,3%)	18 (21,4%)	19 (22,6%)	5 (5,9%)	3 (3,6%)	3 (3,6%)	3 (3,6%)
	Успішних	78	29 (87,9%)	17 (94,4%)	18 (94,7%)	5 (100%)	3 (100%)	3 (100%)	3 (100%)
2012	Усього	78	26 (33,3%)	13 (16,6%)	19 (24,3%)	8 (10,3%)	2 (2,6%)	2 (2,6%)	8 (10,3%)
	Успішних	73	24 (92,3%)	12 (92,3%)	19 (100%)	8 (100%)	2 (100%)	2 (100%)	5 (62,5%)
2013	Усього	82	33 (40,2%)	19 (23,2%)	15 (18,3%)	5 (6,1%)	3 (3,6%)	3 (3,6%)	4 (5,0%)
	Успішних	78	31 (93,9%)	19 (100%)	14 (93,3%)	5 (100%)	3 (100%)	3 (100%)	3 (75,0%)
2014	Усього	92	36 (39,1%)	23 (25,0%)	16 (17,4%)	7 (7,6%)	4 (4,35%)	4 (4,35%)	2 (2,2%)
	Успішних	89	34 (94,4%)	22 (95,7%)	16 (100%)	7 (100%)	4 (100%)	4 (100%)	2 (100%)
2015	Усього	87	29 (33,3%)	20 (23%)	19 (21,8%)	9 (10,3%)	4 (4,6%)	5 (5,7%)	1 (1,2%)
	Успішних	82	26 (89,6%)	18 (900%)	19 (100%)	9 (100%)	4 (100%)	5 (100%)	1 (100%)
2016	Усього	85	19 (22,3%)	22 (25,9%)	22 (25,9%)	9 (10,6%)	4 (4,7%)	7 (8,2%)	2 (2,4%)
	Успішних	81	18 (94,7%)	22 (100%)	21 (95,5%)	9 (100%)	4 (100%)	7 (100%)	1 (50%)
2017	Усього	91	20 (21,9%)	29 (31,8%)	18 (19,8%)	9 (9,9%)	7 (7,7%)	5 (5,6%)	3 (3,3%)
	Успішних	82	18 (90%)	29 (100%)	16 (88,9%)	9 (100%)	6 (85,7%)	4 (80%)	1 (33,3%)
2018	Усього	114	**17 (14,9%)**	31 (27,2%)	**39 (34,2%)**	11 (9,6%)	6 (5,3%)	7 (6,2%)	3 (2,6%)
	Успішних	111	16 (94,1%)	31 (100%)	38 (97,4%)	10 (90,9%)	6 (100%)	7 (100%)	3 (100%)

Нині також відбувається якісний перелом у фінансуванні космонавтики за рахунок інвестицій приватного капіталу (рис. 2). Окремі галузі практичної космонавтики, насамперед телекомунікаційна, взагалі не потребують бюджетних коштів, а перші зразки приватних ракет-носіїв свідчать про втрату державних монополій на здійснення космічних запусків і початок приватної комерціалізації в космосі [8]. Тенденцією сучасної космічної діяльності є зацікавленість оборонних структур провідних держав в участі в комерційних проєктах із запуску супутникових угруповань, оскільки вони є ідеальним варіантом для реалізації космічних пріоритетів країни.

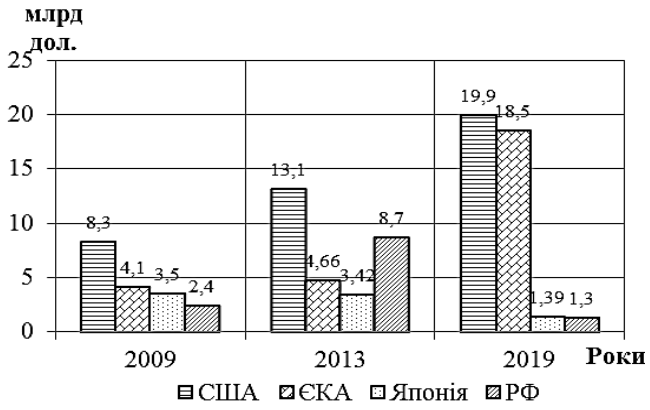


Рис. 2. Обсяги фінансування космічної діяльності в провідних державах світу (млрд дол.)

Ще однією рисою сучасної космонавтики є суттєве нарощування обсягу космічних продуктів та послуг, що потребує отримання й оброблення великих потоків даних. Для отримання бажаного ефекту, особливо для розвідувальних відомств, необхідне застосування (використання) відповідних новітніх засобів оброблення великих об'ємів інформації: сучасних баз даних та підходів "штучного інтелекту" (машинного навчання). На найближчі роки саме вони будуть основними напрямками наукових досліджень, зокрема, в інтересах ЗС.

Важливим питанням сучасної космічної діяльності є гарантування безпеки запуску нових і польоту наявних КА. На сьогодні в НЗКП знаходяться більше 1500 працюючих (активних) КА. За прогнозами впродовж 10 років з'явиться ще 3000 КА вагою більше 50 кг та близько 7000 менших апаратів. Крім того, від 500000 до 750000 об'єктів ("космічне сміття") більше 1 см обертаються на навколоземних орбітах. За цих умов зростає ймовірність зіткнень діючих КА з "космічним сміттям", що в результаті призведе до виходу їх з ладу або завдання їм критичних ушкоджень.

Отже, аналіз стану світової космічної діяльності дозволяє визначити основні тенденції її розвитку в інтересах національної безпеки й оборони, а саме:

розширення кола держав, що проводять космічну діяльність, та вільне використання космічного простору;

зростання значущості космічної компоненти озброєнь іноземних держав і важливості космічної діяльності в їх потенціалі, використання космосу в інтересах національної безпеки й оборони як інформаційного ресурсу і місця розміщення бойових космічних засобів;

поява реальних протисупутникових засобів наземного (морського, повітряного) та космічного базування, засобів космічної інспекції;

досягнення переваг у космосі, зокрема, за рахунок налагодження співпраці з дружніми державами щодо використання результатів космічної діяльності з одночасним прагненням до досягнення автономії космічної діяльності провідних країн;

зростання рівня засміченості НЗКП "космічним сміттям" і, відповідно, затребуваності попереджувальної інформації про небезпечні зближення діючих КА з його елементами для проведення маневрів з метою запобігання зіткненню;

виведення на орбіти та очікування зростання застосування малорозмірних КА різного призначення на базі мікротехнологій;

використання комерційних КА та суттєве нарощування обсягу космічних продуктів та послуг в інтересах забезпечення завдань національної безпеки й оборони.

Висновки. Сучасні завдання забезпечення обороноздатності нашої держави вимагають прискореного розвитку вітчизняних космічних інформаційних технологій та визначають нагальну потребу удосконалення організації застосування (використання) космічної техніки та технологій у ЗС України: створення необхідних організаційних структур; розгортання сучасних програмно-технічних засобів оброблення та використання космічної інформації; застосування високошвидкісних ліній зв'язку та передачі даних; підготовка військових фахівців за напрямками застосування (використання) космічних засобів тощо. Розв'язання проблеми невідповідності нинішнього стану космічної діяльності у сфері оборони України сучасним загрозам і завданням забезпечення обороноздатності держави можливе за умови реалізації цілого комплексу заходів на основі аналізу основних тенденцій світової космічної діяльності в інтересах національної безпеки та оборони з урахуванням методологічних підходів до формування космічної стратегії держави.

Серед тенденцій світової космічної діяльності особливо виділяються такі: збільшення кількості космічних держав; поява реальних протисупутникових засобів наземного (морського, повітряного) та космічного базування, засобів космічної інспекції; використання комерційних космічних апаратів та суттєве нарощування обсягу космічних продуктів і послуг в інтересах забезпечення завдань національної безпеки й оборони.

Основні світові тенденції космічної діяльності однозначно визначають її як фактор безпеки держави.

Саме тому суттєве удосконалення вітчизняної космічної діяльності потребує вирішення таких першочергових завдань: покращення її нормативно-правового забезпечення у сфері національної безпеки та оборони України, зокрема щодо уточнення мети, визначення основних завдань і пріоритетних напрямів (проєктів), які відповідають сучасним загрозам і завданням забезпечення національних інтересів та обороноздатності держави; формування системи управління; організація і розвиток міжвідомчої координації, взаємодії та спільного вирішення завдань космічної діяльності.

СПИСОК ЛІТЕРАТУРИ

1. Про схвалення Концепції Загальнодержавної цільової науково-технічної космічної програми України на 2018–2022 роки : розпорядження Кабінету Міністрів України від 05.09.2018 № 629-р. URL: http://zakon.rada.gov.ua/laws/show/629-2018-%D1%80/sp:max100 (дата звернення: 18.03.2019).

2. Про рішення Ради національної безпеки і оборони України від 06.05.2015 "Про Стратегію національної безпеки України" : Указ Президента України від 26.05.2015 № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 18.03.2019).

3. Про рішення Ради національної безпеки і оборони України від 02.09.2015 "Про нову редакцію Воєнної доктрини України" : Указ Президента України від 24.09.2015 № 555/2015. URL: https://zakon.rada.gov.ua/go/555/2015 (дата звернення: 18.03.2019).

4. Про рішення Ради національної безпеки і оборони України від 04.03.2016 "Про Концепцію розвитку сектору безпеки і оборони України" : Указ Президента України від 14.03.2016 № 92/2016. URL: https://zakon.rada.gov.ua/laws/show/92/2016. (дата звернення: 18.03.2019).

5. Про рішення Ради національної безпеки і оборони України від 20.05.2016 "Про Стратегічний оборонний бюлетень України" : Указ Президента України від 06.06.2016 № 240/2016. URL: https://zakon.rada.gov.ua/laws/show/240/2016 (дата звернення: 18.03.2019).
6. Випорханюк Д. М., Ковбасюк С. В. Основи космічної ситуаційної обізнаності (Space Situational Awareness, SSA). Іноземний і вітчизняний досвід космічної діяльності у сфері оборони : Монографія. Житомир : Видавець О. О. Євенок, 2018. 532 с.
7. Горбулін В. П., Федоров О. П. Космічна стратегія: не маєш своєї – стаєш частиною чужої // Дзеркало тижня. 19–26.02.2010. № 6–7 (786). С. 11.
8. Миллиарды на космос: сколько тратит Украина и другие страны мира. URL: https://www.bbc.com/ukrainian/news-russian-45426959 (дата обращения: 01.04.2019).
9. Дубинина М. Г. Мировая космическая деятельность: состояние и перспективы развития // Анализ и моделирование экономических и социальных процессов: математика. компьютерное образование. 2015. № 3. С. 164–171.

Подано 24.06.2019

Ф. М. Андреев, И. А. Беспалко, Д. Н. Випорханюк, С. В. Ковбасюк

ОСНОВНЫЕ ТЕНДЕНЦИИ МИРОВОЙ КОСМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В ИНТЕРЕСАХ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И ОБОРОНЫ

Последние десятилетия космос, как и суша, море, воздух и киберпространство, стал ареной соперничества мощных мировых государств, что привело к изменению природы действий в околоземном космическом пространстве ряда стран. Следствием космической деятельности стало то, что географическое положение перестало быть доминантой международных отношений. Отечественная космическая деятельность, к сожалению, не стала действенным инструментом для достижения геополитических целей Украины и обеспечения выполнения задач в интересах национальной безопасности и обороны. В связи с этим актуальным является проведение анализа современных тенденций развития космической деятельности в мире в секторе безопасности, результаты которого должны стать основанием для введения в отечественную практику ее передового мирового опыта.

В статье авторами проанализированы направления использования космического пространства, космических продуктов и услуг ведущими странами в интересах безопасности и обороны. Определены основные тенденции развития космической деятельности: глобализация в связи с увеличением количества космических государств; расширение партнерства с одновременным стремлением к автономии в этой сфере; появление технологий инспекции орбитальных средств и т. п. Рассмотрены космические возможности в интересах национальной безопасности и обороны, в частности использование военных и гражданских, разведывательных и коммерческих космических систем и инфраструктуры для поддержания безопасности стратегий, достижения национальных целей и защиты государственных интересов. Предложены дальнейшие направления совершенствования отечественной космической деятельности в сфере национальной безопасности и обороны Украины, а именно: улучшение ее нормативно-правового обеспечения; уточнение цели, определение основных задач и приоритетных

направлений ее модернизации; формирование системы управления; организация и развитие межведомственной координации, взаимодействия и совместного решения задач.

Ключевые слова: *космическая деятельность; космические продукты и услуги; средства космической инспекции; национальная безопасность и оборона.*

F. M. Andreiev, I. A. Bespalko, D. M. Vyporkhaniuk, S. V. Kovbasiuk

THE MAIN TRENDS OF WORLD SPACE ACTIVITY IN THE INTERESTS OF NATIONAL SECURITY & DEFENSE

In recent decades, space, like land, sea, air and cyberspace, has become a platform for the confronting between powerful states, which has led to a change in the nature of action in the near-Earth space of a number of countries. The consequence of space activities was that the geographical location ceased to be dominant in international relations. Unfortunately, the national space activity has not become an effective tool for achieving the geopolitical goals of Ukraine, ensuring the fulfillment of tasks in the interests of national security and defense. In this regard, it is important to analyze current trends in the development of space activities in the world in the security sector, the results of which should be the basis for the introduction of best international experience in domestic practice.

The article analyzes the directions of use of outer space, space products and services by leading countries in the interests of security and defense. The main trends of development of space activity are defined: globalization in connection with the increasing number of space states; expansion of partnership with simultaneous aspirations for autonomy in this sphere; emergence of inspection technologies for orbital means, etc. Space capabilities in the interests of national security and defense are considered, in particular the usage of military and civilian, intelligence and commercial space systems and infrastructure for supporting security strategies, achieving national goals and protecting public interests. Further directions of improvement of national space activity in the field of national security and defense of Ukraine are proposed, namely: improvement of its normative and legal support; clarification of the purpose, definition of the main tasks and priority directions of its improvement; formation of a management system; organization and development of interagency coordination, interaction and joint problem solving.

Keywords: *space activities; space products and services; space inspection facilities; national security and defense.*

УДК 004.056.55

М. В. Єсіна, С. Г. Вдовенко, І. Д. Горбенко

МОДЕЛІ БЕЗПЕКИ ПОСТКВАНТОВИХ АСИМЕТРИЧНИХ ШИФРІВ НА ОСНОВІ НЕРОЗРІЗНЮВАНОСТІ

У статті подано доведення еквівалентності властивості нерозрізнюваності (невизначеності) властивості семантичної безпеки для захисту криптосистем від криптоаналізу зловмисника на основі підібраного (вибраного) відкритого тексту.

Питання аналізу й дослідження моделей безпеки постквантових криптоалгоритмів відносно криптопримітивів усіх типів, визначення критеріїв оцінки їх відповідності різним моделям безпеки (згідно з різними типами криптоперетворень) є актуальними та такими, що мають практичне значення. Нерозрізнюваність (невизначеність) зашифрованого тексту – це важлива властивість безпеки багатьох схем шифрування, яка в разі атаки на основі підібраного (вибраного) відкритого тексту вважається основною вимогою для більшості достовірно захищених криптосистем із відкритим ключем. Деякі схеми також забезпечують нерозрізнюваність у ході атак на основі підібраного (вибраного) та адаптивно підібраного (вибраного) зашифрованого тексту. Використання властивості нерозрізнюваності (невизначеності) зашифрованого тексту на даний час дозволяє гарантовано здійснити захист усіх відомих симетричних та асиметричних криптосистем від класичного чи квантового криптоаналізу зловмисника.

Запропоновано три моделі безпеки, що стосуються шифрування, електронного підпису та механізмів інкапсуляції ключів. Розглянуті найпоширеніші сучасні види атак на безпеку механізмів шифрування, а саме: атака на основі адаптивно підібраних (вибраних) шифртекстів; атака на основі адаптивно підібраних (вибраних) відкритих текстів; атака на основі адаптивно підібраних (вибраних) відкритих текстів та адаптивно підібраних (вибраних) шифртекстів; атака на основі підібраних (вибраних) шифртекстів; атака на основі підібраних (вибраних) відкритих текстів; атака на основі підібраних (вибраних) відкритих текстів та підібраних (вибраних) шифртекстів; атаки розрізнення (розрізнюваності).

Ключові слова: *атака на основі адаптивно підібраних (вибраних) шифр текстів; атака на основі підібраних (вибраних) відкритих текстів; нерозрізнюваність (невизначеність) зашифрованого тексту; нерозрізнюваність ключів.*

Постановка проблеми в загальному вигляді. Національний інститут стандартів і технології (NIST) США проводить конкурс на постквантові криптографічні алгоритми. У критеріях відбору кандидатів є пункт, що стосується моделей безпеки, а саме: кожен тип криптоалгоритму повинен відповідати певній моделі безпеки. NIST наводить три моделі безпеки, що стосуються шифрування, електронного підпису та механізмів інкапсуляції ключів: моделі *IND-CPA*, *IND-CCA*, *IND-CCA2* стосуються механізмів шифрування; модель *EUF-CMA* – механізмів підпису; модель *CK* – механізмів інкапсуляції ключів. Тому актуальною є проблема узагальненого визначення та дослідження моделей безпеки щодо криптопримітивів усіх типів, зокрема визначення

умов застосування постквантових асиметричних шифрів у процесі здійснення класичного чи квантового криптоаналізу.

У термінах моделей безпеки щодо криптоперетворень асиметричного шифрування існують такі атаки: на основі адаптивно підібраних (вибраних) шифртекстів; на основі адаптивно підібраних (вибраних) відкритих текстів; на основі адаптивно підібраних (вибраних) відкритих текстів та адаптивно підібраних (вибраних) шифртекстів; на основі підібраних (вибраних) шифртекстів; на основі підібраних (вибраних) відкритих текстів; на основі підібраних (вибраних) відкритих текстів та підібраних (вибраних) шифртекстів; атаки розрізнення (розрізнюваності).

Нерозрізнюваність (невизначеність) у разі атаки на основі підібраного (вибраного) відкритого тексту еквівалентна властивості семантичної безпеки, тому багато криптографічних доказів використовують ці визначення як еквівалентні Якщо криптосистема володіє властивістю нерозрізнюваності, то зловмисник не зможе відрізнити пари шифрованих текстів на основі повідомлення, що вони шифрують [1].

Аналіз останніх досліджень і публікацій. Властивість нерозрізнюваності (невизначеності) розглянута в роботах Х. ван Тілборга та М. Білара [2, 5]. В опублікованих роботах не досліджено питання умов використання властивості нерорізнюваності (невизначеності) для захисту асиметричних криптосистем від класичного чи квантового криптоаналізу зловмисника.

Формулювання завдання. Метою статті є доведення еквівалентності властивості нерозрізнюваності (невизначеності) властивості семантичної безпеки для захисту криптосистем від криптоаналізу зловмисника на основі підібраного (вибраного) відкритого тексту.

Виклад основного матеріалу

1. Рекомендовані позначення та скорочення

Наведемо дефініції, позначення, допоміжні (довідкові) визначення та короткий опис атак у термінах цих моделей безпеки [2, 3].

IND – нерозрізнюваність (Indistinguishability);

IK – нерозрізнюваність ключів (Indistinguishability of keys);

IE – нерозрізнюваність зашифрованих текстів (Indistinguishability of encryptions);

CPA – атака на основі підібраних (вибраних) відкритих повідомлень (Chosen plaintext attack);

CCA2 – атака на основі адаптивно підібраних (вибраних) шифртекстів (Adaptive chosen ciphertext attack);

IE-CPA – нерозрізнюваність шифртекстів (зашифрованих текстів) у разі атаки на основі підібраних (вибраних) відкритих текстів;

IE-CCA – нерозрізнюваність шифртекстів (зашифрованих текстів) у разі атаки на основі підібраних (вибраних) шифртекстів.

PKE є *IND-CPA*, якщо шифртекст не розкриває жодної інформації про відкритий текст.

Оракул – це третя сторона, з якою ви спілкуєтеся, коли вам потрібні дані, які ви не хочете або не можете отримати самостійно. Це сторона, яка відповідає за підключення до джерела даних.

Роль оракула розшифрування може грати наївний користувач, змушений розшифровувати повідомлення зловмисника.

Випадковий оракул є потужною гіпотетичною детермінованою функцією, що ефективно обчислює рівномірно розподілені випадкові величини. Він точно імітується поліноміально обмеженим алгоритмом.

Модель із випадковим оракулом (*RAM*) – розширена математична модель криптографічного протоколу, у якій усі учасники мають доступ до оракула, що обчислює випадкову функцію. При кожному новому запиті значення функції на заданому аргументі вибирається випадковим чином. При цьому оракул запам'ятовує пару (аргумент – значення), у разі повторного запиту для цього аргументу, незалежно від того, хто з учасників його видав, буде повернено те ж саме запам'ятоване значення.

Оракул зашифрування забезпечує зашифрування запитуваного відкритого тексту, а оракул розшифрування – розшифрування запитуваного шифртексту.

2. Визначення моделі безпеки та нерозрізнюваності

Криптосистема вважається безпечною щодо нерозрізнюваності, якщо жоден зловмисник *A*, отримавши зашифрований текст, довільно вибраний з двоелементного простору повідомлень, визначеного ним самим, не може ідентифікувати свій вибір з імовірністю значно кращою, ніж у разі випадкових вгадувань (½). Якщо будь-який зловмисник може вдало відрізнити вибраний шифрований текст з імовірністю значно більшою, ніж ½, тоді він вважається таким, що має «перевагу» в розрізненні шифрованого тексту, а схема «не» вважається безпечною щодо нерозрізнюваності [1].

Безпека щодо нерозрізнюваності (невизначеності) розуміється як гра, де криптосистема вважається безпечною, якщо жоден зі зловмисників не може її виграти з значно більшою ймовірністю, ніж опонент, який повинен вгадати випадковим чином.

Найпоширеніші поняття, використовувані в криптографії [1, 2]:

нерозрізненість у разі атаки на основі підібраного (вибраного) відкритого тексту (*IND-CPA* безпека);

нерозрізненість у разі атаки на основі підібраного (вибраного) шифртексту (*IND-CCA* безпека);

нерозрізненість у разі атаки на основі адаптивно підібраного (вибраного) шифртексту (*IND-CCA2* безпека).

Безпека за будь-яким з останніх визначень передбачає безпеку за попередніми [1]:

схема, яка є *IND-CCA*-безпечною, також є *IND-CPA*-безпечною;

схема, яка *IND-CCA2*-безпечна, є як *IND-CCA*-безпечною, так і *IND-CPA*-безпечною.

Отже, *IND-CCA2* є найсуворішим із цих трьох визначень безпеки.

У разі нерозрізнюваності (невизначеності) відбувається захист від зловмисника *A*, який [4]: є ймовірнісною машиною Тюрінга поліноміального часу; має всі алгоритми; має повний доступ до засобів зв'язку.

3. Поняття семантичної безпеки

Семантична безпека – це поняття, яке описує безпеку схеми шифрування, позначається як *SEM-CPA* та фіксує ідею, що безпечна схема шифрування повинна приховувати всю інформацію про невідомий відкритий текст.

Зловмиснику дозволяється вибирати між двома відкритими текстами (m_0 та m_1), і він отримує зашифрування будь-якого з відкритих текстів.

Схема шифрування є семантично безпечною, якщо зловмисник не може здогадатися з кращою ймовірністю, ніж ½, чи даний шифртекст є зашифруванням повідомлення m_0 або m_1.

За Shannon схема шифрування є безпечною, якщо те, що можна визначити про відкритий текст із його шифртекстів, можна визначити за їх відсутності. Семантична безпека вимагає, щоб те, що можна ефективно обчислювати щодо деяких відкритих текстів з їх шифртекстів, можна було обчислювати так само легко, як за їх відсутності [5].

Поняття семантичної безпеки можна застосувати як до симетричних криптосистем, так і до криптосистем із відкритим ключем. Але, оскільки конкретний аналіз безпеки схеми шифрування на відкритому ключі є більш важливим, цей термін частіше використовується для обговорення безпеки схем шифрування з відкритим ключем [2].

Окрім семантичної безпеки, існують пов'язані поняття: «непідробленість» (Non-Malleability) та «поінформованість про відкритий текст» (Plaintext Awareness) [2].

Визначення 1. [Семантична безпека]. Нехай $SE=(K,E,D)$ – схема симетричного зашифрування; A – алгоритм, який має доступ до оракула. Розглянемо такі експерименти в сценарії семантичної безпеки [5]:

$Experiment\ Exp_{SE}^{SS\text{-}CPA\text{-}1}(A)$
$K \xleftarrow{\$} K, s \xleftarrow{\$} \varepsilon$
$for\ \ i \xleftarrow{} 1\ \ to\ \ q\ \ do$
$(M_{i,s}) \xleftarrow{\$} A(s)$
$M_i, M_i' \xleftarrow{\$} M_i$
$if\ |M_i| \neq M_i'\ \ then\ M_i \xleftarrow{} M_i' \xleftarrow{} \varepsilon$
$C_i \xleftarrow{\$} \varepsilon_K(M_i);\ s \xleftarrow{} \langle s, C_i \rangle$
$(f,Y) \xleftarrow{\$} A(s)$
$return\ f(M_1,...,M_q) = Y,$

$Experiment\ Exp_{SE}^{SS\text{-}CPA\text{-}0}(A)$
$K \xleftarrow{\$} K, s \xleftarrow{\$} \varepsilon$
$for\ \ i \xleftarrow{} 1\ \ to\ \ q\ \ do$
$(M_{i,s}) \xleftarrow{\$} A(s)$
$M_i, M_i' \xleftarrow{\$} M_i$
$if\ |M_i| \neq M_i'\ \ then\ M_i \xleftarrow{} M_i' \xleftarrow{} \varepsilon$
$C_i \xleftarrow{\$} \varepsilon_K(M_i');\ s \xleftarrow{} \langle s, C_i \rangle$
$(f,Y) \xleftarrow{\$} A(s)$
$return\ f(M_1,...,M_q) = Y.$

SEM-CPA перевагу алгоритму A визначаємо за таким виразом:

$$Adv_{SE}^{SEM-CPA}(A) = Pr\left[Exp_{SE}^{SS-CPA-1}(A) \Rightarrow 1\right] - Pr\left[Exp_{SE}^{SS-CPA-0}(A) \Rightarrow 1\right].$$

Отже, кожен експеримент ініціалізує свій оракул, вибравши випадковий ключ K. Усього q раз зловмисник вибирає простір повідомлень M_i, визначений імовірнісним алгоритмом, який завжди зупиняється (always-halting), написаним деякою фіксованою мовою програмування. Код для цього алгоритму – те, що насправді отримує зловмисник. Щоразу, коли виводиться простір повідомлення, дві випадкові вибірки M_i та M'_i виділяються з нього. Очікується, що M_i та M'_i мають однакову довжину, і якщо це не так, то обидва рядки «стираються». Зашифрування одного із цих повідомлень буде повернуто зловмиснику. Те, який рядок зашифрований, залежить від експерименту: M_i для експерименту 1 та M'_i для експерименту 0. За допомогою f позначають детерміністичну функцію. Її описує програма, яка завжди зупиняється (always-halting). Це програма для f, яку виводить зловмисник. За допомогою Y позначається рядок. Рядок s описує збережений стан, який за бажанням зловмисник може бути збережено.

Говорячи про термін виконання *A*, крім реального строку виконання, враховується ще максимальний час для виділення двох вибірок із кожного простору повідомлення *M*, що *A* виводить, і максимальний час для обчислення $f\left(M_1,...,M_q\right)$ над будь-яким вектором рядків. Характеризуючи довжину запитів *A*, підсумовується за всіма просторами повідомлень, що виводяться *A*, максимальна довжина рядка *M*, що знаходиться з ненульовою ймовірністю за допомогою *M*, і підсумовується також за довжинами кодувань кожного простору повідомлення функцією *f*, а рядок *Y* визначається за допомогою *A*.

Підкреслимо, що сказане вище виглядає як винятково сильне поняття безпеки. Зловмиснику надається можливість вибрати простір повідомлень, з якого буде взято кожне повідомлення. Йому дозволяється виокремити часткову інформацію про повідомлення, яку він вважає придатною для прогнозування. Він може повністю адаптуватися. Також вбудовано здатність виконувати атаку на основі підібраного (вибраного) повідомлення (просто виробляючи алгоритм *M*, який вибирає одну і тільки одну точку). Незважаючи на все це, покажемо далі, що безпека в розумінні нерозрізнюваності означає семантичну безпеку [5].

Теорема 1. [*IND-CPA⇒SEM-CPA*]

Нехай $SE=\left(K,E,D\right)$ – схема симетричного за шифрування, *A* – зловмисник (для атаки *SEM-CPA* безпеки *SE*), який виконується за максимальний час *t* та здійснює щонайбільше *q* запитів, які в загальному мають μ бітів. Тоді тут існує і зловмисник *B* (для атаки *IND-CPA* безпеки *SE*), який досягає переваги за рахунок додаткової інформації про відкритий текст (1):

$$Adv_{SE}^{IND-CPA}\left(B\right)\geq Adv_{SE}^{SEM-CPA}\left(A\right), \tag{1}$$

де *B* виконує за час $t + O(\mu)$ щонайбільше *q* запитів, які в загальному мають μ бітів.

Доведення: зловмисника *B*, який має оракул *g*, опишемо за таким алгоритмом:

algoritm B^9
$s \xleftarrow{\$} \varepsilon$
for $i \longleftarrow 1$ *to* q *do*
$\left(M_{i,s}\right) \xleftarrow{\$} A(s)$
$M_i, M_i' \xleftarrow{\$} M_i$
if $\left|M_i\right| \neq M_i'$ *then* $M_i \longleftarrow M_i' \longleftarrow \varepsilon$
$C_i \longleftarrow g\left(M_i, M'\right)$, $s \longleftarrow \langle s, C_i \rangle$
$(f, Y) \xleftarrow{\$} A(s)$
if $f\left(M_1,...,M_q\right) = Y$ *then return 1 else return 0.*

Припустимо спочатку, що *g* підтверджується (вказується) правим оракулом зашифрування, який повертає $C \xleftarrow{\$} E_K(M)$ у відповідь на запит (*M*′, *M*). Тоді алгоритм вище збігається з експериментом $Exp_{SE}^{SS-CPA-1}\left(A\right)$ [5]. Аналогічним чином, якщо *g* підтверджується (вказується) за допомогою лівого оракула зашифрування, то він повертає $C \xleftarrow{\$} E_K(M')$ у відповідь на запит (*M*′, *M*), тоді зазначений вище алгоритм збігається

з експериментом $Exp_{SE}^{SS-CPA-0}(A)$. Звідси випливає, що $Adv_{SE}^{SEM-CPA}(B) = Adv_{SE}^{IND-CPA}(A)$. Щоб завершити теорему, необхідно звернути увагу на те, що час виконання B – це час виконання A та $O(\mu)$. B характеризує загальну кількість запитів q, загальна довжина яких не перевищує загальної довжини запитів A відповідно до нашої умови [5].

4. Сутність найпоширеніших атак

Розглянемо найпоширеніші сучасні види атак [2] на безпеку механізмів шифрування.

4.1. Атака на основі адаптивно підібраних (вибраних) шифртекстів – це сценарій, у якому зловмисник має можливість підібрати (вибрати) вхідні дані для функції розшифрування на основі попередніх запитів підібраних (вибраних) шифртекстів. Сценарій зазвичай є більш потужним, ніж основна атака на основі підібраних (вибраних) шифртекстів, а отже, менш реалістичним. Проте атака може бути досить практичною в налаштуваннях відкритого ключа. Наприклад, звичайний RSA є вразливим до атаки на основі вибраних (підібраних) шифртекстів, а деякі реалізації RSA можуть бути вразливими до атаки на основі адаптивно підібраних (вибраних) шифртекстів.

4.2. Атака на основі адаптивно підібраних (вибраних) відкритих текстів – це сценарій, у якому зловмисник має можливість підібрати (вибрати) вхідні дані для функції зашифрування на основі попередніх запитів підібраних (вибраних) відкритих текстів та їх відповідних шифртекстів. Сценарій зазвичай є більш потужним, ніж основна атака на базі підібраних (вибраних) відкритих текстів, але, ймовірно, менш практичним у реальному житті, оскільки ця атака вимагає взаємодії того, хто атакує, з пристроєм зашифрування.

4.3. Атака на основі адаптивно підібраних (вибраних) відкритих текстів та шифртекстів дозволяє зловмиснику одночасно застосувати запити на адаптивно підібрані (вибрані) відкриті тексти та адаптивно підібрані (вибрані) шифртексти. Вона є однією з найбільш потужних з огляду на можливості зловмисника.

4.4. Атака на основі підібраних (вибраних) шифртекстів – це сценарій, за якого зловмисник має можливість вибирати шифртексти C_i і переглядати їх відповідні розшифрування – відкриті тексти P_i. Це, по суті, такий самий сценарій, як атака на основі підібраних (вибраних) відкритих текстів, але застосована до функції розшифрування, а не до функції зашифрування. Атака вважається менш практичною в реальних ситуаціях, ніж варіант на основі підібраних (вибраних) відкритих текстів. Проте немає прямих відповідностей між складностями атак на основі підібраних(вибраних) відкритих текстів та підібраних(вибраних) шифртекстів. Шифр може бути вразливим до однієї атаки, але не до іншої або навпаки. Атака на основі підібраних (вибраних) шифртекстів є дуже важливою в криптографії з відкритим ключем, де сценарії відомих відкритих текстів і навіть підібраних (вибраних) відкритих текстів завжди доступні для зловмисника через загальновідомий ключ зашифрування. Наприклад, схема шифрування з відкритим ключем RSA не захищена від атаки на основі адаптивно підібраних (вибраних) шифртекстів.

4.5. Атака на основі підібраних (вибраних) відкритих текстів – це сценарій, у якому той, хто атакує, має можливість підбирати (вибирати) відкриті тексти P_i і переглядати їх відповідні зашифрування – шифртексти C_i. Ця атака вважається менш практичною, ніж на основі відомих відкритих текстів, але все ж таки небезпечною. Якщо шифр вразливий до атаки на основі відомих відкритих текстів, то він автоматично вразливий до атаки на основі підібраних(вибраних) відкритих текстів, але не обов'язково навпаки. У сучасній криптографії типовий приклад подібного сценарію – диференційний

криптоаналіз. Це також рідкісний метод, для якого перетворення з підібраного (вибраного) відкритого тексту до відомого відкритого тексту є можливим (через його роботу з парами текстів).

4.6. Атака на основі підібраних (вибраних) відкритих текстів та шифртекстів дозволяє зловмиснику комбінувати атаку на основі підібраних (вибраних) відкритих текстів і на основі підібраних (вибраних) шифртекстів, а також видавати підібрані (вибрані) запити як для функції зашифрування, так і для функції розшифрування.

4.7. Атаки розрізнення (розрізнюваності) – це алгоритм тестування, який намагається виявляти в криптосистемі невипадкову поведінку, що може надати певну інформацію зловмиснику. Розрізнювач – алгоритм тестування, пов'язаний або з ідеальною випадковою процедурою R, або з криптосистемою (або її частиною) C, яка повинна імітувати R. Якщо розрізнювач здатний розпізнати їх зі значною перевагою, то це призводить до атаки розрізнення (розрізнюваності). Це дуже загальний параметр, який може застосовуватися до будь-якої криптосистеми, але є актуальним для оцінки її безпеки.

В основі всіх шифрів лежать деякі детерміністичні функції (інакше було б важко розшифрувати), які приймають як параметр ключ, а як вхідні дані – повідомлення. Просте застосування детерміністичних функцій щодо ключа і повідомлення призводить до елементарної атаки розрізнення (розрізнюваності), оскільки всі повідомлення, що мають однакове значення, зашифруються в однаковий шифртекст за однакового ключа. Саме тому всі схеми шифрування включають елемент рандомізації.

4.8. Нерозрізнюваність у разі атаки на основі підібраних (вибраних) відкритих текстів. Основна ідея нерозрізнюваності полягає в тому, щоб розглянути зловмисника, який не володіє секретним ключем та обирає два повідомлення однакової довжини. Тоді одне з них зашифровується, а шифртекст надається зловмиснику. Схема вважається безпечною, якщо йому важко визначити, яке з двох повідомлень було зашифровано. Схема шифрування вважається захищеною від атаки на основі підібраних (вибраних) відкритих текстів, якщо зловмисник, який обмежується використанням «практичної» кількості ресурсів (обчислювальний час, кількість запитів), не може отримати значну перевагу.

Надамо зловмиснику трохи більше потужності (сили) для вибору цілої послідовності пар повідомлень рівної довжини. Далі деталізуємо цю гру.

Зловмисник вибирає послідовність пар повідомлень $\left(M_{0,1},M_{1,1}\right),\ldots,\left(M_{0,q},M_{1,q}\right)$, де в кожній парі два повідомлення мають однакову довжину. Ми надаємо йому послідовність шифртекстів $C_1,\ldots, C_q$, де C_i – це зашифрування $M_{0,I}$ для всіх $1 \le i \le q$ (1) або, C_i – це зашифрування $M_{1,I}$ для всіх $1 \le I \le q$ (2). Виконуючи зашифрування, алгоритм щоразу використовує ті самі ключі, крім свіжих додаткових випадкових бітів (coins) або оновленого стану. Зловмисник отримує послідовність шифртекстів, і тепер йому слід вгадати: були зашифровані $M_{0,1},\ldots, M_{0,q}$ чи $M_{1,1},\ldots, M_{1,q}$.

Щоб ще більше розширити можливості зловмисника, ми дозволимо йому вибрати послідовність пар повідомлень за допомогою атаки на основі підібраних (вибраних) відкритих текстів. Тобто зловмисник вибирає першу пару й отримує C_1, потім обирає другу пару й отримує C_2 тощо. Іноді це називається атакою на основі адаптивно підібраних (вибраних) відкритих текстів, адже зловмисник може адаптивно підбирати (вибирати) кожен запит у такий спосіб, що відповідає більш раннім результатам.

4.9. Нерозрізнюваність у разі атаки на основі підібраних (вибраних) шифртекстів. Схема шифрування вважається захищеною від атаки на основі підібраних (вибраних) шифртекстів, якщо «розумний» зловмисник не може отримати «значну» перевагу, щоб відрізнити випадки $b = 0$ і $b = 1$, що мають доступ до оракулів, де розумно відображається використання його ресурсів. Технічне поняття називається нерозрізнюваністю в разі атаки на основі підібраних (вибраних) шифртекстів, позначається *IND-CCA*.

5. Моделі основних атак на основі нерозрізнюваності

Наведемо та розглянемо визначення та відповідні схеми виконання атак [2, 3].

5.1. Визначення *IND-CPA/CCA2*. Нехай $PKE = (Gen, Enc, Dec)$ є схемою шифрування з відкритим ключем. Розглянемо такий експеримент у сценарії *IND-CPA* [3]:

$$Expt\frac{IND-CPA}{PKE,\mathrm{A}}(\lambda)$$

$$\begin{aligned}
&(pk, sk) \longleftarrow Gen(1^{\lambda}) \\
&(m^0, m^1, state) \longleftarrow \mathrm{A}_1(pk) \\
&b \longleftarrow \{0,1\} \\
&c^* \longleftarrow Enc(pk, m^b) \\
&b' \longleftarrow \mathrm{A}_2(c^*, state),
\end{aligned}$$

де pk – відкритий ключ;

sk – особистий ключ;

m – відкритий текст;

Gen – генерація ключів;

Enc – зашифрування;

Dec – розшифрування;

state – деяка інформація про стан;

1^{λ} – параметр безпеки (може позначатися ще як k).

Алгоритм *Gen* на вхід приймає параметр безпеки 1^{λ}, виводить пару «відкритий – особистий ключ» (pk, sk).

Алгоритм *Enc* на вхід приймає відкритий ключ pk та відкритий текст m, обчислює шифртекст c.

Алгоритм *Dec* на вхід приймає особистий (секретний) ключ sk та шифртекст c, виводить відкритий текст m.

Потрібно, щоб для будь-якої пари (pk, sk) та m виконувалося рівняння $Dec(sk, Enc(pk, m)) = m$, тоді перевагу визначаємо за таким виразом:

$$Adv_{PKE.A}^{IND-CPA}(\lambda) = \left| Pr[b = b'] - \frac{1}{2} \right|.$$

Зауважимо, що *PKE* є *IND-CPA*-безпечним, якщо $Adv_{PKE.A}^{IND-CPA}(\lambda)$ є незначним.

Сценарій *IND-CCA2* повністю аналогічний *IND-CPA*, за винятком того, що зловмиснику дозволено запитувати c ($\neq c^*$) в оракула розшифрування $Dec(sk,\cdot)$.

5.2. Нерозрізнюваність ключів (визначення *IK-CPA/CCA2*). Конфіденційність ключа визначаємо в разі атак на основі підібраного (вибраного) відкритого тексту та підібраного (вибраного) шифртексту. Нехай зловмисник працює в два етапи [2, 3]. На етапі **find** він приймає два відкриті ключі pk_0 і pk_1 (відповідають секретним ключам sk_0 та sk_1) і виводить повідомлення x разом з деякою інформацією про стан s. На етапі **guess** він отримує виклик шифртексту y, який утворюється шляхом випадкового зашифрування повідомлень з одним із двох ключів. Він повинен визначити, який ключ був вибраний. У разі атаки на основі вибраного шифртексту зловмисник отримує оракули для $D_{sk_0}(\cdot)$ та $D_{sk_1}(\cdot)$ і може дозволити викликати їх у будь-якій точці з обмеженням (на обох оракулах), не запитуючи y під час етапу **guess.** Наведемо деякі основні позначення [3]:

$PE=(G,K,E,D)$ – схема шифрування з відкритим ключем;

G – загальний алгоритм генерації ключів: на вхід подається деякий параметр безпеки k, повертається деякий загальний ключ I;

K – рандомізований алгоритм генерації ключів, на вхід якого подається загальний ключ I та повертається пара ключів (pk,sk);

у $(pk,sk)\xleftarrow{R} K(I)$ I має бути тільки параметром безпеки k або містити додаткову інформацію;

E – рандомізований алгоритм зашифрування, який бере відкритий ключ pk та відкритий текст x для того, щоб повернути шифртекст y: $y\xleftarrow{R} E_{pk}(x)$;

D – детермінований алгоритм розшифрування, який приймає секретний ключ sk та шифртекст y для того, щоб повернути відповідний відкритий текст x або спеціальний символ $\perp$ та показати, що шифртекст є недійсним; записується $x\leftarrow D_{sk}(y)$, коли y є дійсним, та $\perp\leftarrow D_{sk}(y)$ – в іншому разі;

$MsgSp(pk)$ – простір повідомлень, з якого вибирається x.

Необхідно, щоб $D_{sk}(E_{pk}(x))=y$ для всіх $x\in MsgSp(pk)$.

Далі наведемо визначення для варіантів нерозрізнюваності ключів [2, 3].

Визначення 2. Нехай $PKE=(Gen,\ Enc,\ Dec)$ є схемою шифрування на відкритому ключі. Розглянемо такий експеримент у сценарії *IK-CPA:*

$$Expt\frac{IK-CPA}{PKE,\mathrm{A}}(\lambda)$$

$$(pk^0,sk^0),(pk1,sk^1)\xleftarrow{}Gen(1^\lambda)$$
$$(m,state)\xleftarrow{}\mathrm{A}_1(pk^0,pk^1)$$
$$b\xleftarrow{}\{0,1\}$$
$$c^*\xleftarrow{}Enc(pk^b,m)$$
$$b'\xleftarrow{}\mathrm{A}_2(c^*,state).$$

Перевагу зловмисника визначаємо як

$$Adv_{PKE.A}^{IK-CPA}(\lambda) = \left| Pr[b = b'] - \frac{1}{2} \right|.$$

Припустимо, що *PKE* є *IK-CPA*-безпечним, якщо $Adv_{PKE.A}^{IK-CPA}(\lambda)$ є незначним.

Сценарій *IK-CCA2* повністю аналогічний *IK-CPA*, за винятком того, що зловмиснику дозволено запитувати c ($\neq c^*$) в оракулів розшифрування $Dec(sk^0, \cdot)$ та $Dec(sk^1, \cdot)$.

Визначення 3. [*IK-CPA, IK-CCA*]. Нехай $PE = (G, K, E, D)$ є схемою шифрування, $b \in \{0, 1\}$ та $k \in N$. При цьому A_{CPA}, A_{CCA} є зловмисниками. A_{CCA} має доступ до оракулів $D_{sk_0}(\cdot)$ та $D_{sk_1}(\cdot)$. Розглянемо такі експерименти в сценаріях *IK-CPA* та *IK-CCA*:

$Experiment\ Exp_{PE,A_{CPA}}^{SS\text{-}CPA\text{-}b}(k)$
$I \xleftarrow{R} G(k)$
$(pk^0, sk^0) \xleftarrow{R} K(I); (pk^1, sk^1) \xleftarrow{R} K(I)$
$(x, s) \longleftarrow A_{cpa}(find, pk_0, pk_1)$
$y \longleftarrow \varepsilon_{pk_b}(x)$
$d \longleftarrow A$
$Return\ \ d,$

$Experiment\ Exp_{PE,A_{CCA}}^{SS\text{-}CPA\text{-}b}(k)$
$I \xleftarrow{R} G(k)$
$(pk_0, sk_0) \xleftarrow{R} K(I); (pk_1, sk_1) \xleftarrow{R} K(I)$
$(x, s) \longleftarrow A^{D_{sk_0}(\bullet), D_{sk_1}(\bullet)}{}_{cca}(find, pk_0, pk_1)$
$y \longleftarrow \varepsilon_{pk_b}(x)$
$d \longleftarrow A^{D_{sk_0}(\bullet), D_{sk_1}(\bullet)}{}_{cca}(guess, y, s)$
$Return\ \ d.$

Вище передбачено, що A_{CCA} ніколи не запитує $D_{sk_0}(\cdot)$ або $D_{sk_1}(\cdot)$ на виклик шифртексту y. Для $\boldsymbol{atk} \in \{\boldsymbol{cpa}, \boldsymbol{cca}\}$ визначаємо переваги зловмисників за виразом

$$Adv_{PE.A_{ATK}}^{IK-ATK}(k) = Pr[Exp_{PE.A_{ATK}}^{IK-ATK-1}(k) = 1] - Pr[Exp_{PE.A_{ATK}}^{IK-ATK-0}(k) = 1].$$

Схема *PE* вважається *IK-CPA*-безпечною (відповідно, *IK-CCA*-безпечною), якщо функція $Adv_{PKE.A}^{IK-CPA}(\cdot)$ (а отже, $Adv_{PKE.A}^{IK-CCA}(\cdot)$) є незначною для будь-якого зловмисника A, часова складність якого поліноміальна за k.

Висновки. На сьогодні запропоновано три моделі безпеки, що стосуються шифрування, електронного підпису та механізмів інкапсуляції ключів: *IND-CPA*, *IND-CCA/CCA2* для механізмів шифрування; *EUF-CMA* для механізмів підпису; модель *CK* для інкапсуляції ключів.

Безпека за будь-яким із наступних визначень означає безпеку за попередніми, тобто: схема, яка є *IND-CCA*-безпечною, також є *IND-CPA*-безпечною; схема, яка є *IND-CCA2*-безпечною, є як *IND-CCA*-безпечною, так і *IND-CPA*-безпечною. Отже, *IND-CCA2* є найсуворішим із цих трьох визначень безпеки.

Нерозрізнюваність (невизначеність) у разі атаки на основі підібраного (вибраного) відкритого тексту (*IND-CPA*) еквівалентна властивості семантичної безпеки (*SEM-CPA*). За нерозрізнюваності (невизначеності) шифртекстів відбувається захист усіх відомих криптосистем від зловмисника A, який: є імовірнісною машиною Тюрінга поліноміального часу; має всі алгоритми; володіє повним доступом до засобів зв'язку.

Подальші дослідження будуть спрямовані на вивчення властивостей криптографічної стійкості національних криптоалгоритмів.

СПИСОК ЛІТЕРАТУРИ

1. Ciphertext indistinguishability. URL: http://cse.iitkgp.ac.in/~debdeep/courses_iitkgp/FCrypto/scribes/scribe8.pdf (last accessed: 15.12.2018).
2. Henk C. A. van Tilborg, Sushil Jajodia. Encyclopedia of Cryptography and Security Springer. 2011. – 1416 p.
3. Yusuke Yoshida, Kirill Morozov, Keisuke Tanaka. CCA2 Key-Privacy for Code-Based Encryption in the Standard Model, Springer International Publishing AG 2017: PQCrypto 2017, LNCS 10346. P. 35–50. DOI: 10.1007/978-3-319-59879-6_3.
4. Dan Bogdanov. IND-CCA2 secure cryptosystems MTAT.07.006 // Research Seminar in Cryptography, 2005. URL: https://courses.cs.ut.ee/2005/crypto-seminar-fall/slides/S5.Bogdanov.indcca2.pdf (last accessed: 10.11.2018).
5. Bellare M. Symmetric encryption. URL: https://cseweb.ucsd.edu/~mihir/cse207/w-se.pdf (last accessed: 18.11.2018).

Подано 29.03.2019

М. В. Есина, С. Г. Вдовенко, И. Д. Горбенко

МОДЕЛИ БЕЗОПАСНОСТИ ПОСТКВАНТОВИХ АСИММЕТРИЧНЫХ ШИФРОВ НА ОСНОВЕ НЕРАЗЛИЧИМОСТИ

В статье приведено доказательство эквивалентности свойства неразличимости (неопределенности) свойству семантической безопасности для защиты криптосистем от криптоанализа нарушителя на основе подобранного (выбранного) открытого текста.

Вопросы анализа и исследования моделей безопасности постквантовых криптоалгоритмов по отношению к криптопримитивам всех типов, определение критериев оценки их соответствия различным моделям безопасности (согласно различным типам криптопреобразований) актуальны и имеют практическое значение. Неразличимость (неопределенность) зашифрованного текста является важным свойством безопасности многих схем шифрования, которое при атаке на основе подобранного (выбранного) открытого текста считается основным требованием для большинства достоверно защищенных криптосистем с открытым ключом. Некоторые схемы также обеспечивают неразличимость при атаке на основе подобранного (выбранного) и адаптивно подобранного (выбранного) зашифрованного текста. Использование свойства неразличимости (неопределенности) зашифрованного текста в настоящее время позволяет гарантированно осуществить защиту всех известных симметричных и асимметричных криптосистем от классического или квантового криптоанализа злоумышленника.

Рассмотрены наиболее распространенные существующие сегодня виды атак на безопасность механизмов шифрования, а именно: атака на основе адаптивно подобранных (выбранных) шифртекстов; атака на основе адаптивно подобранных (выбранных) открытых текстов; атака на основе адаптивно подобранных (выбранных) открытых текстов и адаптивно подобранных (выбранных) шифртекстов; атака на основе подобранных (выбранных) шифртекстов; атака на основе подобранных (выбранных) открытых текстов; атаки различия (разрешения).

Ключевые слова: *атака на основе адаптивно подобранных (выбранных) шифртекстов; атака на основе подобранных (выбранных) открытых текстов; неразличимость (неопределенность) зашифрованного текста; неразличимость ключей.*

M. V. Yesina, S. G. Vdovenko, I. D. Gorbenko

MODELS OF SECURITY OF POST-QUANTUM ASYMMETRIC ENCUSSION BASED ON INDISTINGUISHABILITY

The article takes a verifier of equivalence of the quality of indistinguishability (uncertainty) of the semantic security for the cryptosystems defense against of attacker's cryptanalyses based on matched (selected) open text.

The issues of analysis and research of security models of post-quantum cryptoalgorithms in relation to cryptoprimitives of all types, the definition of criteria for assessing their compliance with different security models (according to different types of crypto-transformations) are relevant and of practical importance. The indistinguishability (uncertainty) of encrypted text is an important property of the security of many encryption schemes. The indistinguishability (uncertainty) property when attacking on the basis of matched (selected) plain text is considered a basic requirement for the majority of reliably protected public-key cryptosystems. Some schemes also provide an indistinguishability for attack based on selected (selected) encrypted text and attack based on adaptively picked (selected) encrypted text. The indistinguishability (uncertainty) of an attack on the basis of a selected (selected) open text is equivalent to the properties of semantic security. If the cryptosystem has the property of indistinguishability, the attacker will not be able to distinguish between pairs of encrypted texts based on the message that they encrypt. In the case of non-differentiation (uncertainty) of ciphertext protects all known cryptosystems from the intruder which: is a probabilistic Turing machine of polynomial time; has all algorithms; has full access to communications. Using the property of the indeterminacy (uncertainty) of the encrypted text at the present time, it is guaranteed to protect all known symmetric and asymmetric cryptosystems from the classical or quantum cryptanalysis of the intruder.

Here are a review of mostly attacks on the encryption security namely an attack based on adaptively matched (selected) ciphertexts, an attack based on adaptively matched (selected) open texts, an attack based on both of this types of texts, an attack based on matched (selected) ciphertexts, an attack based on matched (selected) open texts and a recognition attacks (recognizability).

Keywords: *an attack based on adaptively matched (selected) ciphertexts; an attack based on matched (selected) open messages; indistinguishability (uncertainty) of encrypted text; Indistinguishability of keys.*

УДК 004.056.52 DOI: 10.46972/2076-1546.2019.16.03

М. В. Захарченко, В. В. Гордійчук, О. Г. Данильчук

МОДУЛІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ СКРИТНОСТІ

Аналіз засобів та принципів ведення радіоелектронної розвідки, а також технологій, які дозволяють отримати доступ до інформації, показує, що в умовах сьогодення зростає необхідність у підвищенні ефективності протидії їм. Саме тому актуальним завданням є пошук або синтез сигнальних конструкцій, що забезпечують необхідний рівень стійкості інформаційних повідомлень до можливості несанкціонованого доступу.

З цією метою в статті досліджено принципи формування сигналів на основі таймерного та позиційного кодування. Дані принципи значно відрізняються. За позиційного кодування тривалість окремих відрізків сигналу в кодовій конструкції може дорівнювати t_0, t_1 тощо. Отже, відстань між моментами модуляції кратна тривалості t_0, а кількість кодових слів становить 2^m. У ході використання таймерних сигнальних конструкцій кодове слово буде складатися з декількох інформаційних відрізків, які повинні відповідати умові $t_i = t_0 + z\Delta$, де $z \in 0;1;2;\ldots z_0$ – цілі числа. Тобто t_{ci} не може бути менше t_0, а $z\Delta$ містить інформацію про число.

У статті показано кількість реалізацій таймерних сигнальних конструкцій, потужність позиційного коду, розраховано ентропію з визначенням імовірності появи помилок за різних параметрів. Також розглянуто спосіб часового ущільнення за модулем A_0 та надано рекомендації щодо його використання для збільшення інформаційної скритності шляхом створення невизначеності в разі передачі під час шифрування.

Доведено, що використання модулів системи залишкових класів збільшить ефективність скритності інформації, що передається, за рахунок зміни ймовірності застосування окремих символів у шифрограмі, яка передається сигналом, побудованим на основі таймерних сигнальних конструкцій.

Ключові слова: *таймерні сигнальні конструкції; позиційні коди; ентропія; інформаційна скритність; елемент точності; несанкціонований доступ; інформаційна ємність.*

Постановка проблеми в загальному вигляді. З розвитком технологій радіоелектронної розвідки та несанкціонованого доступу (НСД) до інформації постійно зростає необхідність у підвищенні ефективності протидії їм. Можливими шляхами розв’язання цієї проблеми є покращення структурної та інформаційної скритності (криптостійкості) даних, що передаються.

Аналіз останніх досліджень і публікацій. НСД до інформації, що передається, передбачає виявлення і визначення структури сигналу, а також розкриття змісту повідомлення в разі його перехоплення [1], що зумовлює, у свою чергу, три види скритності сигнальних конструкцій: енергетичну, структурну й інформаційну. У зв'язку

з цим актуальним завданням є пошук і синтез таких сигнальних конструкцій, яким притаманні властивості скритності [5].

У роботі [2] описано суть таймерних сигнальних конструкцій (ТСК) та їх основні властивості. У [3] надано оцінку структурній та інформаційній скритності ТСК.

Повністю розкрито будову та властивості системи залишкових класів у [4].

Формулювання завдання дослідження. Метою статті є дослідження можливості підвищення стійкості до НСД до повідомлень, що передаються, за допомогою синтезу сигналів на основі ТСК та обробки символів відповідних шифрограм із застосуванням модулів системи залишкових класів.

Виклад основного матеріалу

1. Таймерні сигнальні конструкції

Принцип побудови ТСК полягає в такому: сигнальний алфавіт бінарних ТСК формується на інтервалі часу $\left(T_{ck} = mt_0\right)$ із мінімальною різницею довжин інформаційних відрізків величиною

$$\left|\tau_{ci} - \tau_{cj}\right| = \Delta, \ \left(\Delta = {t_0}/{S}\right).$$

Тоді на інтервалі кодового слова $T_{ck} = mt_0$ розташовано $n = mS$ відрізків Δ.

У разі позиційного кодування тривалості окремих відрізків сигналів передають двійкові цифри ("0" чи "1"), рівні тривалості найквістового елемента $t_0 = {1}/{\Delta F}$, де ΔF – смуга спектра, що пропускається (використовується). Залежно від статистичної структури переданих двійкових чисел тривалості окремих відрізків сигнали в кодовій конструкції можуть бути t_0, $2t_0$, $3t_0$ тощо. Отже, у разі позиційного кодування відстань між моментами модуляції T_M кратна тривалості t_0 $\left(T_M = kt_0; k \in \overline{1,n}\right)$, а кількість можливих кодових слів становить $N_k = 2^m$. Наприклад, якщо $m = 5$, то $N_k = 2^5 = 32$. За використання ТСК кодове слово складається з декількох інформаційних відрізків, які відповідають умові

$$t_i = t_0 + z\Delta, \tag{1}$$

де $z \in 0;1;2;\ldots z_0$ – цілі числа.

З рівняння (1) випливає, що τ_{ci} не може бути менше t_0, що забезпечує закінчення перехідного процесу, а другий доданок $z\Delta$ містить інформацію про число, яке передається. Це головна відмінність позиційного кодування (ПК) від таймерного: за ПК відстань між моментами модуляції кратна t_0, а за таймерного вона не менша найквістового елемента , але кратна Δ.

Остання особливість забезпечує істотне збільшення кількості реалізацій кодових слів на одному відрізку в разі таймерного кодування N_{PT} порівняно з позиційним $N_{PП}$ [2]:

$$N_p\left(при\ \ i=const\right)=C^{i}_{mS-i(S-1)}=\frac{\left[ms-i\left(s-1\right)\right]!}{i!\left(ms-is\right)!},\tag{2}$$

де $C^{i}_{m}=\frac{m!}{i!\left(m-i\right)!}$.

В (1)–(2) i позначає кількість відрізків у сигнальній кодовій конструкції. З даних виразів бачимо вплив окремих параметрів m, s, i на потужність N_{PT} реалізованої множини.

Для прикладу в табл. 1 наведено кількість реалізацій ТСК $\left(N_{PT}\right)$ на інтервалі $T_{ck}=mt_0s$ (в елементах Δ) і сигналів позиційного двійкового коду $N_{PП}=2^m$.

Таблиця 1

Кількість реалізацій ТСК і потужність позиційного коду $N_{PП}$ для деяких величин:

$i=3$, $T_c=mt_0s$ для $s\in 2\div 7$ та $N_{PП}=2^m$

m / s	$m=4$	$m=5$	$m=6$	$m=7$	$m=8$	$m=9$	$m=10$
	$N_{PП}=16$	$N_{PП}=32$	$N_{PП}=64$	$N_{PП}=128$	$N_{PП}=256$	$N_{PП}=512$	$N_{PП}=1024$
2	10	35	84	165	286	485	680
3	20	84	220	455	816	1330	2024
4	35	165	455	969	1771	2925	4495
5	56	286	816	1771	3276	5456	8436
6	84	455	1330	2925	5456	9139	14190
7	120	680	2024	4495	8436	14190	22900

З табл. 1 випливає: якщо $s=const$, то зі зростанням m кількість реалізацій набагато більша за $N_{PП}$; якщо $m=const$, то зі зростанням s кількість реалізацій N_P також збільшується.

У табл. 2 наведено значення величини інформації в кодових словах – ентропії $\left(H\right)$ у разі $s\in 2;3;4;5;6;7$ на інтервалі $T_{ck}\in\left(4\div 10\right)t_0$ при $i=3$, а в табл. 3 – інформаційну ємність $\left(J_H\right)$ найквістового елемента, що визначаються за такими формулами [3]:

$$\left.\begin{aligned} H&=log_2\,N_p\\ J_H&=\frac{H}{m}\end{aligned}\right\}.\tag{3}$$

Таблиця 2

Ентропія H кодових слів, якщо $m\in\left(4\div 10\right)t_0$, $s\in 2\div 7$, $i=3$

m / s	4	5	6	7	8	9	10
2	3,3	5,1	6,4	7,3	8,1	8,8	9,4
3	4,3	6,4	7,8	8,8	9,6	10,3	11
4	5,1	7,3	8,8	9,9	10,8	11,5	12,1
5	5,8	8,1	9,6	10,8	11,6	12,4	13
6	6,4	8,8	10,3	11,5	12,4	13,1	13,8
7	6,9	9,4	11	12,1	13	13,8	14,4

Таблиця 3

Інформаційна ємність J_H, якщо $m \in (4 \div 10)t_0$, $s \in 2 \div 7$, $i = 3$

s \ m	4	5	6	7	8	9	10
2	0,830482	1,065386	1,025857	1,052332	1,019984	0,98108	0,94039
3	1,080482	1,296893	1,278463	1,261389	1,209053	1,153023	1,098299
4	1,282321	1,47162	1,473264	1,417193	1,348794	1,279358	1,213411
5	1,451839	1,631974	1,612071	1,541478	1,459715	1,379292	1,304234
6	1,598079	1,765945	1,729535	1,644889	1,551703	1,46198	1,379259
7	1,726723	1,881878	1,830499	1,733444	1,630293	1,53251	1,443176
8	1,841581	1,984071	1,919037	1,810882	1,698896	1,594003	1,498855
9	1,94534	2,075442	1,997877	1,879689	1,759769	1,648516	1,54818
10	2,039968	2,15807	2,068938	1,941596	1,814478	1,697472	1,592453

З табл. 2–3 випливає:

зі зростанням m для всіх значень s ентропія H зростає;

якщо $s = const$, то зростає m, а інформаційна ємність найквістового елемента максимальна за $m = 5$;

якщо $m = const$, то зростає s, збільшується величина J_H (імовірність помилок також зростає за рахунок зменшення Δ).

Необхідно зазначити, що інформаційна ємність одного найквістового елемента зростає до значення $m = 5$, а якщо $m > 5$, то вона зменшується (табл. 3). Отже, ефективна швидкість передачі, тобто кількість інформації, що передається, на інтервалі $T_{ck}(4 \div 6)t_0$ збільшується, а на $T_{ck}(6 \div 10)t_0$ зменшується.

На рис. 1 показано залежності інтервалу реалізації (m) для заданої кількості N_{PT} у разі збільшення s.

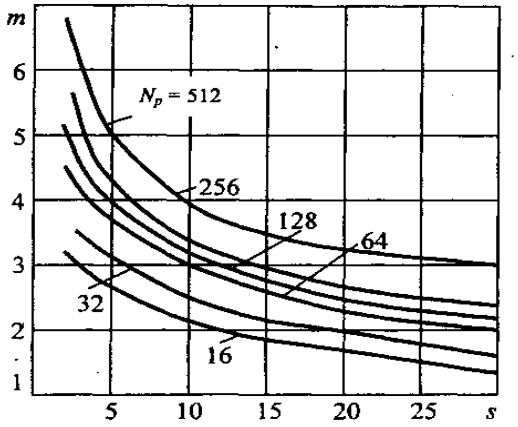


Рис. 1. Залежності тривалості сигнальної конструкції в разі заданої потужності кодової множини та параметра s

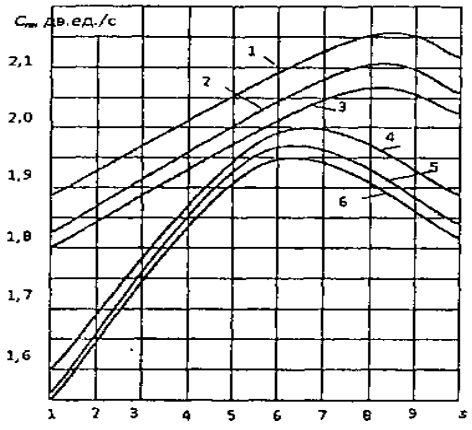


Рис. 2. Залежності пропускної здатності каналу $C_i = f(S)$ за $h = const$, $m = const$

Враховуючи, що кількість інформації, яка надходить до одержувача, менша тієї, що передається, на величину H_n (втрат) [2], то

$$H_n = -\left[P_{np} \log_2 P_{np} + \left[\left(1 - P_{np}\right) \log_2 \frac{1 - P_{np}}{N_p} \right] \right], \tag{4}$$

де P_{np} – імовірність правильного прийому.

Отже, швидкість передачі інформації на 1 елемент дорівнює

$$C = \frac{1}{m} \left[\log_2 N_p - H_n \right] \text{біт/с}. \tag{5}$$

На рис. 2 наведено залежності швидкості передачі $c = f(s)$ для двох значень h: залежності 1, 2, 3 для $h_1 = 7{,}5$ та $m = 8, 6, 5$ відповідно; залежності 4, 5, 6 для $h_2 = 5{,}5$ і для тих самих значень m.

З рис. 2 випливає, що для кожного значення h існує величина зони $\Delta(s)$, за якої C_m буде максимальною: зростаюча частина зазначених залежностей характеризується великим впливом збільшення кількості реалізацій (5), а спадна – значним впливом втрат H_n (2).

2. Часове ущільнення за $(mod\ A_0)$

З метою створення умов оцінювання якості передачі в ТСК, що формуються, значущі моменти модуляції розташовані на місцях, які відповідають певним співвідношенням [3]:

$$A_1 x_1 + A_2 x_2 + \ldots + A_n x_n \equiv 0 (mod\ A_0), \tag{6}$$

де x_n – тривалості окремих інформаційних відрізків у межах сигнальних конструкцій;

A_i – цілі числа, що визначають кодову відстань (у Δ) дозволених сигнальних конструкцій.

Окрім цього, за використану множину можуть синтезуватися кодові конструкції як з однаковою кількістю інформаційних відрізків i, так і з різною. Для створення умов конфіденційності модулі порівняння доцільно змінювати, що забезпечує збільшення інформаційної скритності.

Розглянемо багатоканальну систему з модульним поділом.

Припустимо, що є чотири різні модулі: $A_{01} = 11$, $A_{02} = 13$, $A_{03} = 17$, $A_{04} = 19$. Нехай інтервал реалізації $T_{ck} = 7t_0$ за $s = 7$, $i = 3$.

Згідно з виразом (2) кількість реалізацій з трьома відрізками буде $N_p = 4495$ [2]. Із цієї множини відповідати умовам (6) за різних A_{0i} будуть тільки $N_{PT}(A_{0i})$ [3]:

$$N_p'(A_0(i)) = N_{PT} \Big/ A_{0i}. \tag{7}$$

Тоді кількість реалізацій, які задовольняють умову (6), становить: $N_p'(11) = 4495/11 \approx 409$, $N_p'(13) = 4495/13 \approx 345$, $N_p'(17) = 4495/17 \approx 265$, $N_p'(19) = 4495/19 \approx 236$.

З огляду на те, що в зазначених $N_p'(A_0)$ є однакові сигнальні конструкції, за різних суміжних A_0 маємо:

$$N_p(11)\bigcap N_p(13)=36,\ N_p(11)\bigcap N_p(17)=20,$$
$$N_p(11)\bigcap N_p(19)=28,\ N_p(13)\bigcap N_p(17)=28,$$
$$N_p(13)\bigcap N_p(19)=13,\ N_p(\ )17\bigcap N_p(19)=12),$$

їх необхідно виключити в тій множинні $N_p(A_0)$, у якій міститься більше число N_P.

Унаслідок виключень отримаємо:

$$N_p(11)/\bigcap=409-(36+20+28)=325,$$
$$N_p(13)/\bigcap=345-(28+13)=301,$$
$$N_p(17)/\bigcap=265-12=253.$$

Будемо вважати, що загальна кількість переданих символів становить 60: 32 літери російської мови; 10 цифр; 4 символи арифметичних дій; 2 символи суми і добутку; 2 символи включення і виключення; 10 грецьких символів.

60 символів, що підлягають передачі, кодуються в кожній групі за різними модулями. Оскільки їх чотири, то в ході хаотичного вибору синтезується одна з комбінацій символу при цьому модулі.

З метою створення більшої невизначеності для сторонніх осіб символи краще передавати з різними значеннями модулів A_0. Наприклад, символи на позначення: голосних звуків – з $mod\,11$, приголосних – з $mod\,13$, арифметичних дій – з $mod\,17$, грецьких літер – з $mod\,19$ тощо.

Для збільшення невизначеності передачі під час шифрування для кожного переданого символу можна використовувати заміну його на символ, зміщений в алфавіті на z номерів, або застосувати спосіб змішування. Величина z може змінюватися відповідно до модуля порівняння: змінюючи його, можна одночасно змінювати і кількість інформаційних відрізків "i" у кодових словах, що формуються на передачу.

Висновки. У статті розглянуто особливості формування ТСК та їх можливості щодо підвищення скритності інформації, якої досягають за рахунок складності детермінації (дешифрування) сигналу, оскільки його структура є принципово новою порівняно з відомими: зміщено значущі моменти модуляції (на відміну від позиційних сигналів); інформацію поелементно закладено у відрізках, не кратних найквістовому елементу тощо.

З тією ж метою розглянуто властивості системи залишкових класів, за допомогою якої можна задавати ряд невизначеностей щодо послідовності кодованих символів: символи, що підлягають передачі, необхідно надсилати з різними значеннями модулів A_0; для кожного переданого символу слід використовувати заміну його на символ, зміщений в алфавіті на z номерів, або використовувати їх змішування.

Отже, доведено, що використання модулів системи залишкових класів збільшить ефективність скритності інформації, що передається, за рахунок зміни ймовірності застосування окремих символів у шифрограмі, яка передається сигналом, побудованим на основі ТСК.

СПИСОК ЛІТЕРАТУРИ

1. Куприянов А. И., Сахаров А. В. Теоретические основы радиоэлектронной борьбы. Москва : Вузовская книга, 2007. 356 с.
2. Захарченко М. В. Системи передавання даних. Т. 1. Завадостійке кодування. Одеса : Фенікс, 2009. 477 с.
3. Таймерные сигнальные конструкции как инструмент системы информационной безопасности / М. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский, Ю. С. Горохов // Вимірювальна та обчислювальна техніка в технологічних процесах. 2015. № 1. С. 256–259.
4. Обработка информации в системе остаточных классов (СОК) : учеб. пособ. / Н. И. Червяков, П. А. Ляхов, Л. Б. Копыткова, А. В. Гладков. Ставрополь : Изд-во СКФУ, 2016. 225 с.
5. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. Киев : Юниор, 2003. 504 с.

Подано 20.12.2018

Н. В. Захарченко, В. В. Гордейчук, А. Г. Данильчук

МОДУЛИ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ КАК ИНСТРУМЕНТ ИНФОРМАЦИОННОЙ СКРЫТНОСТИ

Анализ средств и принципов ведения радиоэлектронной разведки, а также технологий, которые позволяют получить доступ к информации, показывает, что в современных условиях возрастает необходимость в повышении эффективности противодействия им. Именно поэтому актуальной задачей является поиск или синтез сигнальных конструкций, обеспечивающих необходимый уровень стойкости информационных сообщений к возможности несанкционированного доступа.

С этой целью в статье исследованы принципы формирования сигналов на основе таймерного и позиционного кодирования. Данные принципы сильно отличаются. При позиционном кодировании длина отдельных сегментов сигнала в структуре кода может быть равна t_0, t_1 *и т. д. Таким образом, расстояние между моментами модуляции кратно длине* t_0 *и точному количеству кодовых слов* 2^m. *При использовании таймерных сигнальных конструкций кодовое слово будет состоять из нескольких информационных разделов, которые должны соответствовать условию* $t_i = t_0 + z\Delta$, *где* $z \in 0;1;2;\dots z_0$ – *целые числа. Следовательно,* t_{ci} *не может быть меньше* t_0, *а* $z\Delta$ *содержит информацию о числе.*

В статье показаны количество реализаций таймерных сигнальных конструкций и мощность кода позиции, рассчитана энтропия, указывающая вероятность ошибок в различных параметрах. Также рассмотрен метод консолидации времени по модулю A_0 *и даны рекомендации по его использованию для повышения скрытности информации путем генерирования неопределенности при передаче во время шифрования.*

Кроме того, доказано, что использование модулей системы остаточных классов увеличит эффективность скрытности информации, передаваемой сигналом, построенным на основе таймерных сигнальных конструкций.

Ключевые слова: *таймерные сигнальные конструкции; позиционные коды; энтропия; информационная скрытность; элемент точности; несанкционированный доступ; информационная емкость.*

M. V. Zaharchenko, V. V. Hordiichuk, O. G. Danylchuk

MODULES OF THE RESIDUAL CLASSES' SYSTEM AS AN INFORMATION ACCURACY TOOL

An analysis of the means and principles of electronic intelligence, as well as technologies, that allow access to information, shows that in modern conditions, the need for increasing the effectiveness of countering them is growing. That is why the urgent task is the search or synthesis of signal structures that provide the necessary level of resistance of information messages to the possibility of unauthorized access.

To this end, the article explores the principles of signal generation based on timer and position coding. These principles are very different. In positional coding, the length of individual signal segments in the code structure can be equal t_0, t_1 *and so on. Thus, the distance between the moments of modulation is a multiple of the length* t_0 *and the exact number of code words* 2^m. *When using timer signal constructions, the code word will consist of several information sections that must correspond to the condition* $t_i = t_0 + z\Delta$, *where* $z \in 0;1;2;...z_0$ *are integers. Therefore,* t_{ci} *cannot be less* t_0, *but* $z\Delta$ *contains information about the number.*

The article shows the number of implementations of timer signal structures and power of the position code, entropy calculated indicating the probability of errors in various parameters. Also considered is a modular time consolidation method and recommendations are given for its use to increase the secrecy of information by generating uncertainty during transmission during encryption.

In addition, it is proved that the use of modules of the system of residual classes will increase the efficiency of secrecy of information transmitted by a signal constructed on the basis of timer signal structures.

Keywords: *timer constructions; position codes; entropy; precision element; information secrecy; preciseness element; information capacity.*

УДК 623.618 DOI: 10.46972/2076-1546.2019.16.04

І. А. Пількевич, О. М. Перегуда, О. П. Черкес

ОСОБЛИВОСТІ ПРОЄКТУВАННЯ АРХІТЕКТУРИ ІНФОРМАЦІЙНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ З ВИКОРИСТАННЯМ NATO ARCHITECTURE FRAMEWORK НА ПРИКЛАДІ НАУКОВО-ДОСЛІДНОГО ПІДРОЗДІЛУ

У статті запропоновано використання методологічного підходу NATO Architecture Framework v. 4.0 для опису архітектури інформаційної системи військового призначення, який доповнено методикою побудови моделей Architecture Development Method (взятою з методології The Open Group Architecture Framework).

Наведена методологія дозволяє здійснювати комплексне проєктування та подальше супроводження архітектури інформаційної системи військового призначення на основі застосування моделей. Вона класифікує основні елементи архітектури на різних рівнях абстракції, єдині політики (правила) для опису їх взаємодії один з одним, забезпечує підтримку прийняття рішень у контексті виконання стратегічної місії, тактичних та оперативних завдань. Супроводження архітектури інформаційної системи на основі застосування моделей дозволяє налаштовувати середовище моделювання таким чином, щоб застосовувати стандарти та правила в процесі збору інформації. Введення інформації та управління нею відповідно до NATO Architecture Framework допомагає досягнути узгодженості, зрозумілості та точності на всіх рівнях архітектури.

Для апробації запропонованого підходу розроблено метамодель архітектури наукового підрозділу з використанням спеціалізованого програмного забезпечення Cameo Enterprise Architecture, функціонал якого орієнтований на спільну роботу, що забезпечує: інтеграцію моделей, створених за різними стандартами; можливість перевірки моделі на повноту та правильність; візуалізацію даних, це сприяє відображенню моделі у вигляді діаграм, таблиць, матриць відношень, часових графіків, мапи відношень, звітів тощо.

Створена метамодель може бути використана для: формування та корегування стратегічних (довготермінових), тактичних (річних, місячних) та оперативних цілей (завдань) підрозділу; оптимізації основних процесів діяльності підрозділу; раціонального розподілу наявних ресурсів та з'ясування потреб у додаткових ресурсах; визначення місця та порядку впровадження засобів автоматизації; тиражування позитивного досвіду побудови архітектури підрозділу тощо.

Ключові слова: *інформаційна система; архітектура підприємства; Architecture Framework; NAF.*

Постановка проблеми в загальному вигляді. з урахуванням євроатлантичних прагнень України процес розбудови сфери оборони за єдиним задумом та підходом вимагає використовувати прийняті в країнах – членах НАТО принципи адміністрування, висуває цілу низку нових системних вимог щодо рівня технологічного (у тому числі й програмного) забезпечення системи військового управління. Значна частина «вузьких місць» у системі військового управління локалізується в сегменті збільшення інформаційних потоків і, відповідно, потребує ефективної роботи з ними. Функціонування

сучасної складної (корпоративної) інформаційної системи (ІС) повинно будуватися навколо основних процесів діяльності (бізнес-процесів, далі – Процесів) організації (органу військового управління, військової частини (установи, закладу, організації, підприємства, підрозділу, організаційного чи організаційно-технічного елементу) в Збройних Силах (Міністерстві оборони (МО)) України (далі – Організації). Процеси в Організації повинні підтримувати динамічний розвиток, а не жорсткі правила та забезпечувати наскрізний доступ та зв'язок інформації за горизонтальним (у межах вирішення різних прикладних (тематичних) завдань) та вертикальним напрямами – між стратегічними цілями та завданнями (задачами) тактичного рівня. Організаційно-технічна складова повинна бути гнучкою та підлаштовуватися під Процеси та відповідні їм інформаційні моделі (структури, потоки) управління корпоративним контентом. Процеси повинні здійснюватися відповідно до вимог керівних документів, наприклад [1–4].

У ході виконання зазначених вимог виникають складності, подолання яких зводиться до забезпечення раціонального підходу до процесу проєктування, реалізації й подальшої експлуатації ІС Організації, встановлення взаємозв’язків між різними складовими ІС. Розглядаючи архітектуру ІС як сукупність взаємопов’язаних функціональної, організаційної та організаційно-технічної структур, можна однозначно вважати обрану архітектуру одним з основних показників ефективності створюваної ІС, а отже, і показником успішності військового управління (ефективності реалізації рішень у всій ієрархії системи управління – від рішень вищого військово-політичного керівництва до окремого підрозділу). Отже, актуальним є впровадження методології проєктування та реалізації архітектури ІС військового призначення й подальшого її супроводження в процесі експлуатації.

Аналіз останніх досліджень та публікацій. Сучасна методологія Architecture Framework (AF) дозволяє здійснювати комплексне проєктування та подальше супроводження архітектури ІС [5]. У термінології AF архітектура ІС розглядається як Enterprise Architecture (EA). AF описує перелік осіб (stakeholders), що взаємодіють з ІС, та їх інтереси, типові проблеми предметної області, архітектурні «точки зору» (часткові описи окремих складових EA) і методи їх інтеграції. У разі використання AF з’являється можливість комплексно коригувати функціональність ІС за рахунок ітерації процесу проєктування, коли зміни стратегічних цілей втілюються в конкретних змінах організаційно-технічної структури. У свою чергу, AF є складовим елементом більш глобального підходу – MBSE (Model Based Systems Engineering) – моделеорієнтованого системного проєктування [6]. MBSE, на відміну від традиційного документоорієнтованого підходу, передбачає створення та використання моделей ІС на всіх етапах її життєвого циклу. На даний час загальна кількість відомих AF більше 70 [7]. Розглянемо найбільш розповсюджені AF.

За допомогою TOGAF (The Open Group Architecture Framework) ІС подається як сукупність модулів, що описують цілісний підхід до розробки EA для чотирьох рівнів: бізнес-архітектура; архітектура рівня додатків; архітектура рівня даних; технічна архітектура [8, 9]. Відповідно до методики ADM (Architecture Development Method) TOGAF [10], процес побудови EA є ітераційним, поділяється на фази та має два рівні. На верхньому рівні кожної ітерації повторюються загальні для кожної з фаз дії. Нижній

описує ітерації всередині кожної фази. TOGAF отримав найбільше практичне використання у світі, зорієнтований на застосування в промислово-комерційній сфері, може використовуватися в сукупності з іншими AF, зокрема з AF Захмана.

Оборонні відомства провідних держав використовують: DoDAF (Department of Defense Architecture Framework) – США, MoDAF (Ministry of Defense Architecture Framework) – Великобританія та Швеція, NAF (NATO Architecture Framework) – решта країн НАТО. Як можливий перспективний єдиний універсальний AF розглядається UAF (Unified Architecture Framework) [7, 11, 12].

AF DoDAF [8] визначає загальний підхід до опису ЕА для відображення військових дій (операцій) та Процесів (у військовій сфері). Забезпечує порівняння описів архітектури різних військових ІС, у тому числі не військових, які задіяні в спільних місіях (військових операціях). Основним класом систем, що проєктуються за допомогою цього AF, є системи збору, зберігання та аналізу даних для підтримки прийняття рішень [9]. Головна особливість даного AF – високі вимоги щодо захищеності та збереження даних, їх повторного використання. На його базі були сформовані AF NAF, MODAF та інші.

На даний час у НАТО використовують версію NAF v 3.2 [12, 13], розробляють та обговорюють NAF v 4 [14], для якої визначено перелік моделей (Viewpoints) і спосіб їх формалізованого опису.

Відкритим залишається питання методології побудови моделей: передбачається, що її основою буде методологія TOGAF ADM із комбінацією інших підходів (наприклад, стандартів проєктування систем, таких як ISO15288). Частина провідних країн Північноатлантичного альянсу вже заявила про відмову в перспективі від власних AF та перехід на NAF v 4, який підтримує сумісність із поточними діючими версіями DoDAF, MODAF, NAF [11–13].

Досвід використання Збройними силами Норвегії методології NAF ґрунтується на фактичному об’єднанні структури TOGAF ADM і NAF [15]. У ході впровадження метамоделі з’ясувалося, що використання загальної методології недостатньо для моделювання архітектури ІС, тому були розроблені індивідуальні методології для управління вимогами на рівні проєкту та портфоліо, а також для надання інтегрованих рішень за проєктами.

Під час проєктування архітектури Command and Control Information System (C2IS) одночасно використано метамодель NAF та методологію TOGAF ADM [16].

У [17] запропоновано підхід для використання моделей NAF у разі реорганізації MODAF, визначено критерії для оцінювання та порівняння наслідків такого переходу.

В Україні запропоновано інформаційну інфраструктуру МО України з функціональними підрозділами та різноманітним набором технологій [18]. Акцент було зроблено на системно-архітектурній методології військового призначення класу C4ISR із можливістю використання відповідних AF (DODAF, MODAF, NAF).

Інші AF (GERAM, FEA, Gartner) мають набагато менше практичне застосування [7].

Формулювання завдання дослідження. Для України, з урахуванням її євроатлантичних стратегічних прагнень і необхідності розбудови корпоративної ІС для

сфери оборони за єдиним задумом та підходом, доцільним є використання NAF v 4.0, тому дослідження особливостей її використання є актуальним.

Мета статті – розглянути підходи методології NATO NAF v 4.0 та провести аналіз особливостей проєктування архітектури ІС на прикладі науково-дослідного підрозділу.

Виклад основного матеріалу. NAF забезпечує стандартизований спосіб розробки складових елементів (artefacts) архітектури ІС, визначає основні методологічні напрямки дослідження діяльності ІС на різних фазах (етапах) її життєвого циклу.

NAF v 4.0 [19] традиційно, як і інші AF, складається з таких компонент:

Viewpoints (з англ. «точка зору») – це впорядкований набір структурних схем (діаграм, моделей), які відображають особливості побудови та функціонування ІС у різних сферах застосування, на різних рівнях абстракції, у статиці та динаміці. Кожна схема будується з урахуванням певної «точки зору» – способу надання та формалізованого опису ІС (або її частини), які відображають реалізацію функцій, контроль та виконання завдань в інтересах «учасників» ІС (stakeholders): власників, користувачів, обслуги, менеджерів тощо. Для опису ІС на кожному етапі її життєвого циклу використовується свій набір Viewpoints (набір Viewpoints NAF v 4.0 наведено в табл. 1).

Таблиця 1

Viewpoints («точки зору») NAF v 4.0

Точка зору	Таксономія	Структура	Зв'язок	Діяльність	Стан	Послідовність	Інформація	Обмеження	Дорожня карта
Концепція	C1	C2	C3	C4		C6	C7		Cr
Технічна специфікація	S1		S3	S4	S5	S6	S7		
Логічна специфікація	L1	L2	L3	L4	L5	L6	L7	L8	Lr
Специфікація фізичних ресурсів	P1	P2	P3	P4	P5	P6	P7	P8	Pr
Структура ресурсів	D1	D2							
Метадані архітектури	A1							A8	

Method – методологія (сукупність взаємопов'язаних методів, правил та умов їх застосування) створення та використання (моделювання, проєктування, верифікація, тестування) Viewpoints (структурних схем) ІС.

Language – формалізована мова, яку використовують для опису елементів системи та зав'язків між ними (в окремих AF дану складову розглядають ширше й оперують поняттям метамоделі (онтології), включаючи до неї перелік усіх сутностей AF). NAF v 4.0 як основний засіб формалізації використовує UPDM (Unified Profile for DoDAF/MODAF) [20].

Архітектура ІС (у розумінні ЕА) становить собою модель ІС з описом Процесів в умовах нестабільного зовнішнього середовища. ЇЇ поділяють на базову, яка описує поточний стан системи, та цільову архітектуру, яку необхідно мати для реалізації стратегічних цілей та набуття визначених спроможностей ІС (з урахуванням прийнятих обмежень) [8].

Особливість використання методології NAF v 4.0 полягає в тому, що модель ЕА будують шляхом послідовного заповнення двомірної матриці на визначених рівнях абстракції: концептуальному (Concepts), логічному (Logical), фізичному (Physical), технічному (Service), метаданих архітектури (табл. 1). Даний підхід є інформаційно-орієнтованим, він поділяє структуру на архітектурні категорії залежно від виду інформації [14], відбувається декомпозиція. Матриця дозволяє користувачам вибирати потрібну модель залежно від виду інформації (горизонтальна вісь) та її специфікації (вертикальна вісь).

Для безпосереднього створення та використання моделей ЕА застосовують засоби моделювання (спеціалізоване програмне забезпечення). Спроможність формувати (редагувати), інтегрувати та підтримувати (супроводжувати) моделі ЕА залежить від можливостей інструменту моделювання. Більшість із них (IBM Rhapsody, No Magic MagicDraw, PTC Integrity Modeler) підтримують використання UPDM (Unified Profile for DoDAF/MODAF) – єдиного профілю (способу формалізації моделей) для DoDAF та MODAF (із підтримкою NAF та DNDAF), а також забезпечують інтеграцію з відомими стандартами OMG (Group Object Management Group), наприклад, SysML (Systems Modeling Language) та UML (Unified Modeling Language). За основний інструмент моделювання для вирішення визначених у статті завдань обрано програмне забезпечення Cameo Enterprise Architecture (MagicDraw) [19], що зумовлено підтримкою таких стандартів, як UPDM, SysML, BPMN (Business Process Model and Notation), UML, а також незначними обмеженнями функціонала пробної версії. Cameo Enterprise Architecture забезпечує: інтеграцію моделей ЕА в єдине сховище для об’єднання елементів з інших моделей, створених за різними стандартами; функціонал, орієнтований на спільну роботу (звернення до загального репозиторію, одночасне редагування моделі, керування версіями); можливість перевірки моделі на повноту та правильність. Візуалізація даних дає можливість відображати модель у вигляді діаграм, таблиць, матриць відношень, часових графіків, мапи відношень, звітів.

Відповідно до методології ADM опис ЕА в рамках NAF v 4.0 доцільно здійснювати таким чином. Першим кроком на шляху є збір метаданих [22], який включає в себе документування чітких визначень і описів усіх артефактів, що формують уявлення про ІС. Використання єдиного засобу моделювання та однакових методів усіх учасників процесу істотно знижують суперечності зібраних даних, роблять їх загальнодоступними.

Наступним кроком є визначення взаємозв'язків між метаданими, що і становить основну цінність підходу до створення ЕА. У ході цього процесу відбувається трансформація (інтеграція) кожної області метаданих у взаємозалежність об'єктів, що в подальшому може бути використано для проведення комплексного різнобічного аналізу, зокрема управління змінами з прогнозованим результатом, дослідження взаємозв'язків, оцінювання ризику та витрат, аналізу відмінності між архітектурою «яка є» (базовою) і «яка буде» (цільовою) тощо. Інтегровані метадані зберігаються в репозиторії.

Останнім етапом інтеграції метаданих є визначення залежностей. За допомогою єдиного інструменту опису ЕА можна з'ясувати: як стратегічні, тактичні та оперативні цілі пов'язані з реальними об’єктами; яким чином нормативно-правові вимоги впливають на потоки інформації; до яких фінансових витрат призводять зміни технологій.

Опис залежностей метаданих в інтегрованому середовищі візуалізується у формі метамоделі [14]. Шаблон її будови наведено на рис. 1.

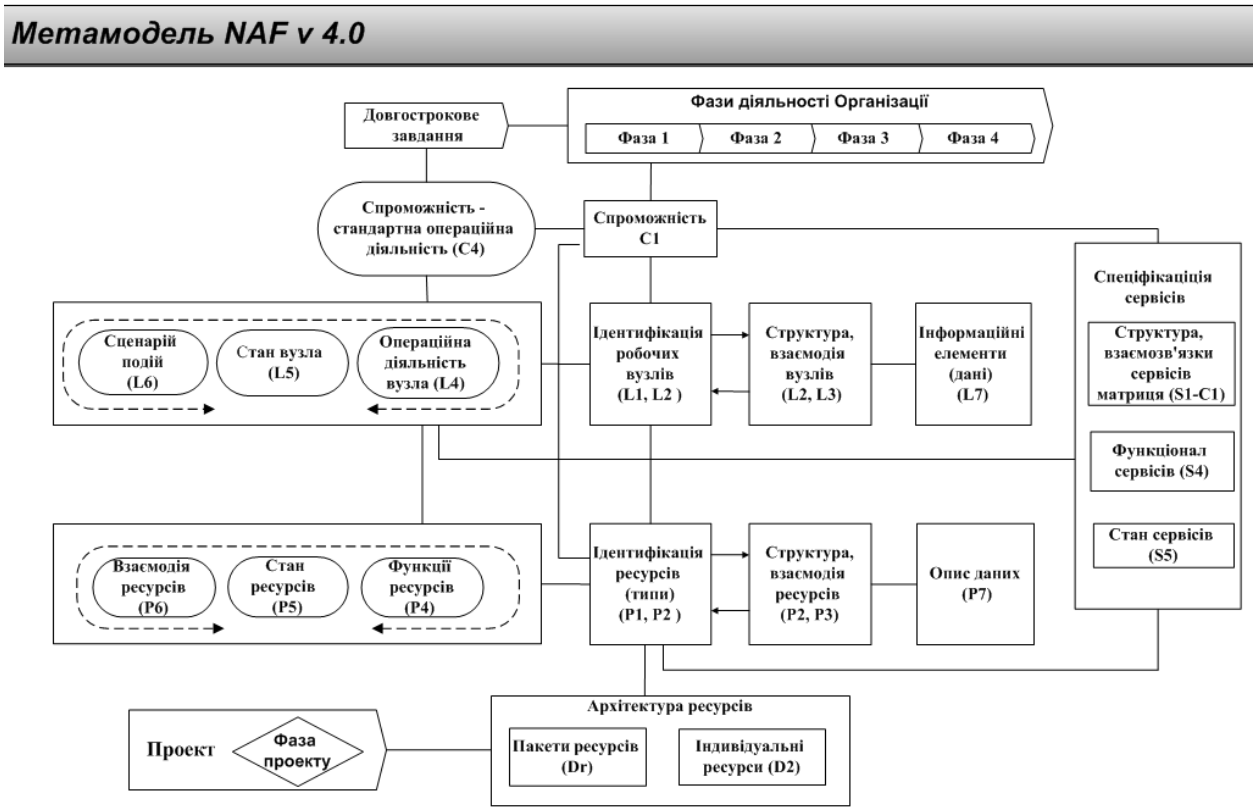


Рис. 1. Метамодель NAF v 4.0

У шаблоні визначено основні елементи моделювання, які можуть використовуватися для опису системи на рівні ІС або на рівні окремого проєкту (задачі). Метамоделі проєктів можуть інтегруватися в модель ІС. Вхідними даними для побудови мета моделі є довгострокове завдання, на виході отримуємо архітектуру ресурсів для кожної фази проєкту.

Далі як приклад практичного застосування NAF v 4.0 наведено окремі моделі (діаграми), що описують діяльність наукового підрозділу. Для визначення спроможностей наукової діяльності необхідно з’ясувати: мету, цілі та завдання наукової діяльності; пріоритетні напрями наукових досліджень; перспективи розвитку структурних наукових підрозділів; організаційні форми наукової діяльності; вимоги до кадрового та науково-інформаційного забезпечення; механізм упровадження в практику наукових розробок; форми науково-технічного співробітництва.

«Точки зору» Concepts забезпечують процес аналізу спроможностей відповідно до глобальних, стратегічних цілей (С2). Спроможності організовуються в таксонометрію (С1), доповнюються показниками ефективності (С7) та даними про етапи виконання (дорожня карта Cr). Залежності між спроможностями відображаються на діаграмі С3, а взаємозв'язки між ними та стандартною операційною діяльністю описує діаграма С4.

Наведений приклад діаграми С1 (рис. 2) відображає ієрархічну структуру спроможностей та їх місце в таксономії на прикладі діяльності науково-дослідного підрозділу.

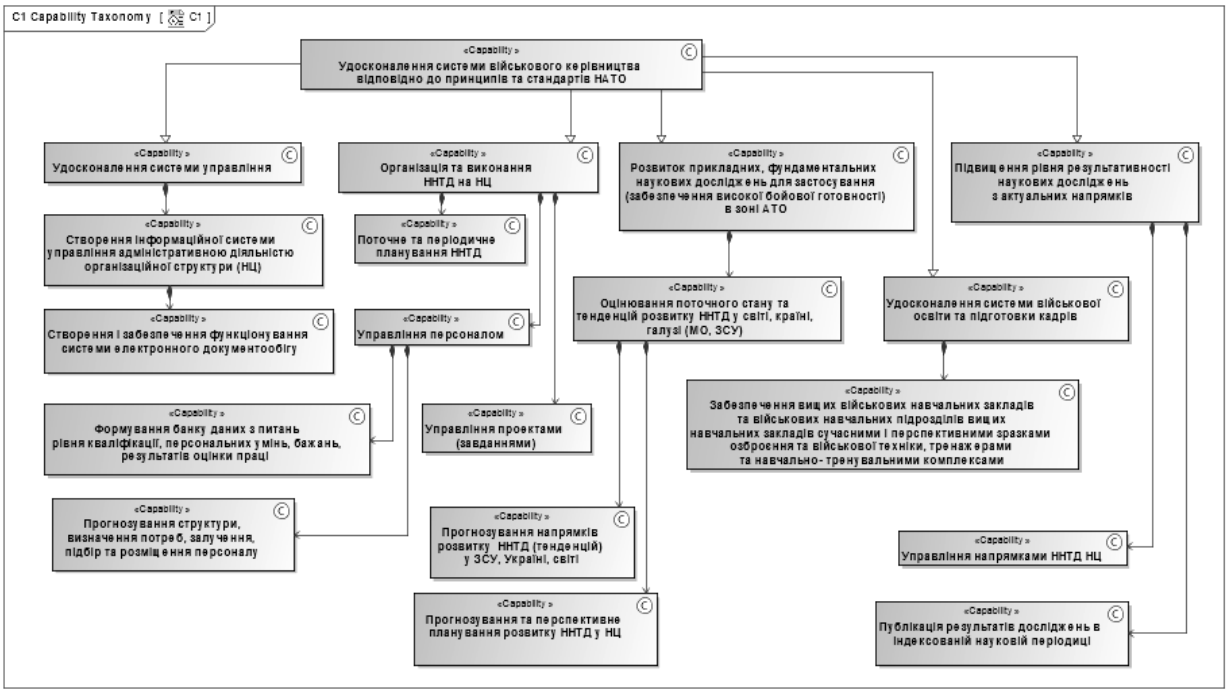


Рис. 2. Діаграма C1 Capability Taxonomy

Матриця C4-L4 ідентифікує стандартну операційну діяльність, яка забезпечує реалізацію спроможностей (рис. 3). «Точки зору» Logical ідентифікують логічні вузли (логічні або фізичні елементи архітектури з визначеним функціоналом), це можуть бути програмні або технічні засоби, окремі виконавці чи їх групи, які забезпечують реалізацію Процесів, відображають обмін ресурсами / інформацією між вузлами (L1) та їх взаємодію (L2, L3), що дає можливість визначати вимоги до функціональної сумісності, потреби у співпраці (взаємодії), аналізувати потоки постачання матеріальних засобів, енергії, кадрових ресурсів, виконувати оперативне планування.

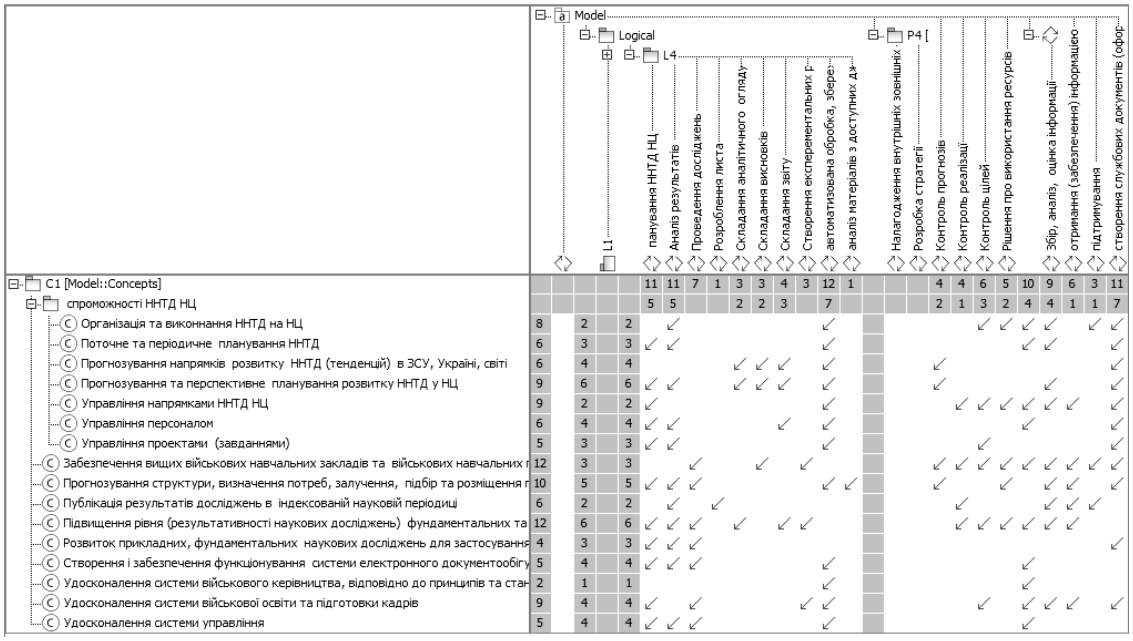


Рис. 3. Матриця C4- L4 Standard Processes

Наведений приклад діаграми L1 (рис. 4) показує таксономію логічних вузлів для забезпечення реалізації спроможності «Організація та виконання ННТД» у науковому підрозділі. У даному разі вузли визначаються функціоналом, що передбачає збереження,

вироблення, споживання або обробку інформації оперативного та тактичного рівнів, призначення якої – відповідати на поточні питання та моніторити стан справ.

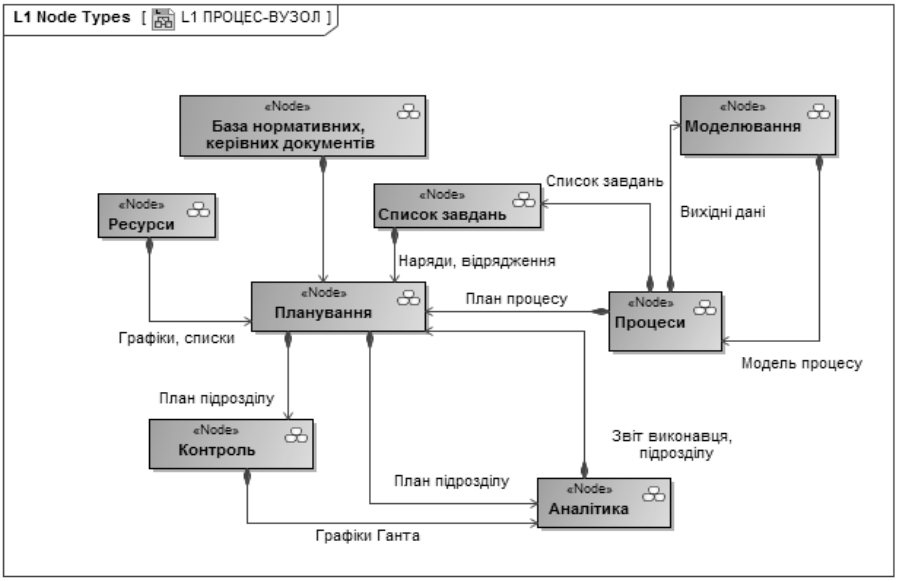


Рис. 4. Діаграма L1 High-Level Operational Concept Description

Наведений приклад діаграми L2 (рис. 5) показує взаємодію між вузлами для виконання типової діяльності (Процесу) – «Виконання науково-дослідної роботи». Залежність між вузлами відображається в контексті інформації, якою обмінюються вузли. Сценарій взаємодії може включати декілька рівнів: стратегічний, тактичний та оперативний. Взаємодія вузлів з урахуванням функціональних змін може доповнюватися або змінюватися.

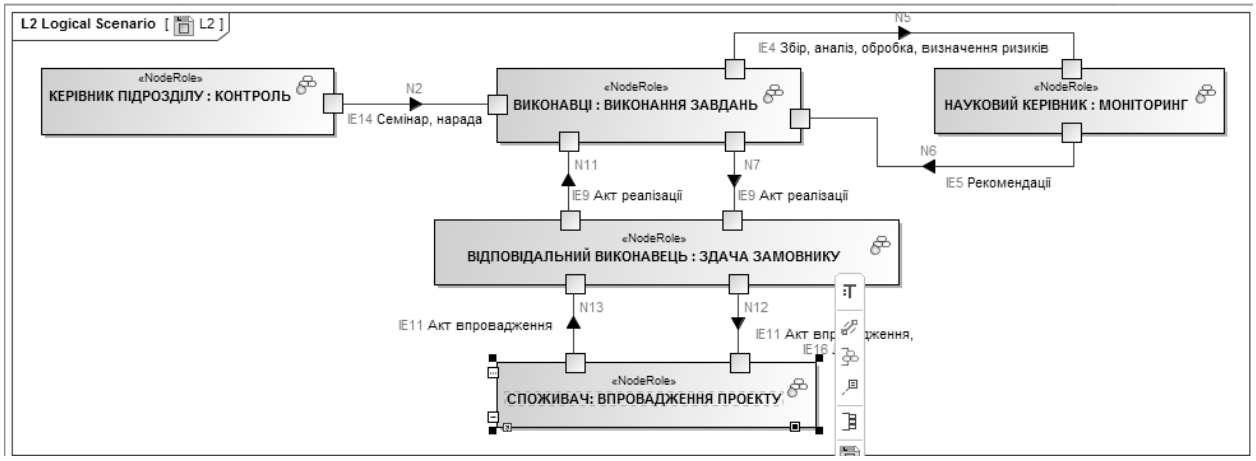


Рис. 5. Діаграма L2 logical scenario

У діаграмі L3 (рис. 6) відображено інформаційні потоки між вузлами. Обмін інформацією між ними вимагає додаткової деталізації вимог до їх функціональної сумісності.

#	Exchange ID	Operational Exchange Item	Sending Role	Sending Node	Receiving Role	Receiving Node
1	OE28	IE5 Рекомендації	НАУКОВИЙ КЕРІВНИК	МОНІТОРИНГ	ВИКОНАВЦІ	ВИКОНАННЯ ЗАВДАНЬ
2	OE27	IE4 Збір, аналіз, обробка, визначення ризиків	ВИКОНАВЦІ	ВИКОНАННЯ ЗАВДАНЬ	НАУКОВИЙ КЕРІВНИК	МОНІТОРИНГ
3	OE33	IE9 Акт реалізації	ВИКОНАВЦІ	ВИКОНАННЯ ЗАВДАНЬ	ВІДПОВІДАЛЬНИЙ ВИКОНАВЕЦЬ	ЗДАЧА ЗАМОВНИКУ
4	OE30	IE9 Акт реалізації	ВІДПОВІДАЛЬНИЙ ВИКОНАВЕЦЬ	ЗДАЧА ЗАМОВНИКУ	ВИКОНАВЦІ	ВИКОНАННЯ ЗАВДАНЬ
5	OE31	IE11 Акт впровадження	ВІДПОВІДАЛЬНИЙ ВИКОНАВЕЦЬ	ЗДАЧА ЗАМОВНИКУ	СПОЖИВАЧ: ВПРОВАДЖЕННЯ ПРОЕКТУ	
6	OE32	IE16 Лист	ВІДПОВІДАЛЬНИЙ ВИКОНАВЕЦЬ	ЗДАЧА ЗАМОВНИКУ	СПОЖИВАЧ: ВПРОВАДЖЕННЯ ПРОЕКТУ	

Рис. 6. Таблиця Node Interactions

Наведений приклад діаграми L4 (рис. 7) показує зв'язок операційної діяльності з вузлами для виконання типової діяльності (Процесу) наукового підрозділу «Виконання науково-дослідної роботи». Крім того, він встановлює логічні потоки, що дає можливість чітко визначити межі відповідальності, у поєднанні з L2 виявити зайву операційну діяльність, забезпечити необхідну основу для відображення послідовності дій та часу виконання операційної діяльності в діаграмах L5, L6, L8.

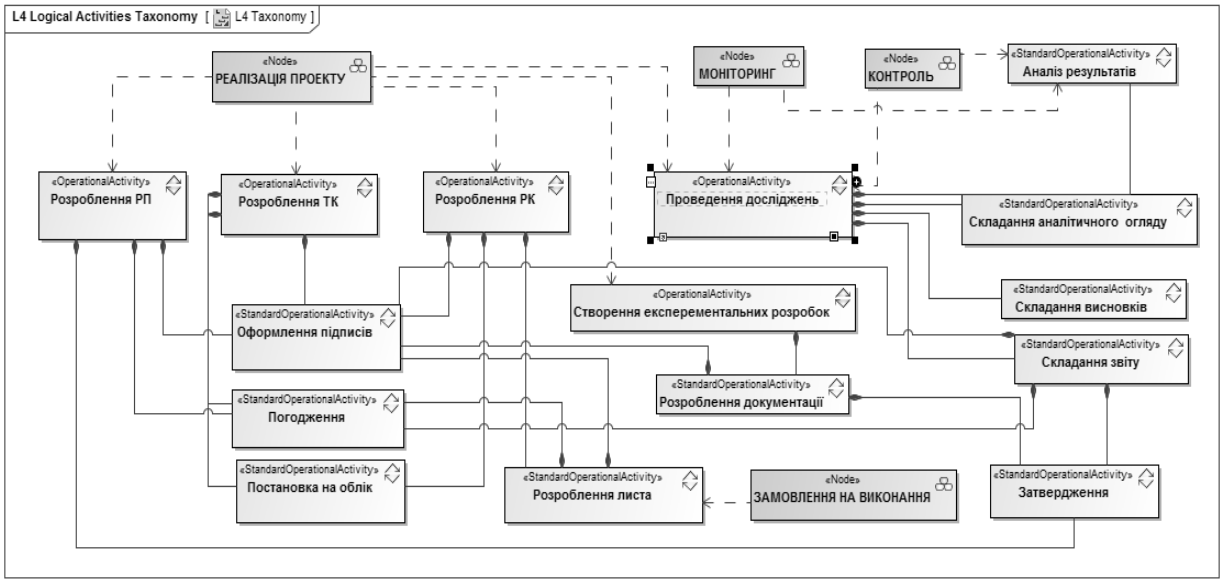


Рис. 7. Діаграма L4 Logical Activities

Приклад діаграми L5 (рис. 8) описує динамічну поведінку вузла «Проєкт», визначає, як унаслідок виконаних дій змінюється стан вузла. Діаграма дає можливість критично оцінити послідовність дій та час виконання, виявити обмеження операційної діяльності.

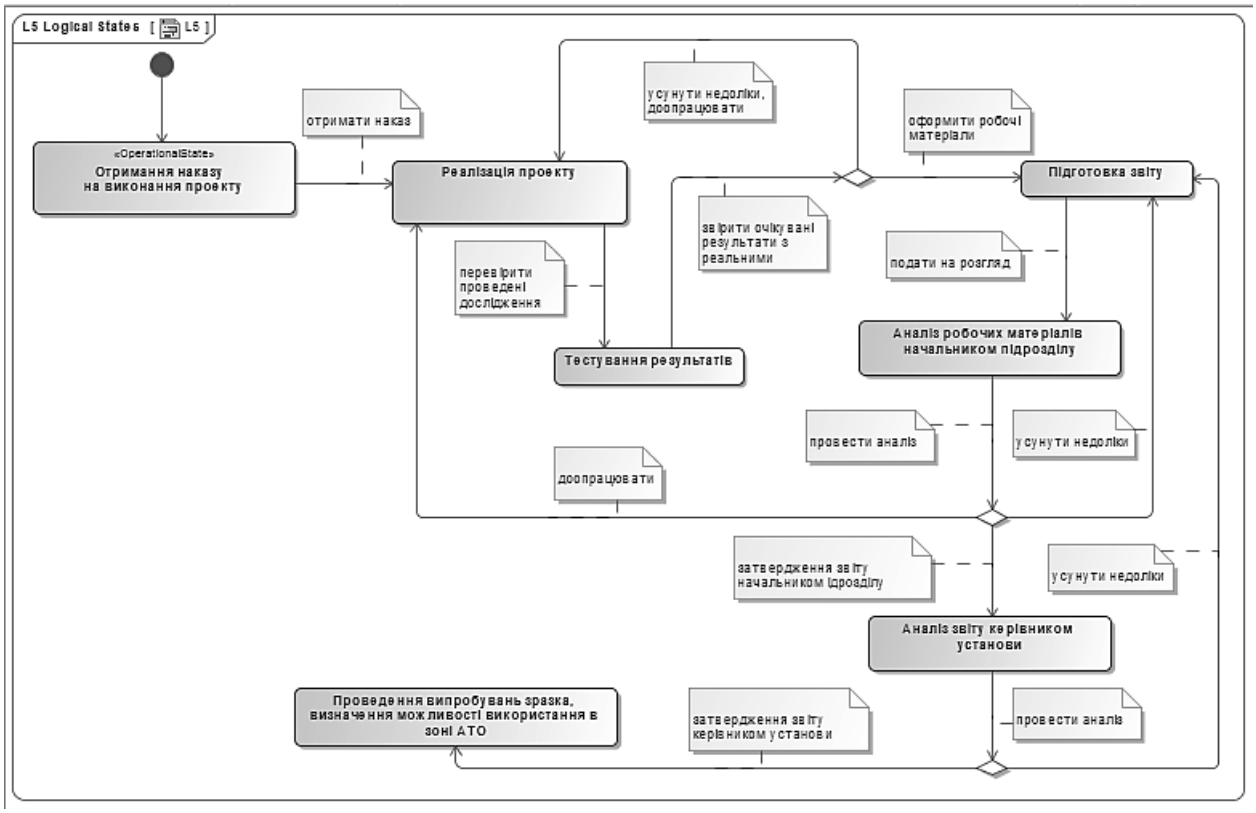


Рис. 8. Діаграма L5 Logical States

Діаграма L6 (рис. 9) відображає хронологічний опис дій та/або логічних потоків за сценарієм типової діяльності «Виконання науково-дослідної роботи», показує логічну послідовність взаємодії між вузлами «Замовник», «Керівник підрозділу», «Науковий керівник», «Відповідальний виконавець», «Виконавці».

«Точки зору» Service ідентифікують сервіси, задіяні для виконання спроможностей (матриця S1-C1); забезпечують контроль операційної діяльності (матриця S4-L4); визначають специфікацію сервісів та функціональну сумісність (S3), стан сервісів, взаємодію з користувачами, сервісні операції (S5, S6); встановлюють обмеження, накладені під час виконання (реалізації) функцій (S8). Для побудови сервісів використовують веб-орієнтований інформаційно-сервісний підхід. Діяльність наукового підрозділу забезпечують:

1) спільні сервіси: чат, форум, електронна бібліотека, пошта, стрічка новин;

2) функціональні сервіси: кабінет, планування, канцелярія, нарада, відеоконференція.

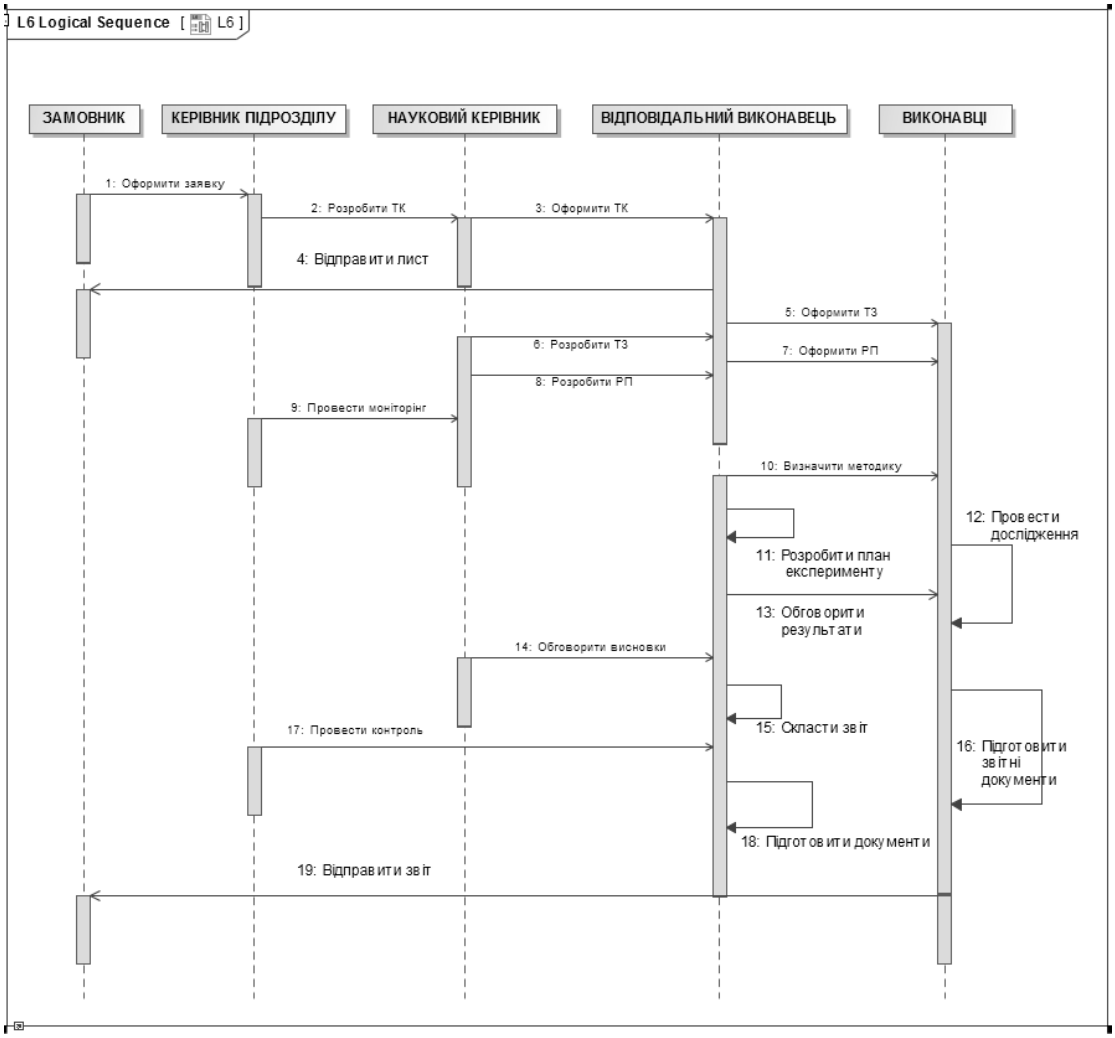


Рис. 9. Діаграма L6 Logical Sequence

У наведеному прикладі діаграми S3 (рис. 10) визначено специфікації окремих сервісів, які перевіряються на функціональну сумісність. Сервіс «Планування» дає можливість керівникам налагодити автоматизований процес управління робочим часом персоналу, складати графіки проведення службових заходів, здійснювати моніторинг доступних кадрових ресурсів, координацію діяльності з урахуванням позаштатних ситуацій, автоматизувати отримання статистично-звітної інформації.

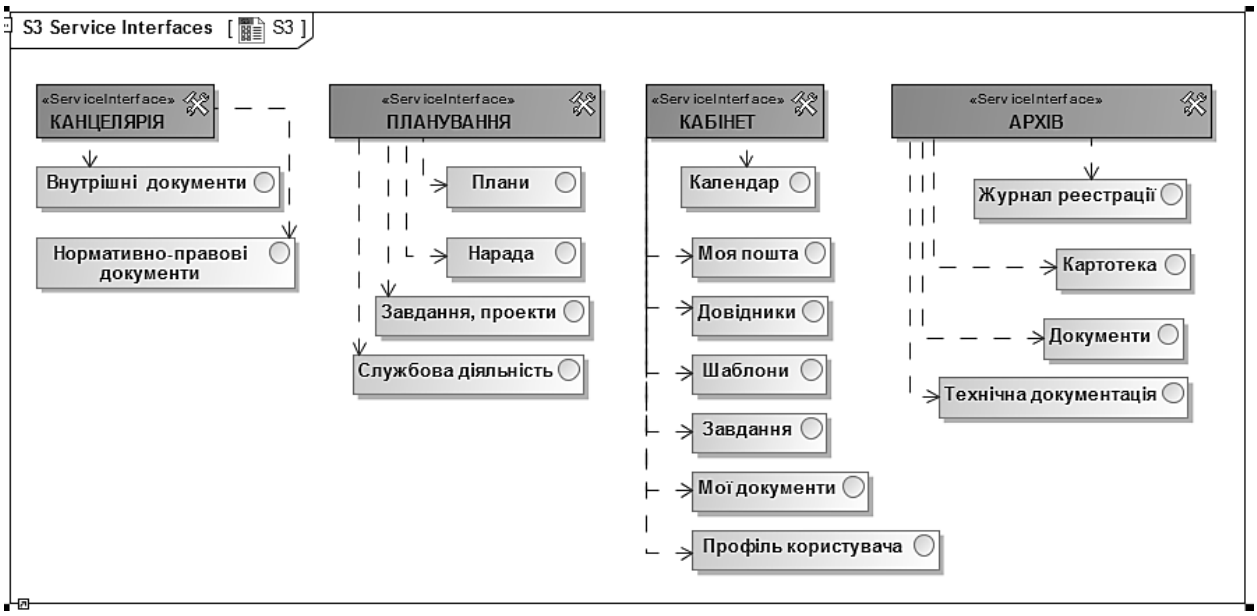


Рис. 10. Діаграма S3 Service Interfaces

У прикладі діаграми S4 (рис. 11) наведено функціонал сервісу «Кабінет» для реалізації службових функцій. Наприклад, функціонал сервісу «Календар» автоматизує складання графіків роботи, планування робочого часу на будь-який період, контроль змін. Для керівника надається інформація зі зручною ієрархічною структурою всіх доступних ресурсів ІС.

«Точки зору» Resource забезпечують опис різних типів ресурсів: кадрових (підрозділи, окремі виконавці); технічних (устаткування, обладнання, техніка); матеріальних (будівлі, споруди); інформаційно-програмного забезпечення та їх взаємодію (рис. 12). У діаграмі P1 відображено автоматизацію процесів комунікації кадрових ресурсів із використанням веб-орієнтованого інформаційно-сервісного підходу.

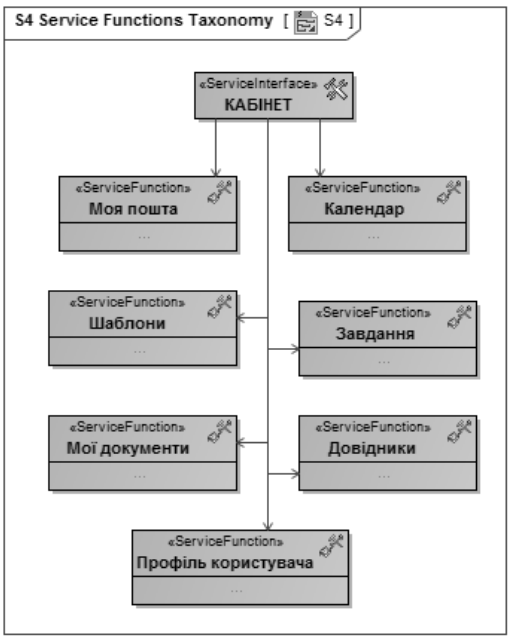


Рис. 11. Діаграма S4 Service

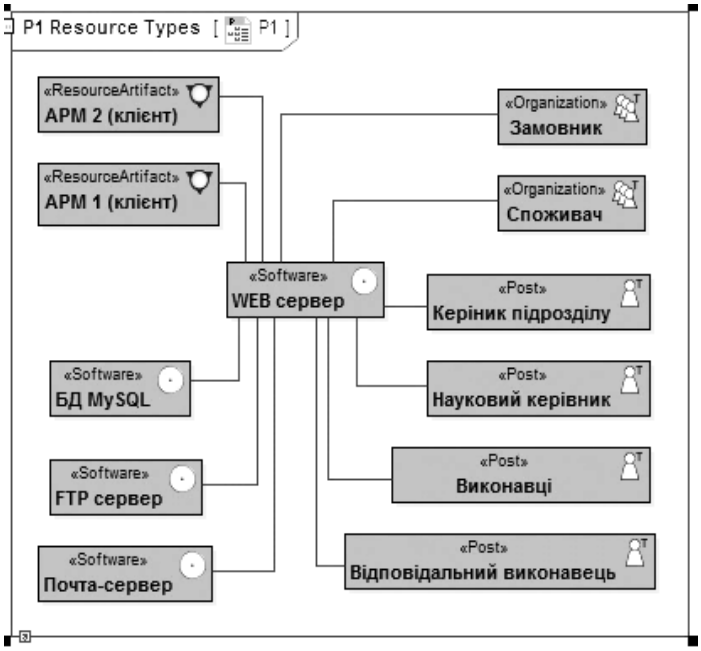


Рис. 12. Діаграма P1 Resource Types

Взаємодія та структура ресурсів для реалізації логічного сценарію L2 відображається в діаграмі P2, яка служить для визначення параметрів системи, способу взаємодії між людиною та системою, типових організаційних структур, оперативного планування. У наведеному прикладі діаграми P2 (рис. 13) визначено компоненти автоматизованого робочого місця (АРМ) користувача.

Діаграма P3 описує шляхи підключення компонентів, які реалізують виконання логічного сценарію L2 або L3. Для веб-орієнтованого інформаційно-сервісного підходу це будуть характеристики архітектури мережі, апаратних засобів (адаптерів, комутаторів), серверів, кабельної мережі. Діаграма створюється для кожної пари компонентів, використовується для проєктування програмного забезпечення, інтерфейсу користувача та бази даних (БД), тобто для опису моделі на фізичному рівні.

Діаграма P4 розглядає функції ресурсів та їх операційну діяльність. Основне призначення: розробити чіткий опис необхідних потоків даних, які використовуються і створюються для кожного ресурсу; досягти необхідного рівня деталізації системних функцій; забезпечити реалізацію конкретних заходів операційної діяльності, зазначених у L4.

У наведеному прикладі діаграми P4 (рис. 14) розглянуто функції керівника підрозділу. На основі діаграми будується матриця залежностей L4-P4 між функціями та операційною діяльністю, яка забезпечує виконання Процесів, ідентифікації вимог функціональної системи, аналізу зв’язку кадрових ресурсів та системних функцій.

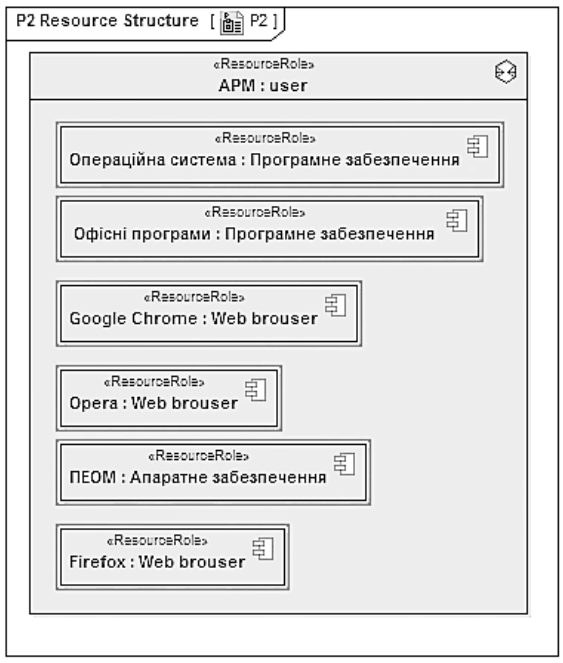


Рис. 13. Діаграма P2 Resource Structure

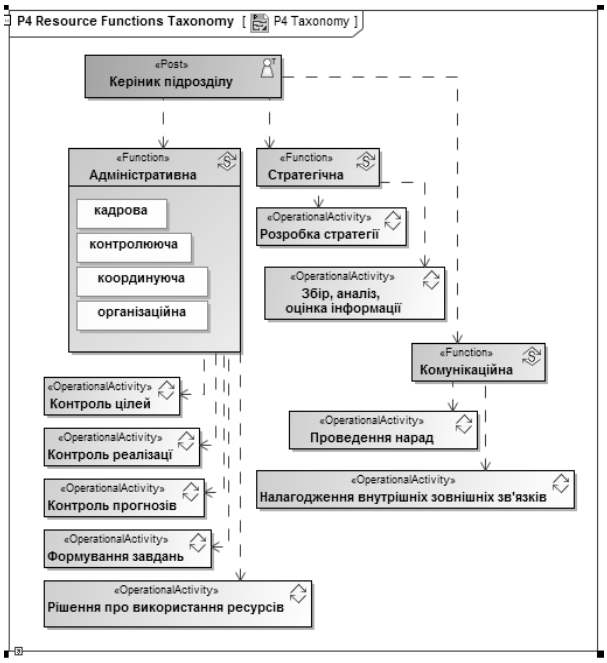


Рис. 14. Діаграма P4 Resource Functoins

Розроблені діаграми архітектури наукового підрозділу дають можливість для: формування та корегування стратегічних (довготермінових), тактичних (річних, місячних) та оперативних цілей (завдань) підрозділу; оптимізації основних процесів діяльності підрозділу; раціонального розподілу наявних ресурсів та з’ясування потреб у додаткових ресурсах; визначення місця та порядку впровадження засобів автоматизації. Автоматичне зведення частини таблиць, звітів виявляє суперечливість або відсутність інформації, некоректність підходу до побудови моделей.

Висновки. У статті запропоновано використання методологічного підходу НАТО NAF v. 4.0 для опису архітектури ІС військового призначення, що сприятиме забезпеченню єдності підходів для проєктування, створення (розробки), планування та управління застосуванням, контролю та оцінювання поточного стану, а також взаємодії ІС та їх складових у різних сферах діяльності та на усіх рівнях управління.

Аналіз методології НАТО NAF v.4.0 проведено з використанням спеціалізованого програмного забезпечення Cameo Enterprise Architecture. Обраний інструмент моделювання дає можливість управління структурою за допомогою деревовидного інтерфейсу, забезпечує взаємозв'язок та кореляцію діаграм на різних рівнях абстракції, автоматичне зведення частини таблиць, звітів, виключає необхідність дублювання інформації в разі опису одних і тих самих об'єктів моделювання в різних аспектах їх застосування (Viewpoints).

Подальші дослідження доцільно присвятити: конкретизації та формалізації методики побудови моделей ЕА; практичній апробації розробленої метамоделі ЕА з метою її використання для проєктування програмного забезпечення, інтерфейсу користувача та БД ІС; розробленню підходів до перевірки адекватності та тестування моделі ЕА.

СПИСОК ЛІТЕРАТУРИ

1. Про рішення Ради національної безпеки і оборони України від 02.09.2015 "Про нову 141 редакцію Воєнної доктрини України" : Указ Президента України від 24.09.2015 № 555/2015. URL: http://zakon4.rada.gov.ua/ laws/show/555/2015 (дата звернення: 06.12.2018).
2. Про рішення Ради національної безпеки і оборони України від 20.05.2016 "Про Стратегічний оборонний бюлетень України" : Указ Президента України від 06.06.2016. № 240/2016]. URL: http://www.president.gov.ua/ documents/2402016-20137 (дата звернення: 14.12.2018).
3. MOD Architecture Framework - GOV.UK. URL: https://www.gov.uk/guidance/mod-architecture-framework (last accessed: 14.12.2018).
4. C4ISR for Future Naval Strike Groups / The National Academies Press. URL: https://www.nap.edu/catalog/11605/c4isr-for-future-naval-strike-groups (last accessed: 16.11.2018).
5. Microsoft Word – Oracle_EA_Framework-Oct2009.doc. URL: https://www.oracle.com/technetwork/articles/entarch/oea-framework-133702.pdf (last accessed: 16.11.2018).
6. MBSE Works: Обзор MBSE + SysML – Что такое MBSE? URL: https://mbseworks.com/mbse-overview/ (дата обращения: 30.11.2018).
7. Сафронов А. А., Давлеткиреева Л. З., Макашова В. Н. Сравнительный анализ методологий построения архитектуры предприятий. URL: http://technology.snauka.ru/2014/01/2721 (дата обращения: 30.11.2018).
8. Togaf Training and Certification. URL: http://www.traffic-jam.info/togaf-training-and-certification/ (last accessed: 14.12.2018).
9. 01м - Моделі і методи проектування інформаційних систем. Проектування інформаційних систем. Тема 2 - Архітектура інформаційних систем. URL: https://elearning.sumdu.edu.ua/free_content/lectured:de1c9452f2a161439391120eef364dd8ce4d8e5e/20160217112601/170352/index.html (дата звернення: 14.12.2018).
10. Introduction to the ADM. URL: http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap03.html (last accessed: 30.11.2018).
11. DODAF – DOD Architecture Framework Version 2.02-DOD Deputy Chief Information Officer. URL: https://dodcio.defense.gov/Library/DoD-Architecture-Framework/ (last accessed: 14.12.2018).
12. NATO Architecture Framework. URL: http://nafdocs.org/wp-content/uploads/2013/07/20130816_MODEM_to_NAF_Review_V1_1-U.pdf (last accessed: 30.11.2018).

13. NAF v 3, Annex A. URL: http://www.silverbulletinc.com/dm2/File_Browser_2/data/files/Socialization%20and%20Pilots/NATO%20-%20Intl%20-%20Coalition/NAF/AC_322(SC_1-WG1)N(2007)0004_NAFv3_Ann3_APP08.pdf (last accessed: 15.12.2018).
14. Methodology / NATO Architecture Framework v 4.0 Documentation (draft). URL: http://nafdocs.org/methodology/ (last accessed: 15.12.2018).
15. (PDF) Aligning TOGAF and NAF-Experiences from the Norwegian Armed Forces. URL: https://www.researchgate.net/publication/221584030_Aligning_TOGAF_and_NAF-Experiences from_the_Norwegian_Armed_Forces (last accessed: 10.12.2018).
16. Submission_Paper_CIISE_2016_Funto_ENG_Rev.2.3. URL: http://ceur-ws.org/Vol-1728/paper11.pdf (last accessed: 15.12.2018).
17. Microsoft Word - Reorganising MODAF and NAF v0_4.docx. URL: http://nafdocs.org/wp-content/uploads/2013/07/Reorganising-MODAF-and-NAF.pdf (last accessed: 15.12.2018).
18. Теоретичні підходи щодо визначення місця інформаційної інфраструктури Міністерства оборони України у розумінні рамкових архітектурних методологій / М. Ю. Голобородько, В. А. Федорієнко, Ю. А. Кірпічніков та ін. Київ : Центр воєнно-стратегічних досліджень Нац. уні-ту оборони України ім. Івана Черняховського. URL: http://nuou.org.ua/pro-universytet/dokumenty/viewcategory/17-zbirnyk-naukovykh-prats-tsentru voienno-stratehichnykh-doslidzhen.html (дата звернення: 14.12.2018).
19. 20180801_180801-ac322-d_2018_0002_naf_final.pdf. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_08/20180801_180801-ac322-d_2018_0002_naf_final.pdf (last accessed: 10.12.2018).
20. AF Forum: Единый профиль для DoDAF / MODAF (UPDM) Обзор. URL: https://architectureframework.com/frameworks/updm/ (дата обращения: 10.12.2018).
21. Cameo Enterprise Architecture. URL: https://www.nomagic.com/products/cameo-enterprise-ar/ chitecture#demos (last accessed: 10.12.2018).
22. Sybase_1238_modellingea_rus.pdf. URL: https://www.sybase.ru/system/files/pdf/sybase_1238_modellingea_rus.pdf (last accessed: 10.12.2018).

Подано 22.12.2018

И. А. Пилькевич, А. М. Перегуда, Е. П. Черкес

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ АРХИТЕКТУРЫ ИНФОРМАЦИОННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ NATO ARCHITECTURE FRAMEWORK НА ПРИМЕРЕ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО ПОДРАЗДЕЛЕНИЯ

В статье предложено использование методологического подхода NATO Architecture Framework v. 4.0 для описания архитектуры информационной системы военного назначения, который дополнен методикой построения моделей Architecture Development Method (взятой из методологии The Open Group Archutecture Framework).

Рассмотренная методология позволяет осуществлять комплексное проектирование и дальнейшее сопровождение архитектуры информационной системы военного назначения на основе применения моделей. Она дает классификацию основных элементов архитектуры на разных уровнях абстракции, единые политики (правила) для описания их взаимодействия друг с другом, обеспечивает поддержку принятия решений в контексте выполнения стратегической миссии, тактических и оперативных задач. Сопровождение архитектуры информационной системы на основе применения моделей позволяет настраивать среду моделирования таким образом, чтобы применять стандарты

и правила в процессе сбора информации. Ввод и управления информацией в соответствии с NATO Architecture Framework помогает достичь согласованности, ясности и точности на всех уровнях архитектуры.

Для апробации предложенного подхода разработана метамодель архитектуры научного подразделения с использованием специализированного программного обеспечения Cameo Enterprise Architecture, функционал которого ориентирован на совместную работу, что обеспечивает: интеграцию моделей, созданных по различным стандартам; возможность проверки модели на полноту и правильность; визуализацию данных, это позволяет отображать модель в виде диаграмм, таблиц, матриц отношений, временных графиков, карты отношений, отчетов.

Созданная метамодель может быть использована для: формирования и корректировки стратегических (долгосрочных), тактических (годовых, месячных), а также оперативных целей (задач) подразделения; оптимизации основных процессов деятельности подразделения; рационального распределения имеющихся ресурсов и выяснения потребностей в дополнительных ресурсах; определения и порядка внедрения средств автоматизации; тиражирование положительного опыта построения архитектуры подразделения и тому подобное.

Ключевые слова: *информационная система; архитектура предприятия; Architecture Framework; NAF.*

I. A. Pilkevich, O. M. Pereguda, O. P. Cherkes

FEATURES OF THE ARCHITECTURE OF THE MILITARY-ORIENTED INFORMATION SYSTEMS WITH THE NATO ARCHITECTURE FRAMEWORK USING OF RESEARCH UNIT (department) AS EXAMPLE

This article suggests using a methodological approach of NATO Architecture Framework v. 4.0 to describe the architecture of military information system whit an addition of Architecture Development Method (taken from The Open Group Architecture Framework).

The above mentioned method allows to conduct complex projecting and further follow up of the architecture of a military information system based on model usage. It gives a classification of the main architectural elements at different abstract levels, general rules to describe their coordination, provides a decision making support in context of strategic mission, tactical and operative tasks. The follow up of the architecture of a military information system based on models allows to configure the modeling environment in order to use standards and regulations to collect data. Data entry and management according to NATO Architecture Framework helps achieve balance and precision at all levels of architecture.

Architectural metamodel has been created by using special software Cameo Enterprise Architecture, in order to implement suggested approach. The software targets cooperation and provides models integrations based on different standards. The possibility to check models precision, data visualization while picturing the model as a diagram, table, matrix.

Hourly graphs, maps and reports. Created metamodel may be used for formation and correction of strategic (long term), tactical (annual, monthly) and operative targets (tasks of the unit), optimization of unit main activities, share existing resources and clarification of additional resources defining the place and order of automatisation implementation spreading positive experiences of units architecture.

Keywords: *information system; units architecture; Architecture Framework; NAF.*

ISSN 2076-1546

УДК 004.9:550.34 DOI: 10.46972/2076-1546.2019.16.05

В. В. Безкоровайний, Ю. О. Гордієнко, А. В. Кошель, К. К. Кулагін, О. І. Солонець

СИСТЕМОЛОГІЧНИЙ АНАЛІЗ ПРОБЛЕМИ ОПТИМІЗАЦІЇ МЕРЕЖІ ОБ'ЄКТІВ ГОЛОВНОГО ЦЕНТРУ СПЕЦІАЛЬНОГО КОНТРОЛЮ

Структурні, вартісні й функціональні характеристики розподілених систем багато в чому визначаються топологією їх підсистем та елементів, яка, у свою чергу, встановлює топологію комунікаційних зв'язків, реалізуючи обмін між елементами і підсистемами ресурсами та інформацією. Це характерно для багатьох сучасних технічних, організаційно-технічних, соціально-економічних систем.

У статті проаналізовано фактори, які визначають ефективність мережі об'єктів Головного центру спеціального контролю Державного космічного агентства України як територіально розподіленої системи, формалізовано її структурний опис та цільове призначення. Порушено проблему оптимізації даної мережі об'єктів, яка включає комплекси задач вибору структури, топології, технології функціонування, параметрів елементів і зв'язків, всебічного оцінювання та вибору варіантів на різних етапах її життєвого циклу. З'ясовано доцільність побудови методології оптимізації мережі об'єктів Головного центру спеціального контролю на ідеях агрегативно-декомпозиційного та блочно-ієрархічного підходів. Запропоновано трирівневу схему декомпозиції проблеми оптимізації мережі, що включає множини завдань її проєктування, планування розвитку, адаптації та реінжинірингу. Визначено склад і схему взаємозв'язку з вхідними і вихідними даними завдань системного проєктування мережі. Практичне застосування отриманих результатів для розв'язання проблеми оптимізації мережі об'єктів Головного центру спеціального контролю дозволить скоротити терміни виконання завдань проєктування та планування її розвитку, зменшити витрати на її модернізацію або реінжиніринг, а за рахунок спільного вирішення завдань – підвищити якість рішень та на цій основі покращити функціональні характеристики мережі. Методологія системологічного аналізу проблеми оптимізації територіально розподілених об'єктів може загалом бути використана для проєктування будь-яких інформаційних систем, розподілених систем обслуговування і великомасштабного моніторингу.

Ключові слова: *мережа; оптимізація; реінжиніринг; спеціальний контроль.*

Постановка проблеми в загальному вигляді. Процеси проєктування, реорганізації, планування розвитку або реінжинірингу систем моніторингу великомасштабних об'єктів, до яких належить мережа об'єктів (пунктів спостереження) Головного центру спеціального контролю (ГЦСК) на території України, неминуче супроводжуються завданнями оптимізації структури. При цьому можуть розглядатися різні аспекти внутрішньої будови мережі ГЦСК: організаційна, топологічна (просторова), функціональна, інші види структур [1–4]. Для подібних об'єктів збільшення відстаней між функціональними підсистемами призводить до появи нової системної властивості, яка не характерна для територіально зосереджених систем. Вона пов'язана з тим, що структурні, вартісні й функціональні характеристики розподілених систем багато в чому

визначаються топологією (розміщенням) їх підсистем та елементів. Топологія підсистем і елементів, у свою чергу, визначає топологію комунікаційних зв'язків, що забезпечують функціонування мережі як єдиного цілого, реалізуючи обмін між елементами і підсистемами, ресурсами та інформацією. Це характерно для багатьох сучасних технічних, організаційно-технічних, соціально-економічних систем (інформаційно-обчислювальних мереж, мереж розподілу та збору інформації, транспортних мереж, розподілених систем обслуговування, виробничо-збутових комплексів, систем управління тощо) [5].

Аналіз останніх досліджень і публікацій. Проблемам проєктування, реорганізації, планування розвитку, реінжинірингу систем моніторингу великомасштабних об'єктів присвячено роботи [6–12]. Зокрема, у [12] для мережі засобів спеціального контролю розроблено ітераційну схему логічного проєктування, що ґрунтується на ідеях агрегативно-декомпозиційного підходу, системного аналізу та системного проєктування складних систем. Для цього проведено аналіз особливостей мережі засобів спеціального контролю як об’єкта проєктування чи реінжинірингу, виконано декомпозицію проблеми її оптимізації на сукупність взаємопов’язаних завдань, що належать до різних ієрархічних рівнів, встановлено схему взаємозв'язків виділених завдань за вхідними даними та отриманими результатами, визначено вимоги, яким повинні відповідати ефективні методи та процедури розв’язання задач оптимізації мережі.

Формулювання завдання дослідження. На основі одержаних у [12] результатів доцільно провести комплексне визначення структури, топології, параметрів та технології функціонування мережі засобів (об’єктів) ГЦСК з метою скорочення часу вирішення завдань проєктування, планування розвитку чи реінжинірингу, зменшення витрат на експлуатацію, покращення функціональних характеристик мережі. Завданням дослідження є аналіз факторів, які визначають ефективність мережі об'єктів ГЦСК як територіально розподіленої системи, формалізація її структурного опису, розробка варіанта декомпозиції проблеми оптимізації мережі, визначення складу і схеми взаємозв'язку з вхідними і вихідними даними завдань системного проєктування мережі.

Виклад основного матеріалу. У процесі оптимізації мережа ГЦСК (як територіально розподілений об'єкт), яка подається в традиційному вигляді $s =< E, R >$ (де E – множина елементів; R – множина відношень між ними), може бути реалізована множиною різних топологій G^*. Виходячи з цього, можна стверджувати, що кожній з топологічних реалізацій $G \in G^*$ мережі відповідає свій набір властивостей [6]:

$$\varphi : \left(E, R, G\right) \to P, \tag{1}$$

де φ – деяке відображення.

Отже, подання мережі у вигляді $s =< E, R >$ є досить загальним і може розглядатися тільки як її концептуальна модель на стадії передпроєктних досліджень. Для вирішення ж завдань оптимізації та управління опис мережі ГЦСК має відображати її топологічні властивості, тобто мати такий вигляд:

$$s =< E, R, G >, \tag{2}$$

де G – топологічна реалізація структури $< E, R >$.

При цьому топологічна реалізація мережі ГЦСК може розглядатися як сукупність топологій елементів G_E, відношень (зв'язків) G_R і траєкторій (переміщень інформації, енергії, інших ресурсів, що визначаються алгоритмами або технологією функціонування мережі A) G_A, тобто $G =< G_E, G_R, G_A >$.

На підставі аналізу цілей і завдань мережі на першому етапі оптимізації (структурного синтезу) необхідно визначити підмножину найважливіших властивостей P', якими вона повинна володіти і які є підмножиною множини властивостей, що можуть бути отримані на універсальних множинах елементів E^U, відношень R^U і топологій G^U мережі:

$$P^U = \varphi\left(E^U, R^U, G^U\right). \tag{3}$$

Множина E^U в (3) включає в себе різні типи елементів, на яких побудована мережа ГЦСК. Безліч відношень R^U характеризується можливими принципами побудови ГЦСК, а також розподілом функцій між елементами мережі і, зокрема, описує можливі схеми взаємозв'язків між множиною елементів E^U. Склад R^U визначається складом E^U, а множини G^U – складом множин E^U та R^U (рис. 1).

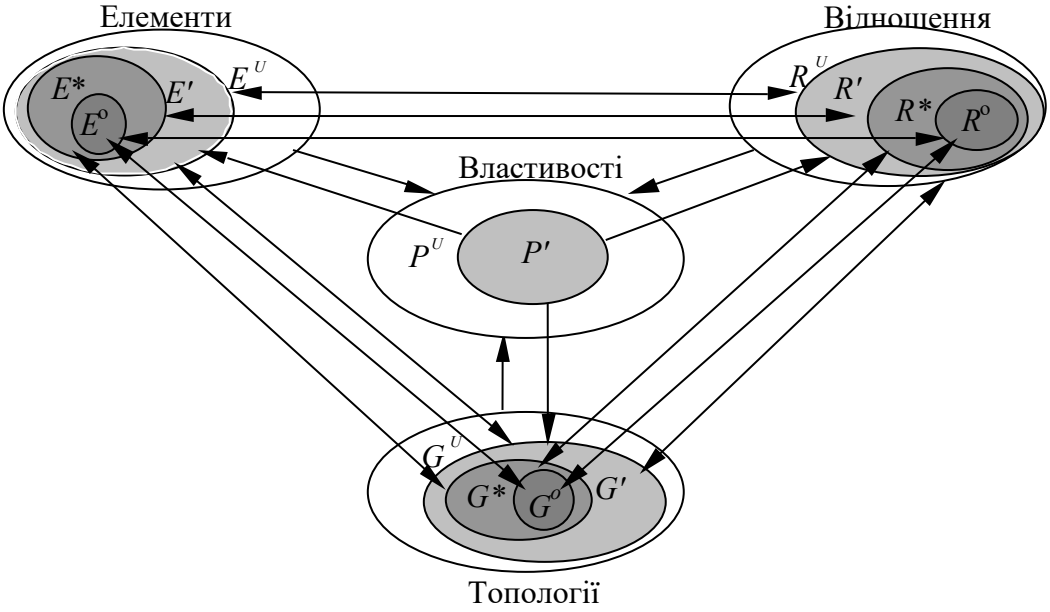


Рис. 1. Схема зв'язку категорій "елементи", "відношення", "топології" та "властивості" в процесі оптимізації мережі ГЦСК

Відображення P' на множині елементів E^U, відношень R^U і топологій G^U неявно визначає підмножини елементів E', відношень R' і топологій G', на яких може бути реалізована мережа з визначеними властивостями P'. У такий спосіб формується область існування мережі $S' = \{s\}$, яка, з урахуванням наявних технічних, економічних, географічних або інших обмежень, звужується до допустимої області синтезу $S^* = \{s\}$, $S^* \subseteq S'$, тобто $E^* \subseteq E' \subseteq E^U$, $R^* \subseteq R' \subseteq R^U$, $G^* \subseteq G' \subseteq G^U$ [6].

На наступних етапах завдання структурного синтезу мережі ГЦСК зводиться до вибору таких підмножин елементів $E^{\circ} \subseteq E^{*}$, відношень $R^{\circ} \subseteq R^{*}$ і топологій $G^{\circ} \subseteq G^{*}$ з допустимої області $S^{*} = \{s\}$, які забезпечують найбільш ефективне (наприклад, з мінімальними затратами ресурсів C°) досягнення необхідних властивостей P'.

Формалізація множини найважливіших властивостей $P' = \{p_i\}$ дозволяє отримати кількісні оцінки ступеня досягнення цілей оптимізації мережі та в цьому сенсі може служити множиною часткових критеріїв її ефективності. Серед найбільш загальних вимог, що висуваються до систем розглянутого класу (властивостей ГЦСК), слід виділити якість, час, витрати, надійність виконання завдань, живучість мережі. Рівень якості виконання завдань визначається, в основному, складом типових елементів (засобів та особового складу) ГЦСК $E \subseteq E^{*}$.

Виконання покладених на ГЦСК завдань має здійснюватися в мінімальні $\tau \to min$ або встановлені $\tau \le \tau^{*}$ терміни (τ^{*} – припустимий час на виконання завдань). Під вартістю виконання функцій *C* розуміють показники витрат на реорганізацію і (або) експлуатацію мережі ГЦСК, що реалізує заданий набір завдань.

У разі вирішення завдань оптимізації подібних мереж прагнуть до інтегральності часткових критеріїв $K = \{k_1, k_2, ..., k_n\}$, щоб $|K| < |P'|$. На практиці ці умови виконуються, оскільки деякі властивості мережевих об'єктів є взаємопов'язаними і змінюються узгоджено. Наприклад, вимога неможливості відмови у виконанні завдання контролю призводить до того, що ненадійність одних елементів ГЦСК збільшує час виконання завдання за допомогою інших елементів; зростання кількості або номенклатури елементів мережі знижує ступінь її завантаження, збільшуючи витрати на виконання завдань тощо.

Оцінювання якості варіантів побудови мережі ГЦСК може бути реалізоване з використанням методології функціонально-вартісного аналізу [13]. Метою оптимізації мережі в даному разі є максимізація її ефективності, тобто отримання максимального співвідношення розміру ефекту від функціонування *Q* та витрачених на це ресурсів *C*. Без втрати спільності можливо припустити, що існують узагальнені оцінки ефекту і витрат ресурсів (вартості) на систему:

$$Q = F_1(E,\ R,\ G), \tag{4}$$

$$C = F_2(E,\ R,\ G), \tag{5}$$

де E, R, G – відповідно множини елементів, відношень між ними та їх топологій;

F_1, F_2 – деякі оператори, що визначають стратегії використання ресурсів, які виділяють на створення або модернізацію об'єкта.

Функціональний ефект мережі в загальному випадку є неспадною функцією від витрачених на його досягнення ресурсів (вартості):

$$\overline{Q} = F(\overline{C}),$$

де $\overline{Q}$ та $\overline{C}$ – узагальнені скалярні оцінки ефекту та вартості мережі;

F – оператор, що відображає стратегію використання ресурсів, яка визначається вибором варіанта побудови мережі $s \in S^*$.

На ранніх етапах проєктування виникає завдання вибору варіанта побудови мережі за критерієм "ефект-вартість" [7–8]:

$$K_{QC} = \underset{Q,C,F}{opt}\Theta\left(Q,\ C,\ F\right), \tag{6}$$

де $opt\ \Theta$ – оператор, який визначає конкретний вид критерію ефективності.

В умовах заданих обмежень на показники ефекту та вартості завдання оптимізації мережі ГЦСК на основі критерію (6) може бути подане як:

$$s_1^o = arg\ \underset{s\in S^*}{max}\left(\overline{Q}(s) - \overline{C}(s) :\ \overline{Q}(s) \ge \overline{Q}^*,\ \overline{C}(s) \le \overline{C}^*\right), \tag{7}$$

$$s_2^o = arg\ \underset{s\in S^*}{max}\left(\overline{Q}(s) / \overline{C}(s) :\ \overline{Q}(s) \ge \overline{Q}^*,\ \overline{C}(s) \le \overline{C}^*\right), \tag{8}$$

де $\overline{Q}^*$, $\overline{C}^*$ – граничні рівні наведених узагальнених оцінок ефекту та вартості мережі;

$S^* = \{s\}$ – множина припустимих варіантів побудови мережі.

Окремими випадками (7)–(8) є завдання інженерного синтезу:

в умовах заданих обмежень на ресурси (вартість) обрати варіант побудови мережі, що максимізує наведений ефект:

$$s_3^o = arg\ \underset{s\in S^*}{max}\left(\overline{Q}(s) : \overline{C}(s) \le \overline{C}^*\right); \tag{9}$$

в умовах заданих обмежень на рівень ефекту обрати варіант побудови, що мінімізує передбачувані витрати на створення та (або) експлуатацію мережі:

$$s_4^o = arg\ \underset{s\in S^*}{min}\left(\overline{C}(s) : \overline{Q}(s) \ge \overline{Q}^*\right). \tag{10}$$

Проблема оптимізації мережі ГЦСК включає комплекси завдань із визначення структури, топології, технології функціонування, параметрів елементів і зв'язків, всебічного оцінювання та вибору варіантів на різних етапах її життєвого циклу. Опис властивостей мережі та завдань її синтезу у вигляді (1)–(10) є досить загальним. Для отримання за ними проєктних рішень потрібна їх деталізація.

З метою забезпечення ефективності та спадковості рішень на всіх етапах життєвого циклу мережі ГЦСК необхідне використання методології її оптимізації, що передбачає коректну декомпозицію проблеми на комплекси завдань, які належать до різних рівнів опису її об'єкта та етапів її оптимізації (реінжинірингу), розробку комплексу відповідних моделей, процедур, логічної схеми та технології оптимізації.

Проблема оптимізації подібних об'єктів розглядається такою, що складається із сукупності не в повному обсязі визначених завдань проєктування, для яких не сконструйовані схеми проєктування та не синтезовані моделі проєктування, що дозволяє віднести її до слабкоструктурованих [9–10].

Методологію оптимізації мережі ГЦСК доцільно будувати на ідеях агрегативно-декомпозиційного та блочно-ієрархічного підходів, які передбачають розбиття опису об'єкта за ступенем деталізації на ієрархічні рівні та аспекти, а процесу оптимізації – на групи проєктних процедур, пов'язаних з отриманням і перетворенням описів (рішень) відносно виділених рівнів і аспектів з подальшим їх об'єднанням (агрегацією) для отримання на відповідному рівні рішень щодо системи в цілому [6, 9].

Пропонуємо подати досліджувану проблему як метазадачу *MetaTask*, що складається з множини задач, які належать до різних ієрархічних рівнів декомпозиції, з їх взаємозв'язками за вихідними даними та результатами рішення (рис. 2) [6]:

$$MetaTask = \{Task_l\},\ Task_l = \{Task_i^l\},\ i = \overline{1, i_l},\ l = \overline{1, n_l}, \tag{11}$$

де $Task_l$ – множина задач оптимізації рівня l;

n_l – кількість рівнів опису мережі;

i – номер задачі (етапу, стадії оптимізації);

i_l – кількість задач рівня l.

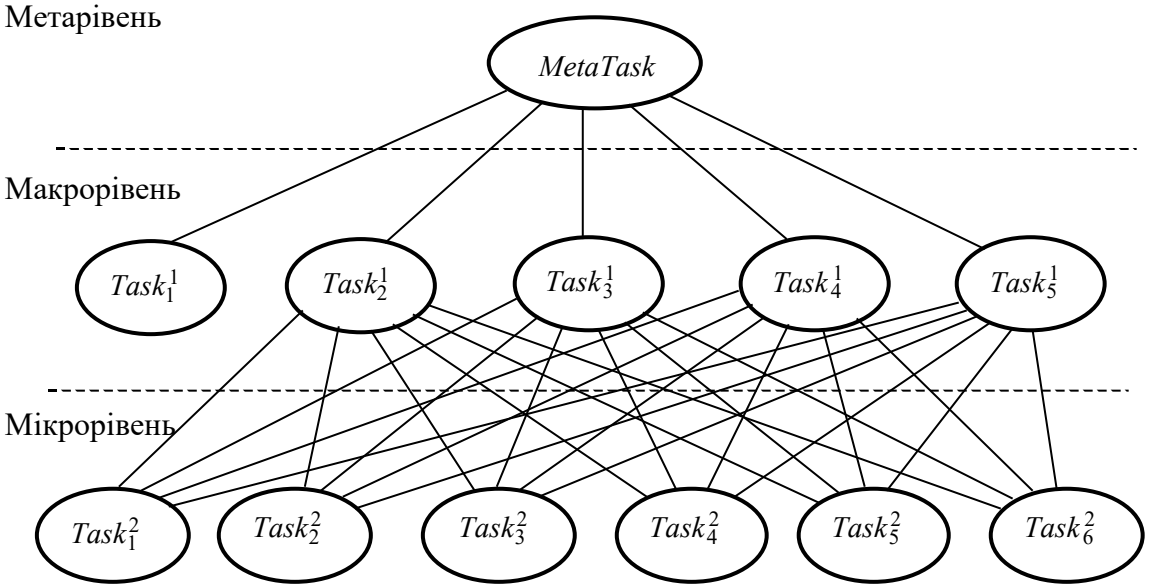


Рис. 2. Схема декомпозиції проблеми оптимізації мережі ГЦСК як територіально розподіленого об'єкта

Кожну із задач на цьому етапі подано в такому вигляді:

$$Task_i^l = In_i^l \rightarrow Out_i^l,\ i = \overline{1, i_l},\ l = \overline{1, n_l}, \tag{12}$$

де In_i^l, Out_i^l – відповідно вхідні та вихідні дані i-ї задачі l-го рівня.

При цьому кожна з виділених задач (12) може бути подана у вигляді множини взаємопов'язаних підзадач $Task_i^l = \{Task_{ij}^l\},\ j = \overline{1, j_i}$, де j_i – кількість підзадач задачі $Task_i^l$.

Системологічний аналіз проблеми оптимізації мережі ГЦСК та огляд її сучасного стану дозволяють зробити висновок про доцільність використання в конструкторському і техніко-економічному аспектах трьох ступенів деталізації їх опису на мета-, макро- та мікрорівнях.

На метарівні проблему *MetaTask* розглядають у цілому, аналізують її місце серед інших проблем глобального моніторингу.

Більшість завдань макрорівня за своєю суттю є задачами системного проєктування і відрізняються обмеженнями, які відображають специфіку основних етапів життєвого циклу мережі:

$$Task^1 = \left\{Task_i^1\right\},\ i = \overline{1,\ 5}, \tag{13}$$

де $Task_1^1$ – формування вимог до мережі та розробка технічного завдання на проєктування;

$Task_2^1$ – системне проєктування;

$Task_3^1$ – планування розвитку;

$Task_4^1$ – структурна адаптація;

$Task_5^1$ – реінжиніринг мережі.

У межах розв'язання задачі $Task_1^1$ визначаються цілі, для досягнення яких оптимізується мережа, уточнюється коло вирішуваних нею завдань, досліджуються властивості зовнішнього середовища, характеристики її впливу, визначаються можливі принципи її побудови $(П)$.

Основна мета вирішення цього завдання полягає у визначенні оптимального співвідношення ефекту Q^* та витрат (вартості) C^*, тобто в розв'язку задачі (6), а також області існування мережі S'. Результат може бути отримано шляхом функціонально-вартісного аналізу мережі, яка оптимізується.

Вхідні та вихідні дані задачі $Task_1^1$ можуть бути подані в такому вигляді:

$$Task_1^1 :\ \left\{ObjS,\ Los,\ Ben,\ S^U\right\} \to \left\{K,\ Q^*,\ C^*,\ П,\ S'\right\}, \tag{14}$$

де *ObjS* – множина характеристик об'єктів, які підлягають спостереженню;

Los – множина втрат за відсутності (невиконання функцій контролю) мережі;

Ben – множина ефектів (вигод) від використання інформації, одержуваної з мережі;

$S^U = \{s\}$ – вихідна множина варіантів побудови мережі, яка визначається універсальними множинами елементів E^U, відношень R^U і топологій G^U;

K – множина критеріїв для оцінювання та вибору варіантів побудови мережі;

$S' = \{s\}$ – область існування мережі, яка визначається множиною елементів E', відношень R' та топологій G', що дозволяють отримати необхідний набір властивостей мережі Q^*.

Особливістю цієї задачі є оцінний характер вихідної інформації, її низька достовірність, евристичний характер оцінок, більшість з яких отримуються експертним шляхом.

Задача системного проєктування $Task_2^1$ полягає у визначенні найкращого в сенсі множини обраних критеріїв *K* варіанта побудови мережі ГЦСК $s°$ в умовах допустимих принципів її побудови *П*, а також заданих структурних, топологічних, параметричних та технологічних обмежень $S' = \{s\}$, рівнів ефекту Q^* та (або) витрат C^*. Ступінь

визначеності вихідної інформації при цьому є більш високим, ніж для попередньої задачі.

Формально вона може бути подана в такому вигляді:

$$Task_2^1 : \left\{ObjS,\ K,\ Q^*,\ C^*,\ S',\ \Pi\right\} \to \left\{s^\circ,\ K\left(s^\circ\right)\right\}, \tag{15}$$

де s° – ефективний варіант побудови мережі, $s^\circ \in S^*$;

$K\left(s^\circ\right)$ – множина критерійних оцінок варіанта s°.

Задача планування розвитку мережі ГЦСК $Task_3^1$ полягає у виборі для заданої множини моментів часу $\{t\}$ ефективної траєкторії зміни структури s_t^o у процесі її створення або еволюції в умовах зміни вимог $ObjS_t$, ресурсного забезпечення C_t^*, поетапної зміни обмежень на якість виконання функцій Q_t^*. Метою є визначення найкращої в сенсі множини критеріїв K послідовності введення в експлуатацію окремих елементів, підсистем і зв'язків, що забезпечують на кожному з етапів необхідний рівень ефективності Q_t^* в умовах обмежень на розміри виділених ресурсів C_t^*. При цьому потрібен розв’язок множини пов'язаних за вхідними та вихідними даними задач системного проєктування у вигляді (15).

Формально задача $Task_3^1$ може бути подана у такому вигляді:

$$Task_3^1 : \left\{T,\ ObjS_t,\ K,\ Q_t^*,\ C_t^*,\ S'\right\} \to \left\{s_t^o,\ K\left(s_t^o\right)\right\}, \tag{16}$$

де $T = \{t\}$ – множина моментів часу, які відповідають етапам планування;

$S' = \{s\}$ – множина припустимих варіантів побудови мережі (область існування);

s_t^o – ефективний варіант побудови мережі на *t*-му етапі;

$K\left(s_t^o\right)$ – множина критерійних оцінок варіанта s_t^o.

Задача структурної адаптації мережі $Task_4^1$ розв’язується в процесі її експлуатації та пов'язана з необхідністю відносно незначних структурних, технологічних, топологічних або параметричних змін отриманого раніше варіанта $s^\circ \in S'$ у зв'язку зі змінами множини та (або) характеристик спостережуваних об'єктів $Obj\widetilde{S}$, виходом з ладу деяких елементів (підсистем), змінами необхідних рівнів ефекту $\widetilde{Q}^*$ або витрат $\widetilde{C}^*$ тощо.

Формально задача $Task_4^1$ може бути подана в такому вигляді:

$$Task_4^1 : \left\{Obj\tilde{S},\ s^\circ,\ \tilde{Q}^*,\ \tilde{C}^*,\ \tilde{S}'\right\} \to \left\{\tilde{s}^\circ,\ K\left(\tilde{s}^\circ\right)\right\}, \tag{17}$$

де $\widetilde{S}'$ – припустима множина варіантів адаптації мережі;

$\tilde{s}^\circ$ – ефективний адаптований варіант побудови мережі;

$K\left(\tilde{s}^\circ\right)$ – критерійна оцінка варіанта $\tilde{s}^\circ$.

Задача реінжинірингу мережі ГЦСК $Task_5^1$ розв’язується в процесі її експлуатації та пов'язана з необхідністю кардинальних структурних, технологічних, топологічних або

параметричних змін у зв'язку зі змінами множини та (або) характеристик спостережуваних об'єктів $Obj\widetilde{S}$, розширенням множини функціональних завдань, удосконаленням бази засобів та (або) технологій реалізації функцій мережі $\widetilde{S}'$, що роблять наявний варіант мережі $s°$ (s_t^o або $\widetilde{s}°$) малоефективним. При цьому допускається як повна заміна елементів $E°$ та зв'язків між ними $R°$, так і їх модернізація, пов'язана зі зміною їх вартісних та функціональних характеристик Δ_{ER}.

Формально задача $Task_5^1$ може бути подана в такому вигляді:

$$Task_5^1 : \left\{Obj\tilde{S},\ s°,\ \tilde{Q}^*,\ \tilde{C}^*,\ \tilde{S}',\ \Delta_{ER}\right\} \to \left\{\tilde{s}°,\ K\left(\tilde{s}°\right)\right\}, \tag{18}$$

де $s°$ та $\widetilde{s}°$ – відповідно старий та новий варіант побудови мережі, який отримано в результаті її реінжинірингу;

Δ_{ER} – множина змін функціональних та вартісних характеристик, пов’язаних із переходом на нову елементну та технологічну базу.

Комплекс задач метарівня (14)–(18) охоплює все коло питань структурного синтезу мережі ГЦСК, які виникають на стадіях передпроєктних досліджень, проєктування, створення та експлуатації, що вирішуються в системах їх проєктування та управління ними.

Основні завдання мікрорівня пов'язані з вирішенням питань системного проєктування мережі ГЦСК:

$$Task^2 = \left\{Task_i^2\right\},\ i = \overline{1,\ 6}, \tag{19}$$

де $Task_1^2$ – вибір принципів побудови мережі;

$Task_2^2$ – вибір структури мережі;

$Task_3^2$ – визначення топології елементів та зв'язків;

$Task_4^2$ – вибір технології функціонування мережі;

$Task_5^2$ – визначення параметрів елементів та зв’язків мережі;

$Task_6^2$ – оцінка ефективності варіантів та вибір рішень.

Вибір принципів побудови та функціонування мережі ГЦСК π із множини припустимих $П$, визначених у процесі розв’язання задачі $Task_1^1$, здійснюється неформальними методами на підставі знань і досвіду проєктувальників. При цьому множина варіантів, які окреслюють область існування мережі S', що подається множинами елементів E', відношень R' та топологій G', скорочується до множини припустимих варіантів побудови мережі $S^* \subseteq S'$, яка визначається множинами елементів $E^* \subseteq E'$, відношень $R^* \subseteq R'$ та топологій $G^* \subseteq G'$.

Формально задачу вибору принципів побудови $Task_1^2$ можна подати в такому вигляді:

$$Task_1^2 : \left\{ObjS,\ П,\ S',\ K,\ Q^*,\ C^*\right\} \to \left\{\pi,\ S^*\right\}, \tag{20}$$

де *ObjS* – множина характеристик об'єктів, які спостерігаються;

K – множина критеріїв для оцінювання та вибору варіантів побудови мережі;

Q^*, C^* – задані рівні ефекту та допустимих витрат на мережу;

$S^* = \{s\}$ – множина припустимих варіантів побудови мережі, що задається множиною елементів E^*, відношень R^* та топологій G^*, виходячи з обраних принципів її побудови $\pi \in \Pi$.

Задача вибору структури мережі $Task_2^2$ присвячена довизначенню варіанта її побудови s_{AB} (із заданими технологією функціонування $A = \psi_A(E,\ R)$, параметрами елементів і відношень $B = \psi_B(E,\ R)$) кількістю елементів $|E|$ і зв'язками між ними $R \subseteq R^*$, а також оцінюванню властивостей отриманого варіанта s_{ER} у критерійному просторі K. Задача розв'язується в умовах заданих рівнів ефекту Q^* та витрат C^*.

Формально $Task_2^2$ можна подати в такому вигляді:

$$Task_2^2 : \{ObjS,\ A,\ B,\ S^*,\ K,\ Q^*,\ C^*\} \to \{|E|,\ R,\ s_{ER},\ K(s_{ER})\}. \qquad (21)$$

Задача вибору топології елементів і зв'язків $Task_3^2$ полягає в довизначенні для заданих елементів E зв'язків між ними R, параметрів B та технології функціонування A варіанта побудови мережі s_{ERAB} кращою топологією $G \subseteq G^*$. При цьому враховуються обмеження на припустимі рівні ефекту Q^* та витрат C^*.

Формально задача $Task_3^2$ може бути подана в такому вигляді:

$$Task_3^2 : \{ObjS,\ E,\ R,\ A,\ B,\ S^*,\ K,\ Q^*,\ C^*\} \to \{G,\ s_G,\ K(s_G)\}, \qquad (22)$$

де s_G – варіант побудови мережі з оптимізованою топологією.

Задача вибору технології функціонування мережі ГЦСК $Task_4^2$ присвячена довизначенню в умовах заданих множин елементів E зв'язків між ними R, топології G, параметрів елементів та зв'язків $B = \psi_B(E,\ R)$ варіанта її побудови s_{ERGB} найкращою технологією $A = \psi_A(E,\ R)$. При цьому також можуть бути задані рівні необхідного ефекту Q^* та граничних витрат C^*.

Формально задачу вибору технології функціонування $Task_4^2$ можна подати як

$$Task_4^2 : \{ObjS,\ E,\ R,\ G,\ B,\ S^*,\ K,\ Q^*,\ C^*\} \to \{A,\ s_A,\ K(s_A)\}, \qquad (23)$$

де s_A – варіант побудови мережі з оптимізованою технологією її функціонування.

Задача визначення параметрів елементів та зв'язків мережі $Task_5^2$ полягає у виборі варіанта її побудови $s_B \subseteq S^*$, який має кращі значення B. Її розв'язання здійснюється в умовах заданих структурних $(|E|, R)$, топологічних G і технологічних A характеристик мережі. Потрібно параметричне довизначення варіанта s_{ERGA}. Результати розв'язання цієї задачі є основою для вибору типів вузлів, елементів та зв'язків із заданих множин типових об'єктів.

Формально задача визначення параметрів елементів та зв'язків мережі ГЦСК $Task_5^2$ може бути подана в такому вигляді:

$$Task_5^2 : \left\{ObjS,\ |E|,\ R,\ G,\ A,\ S^*,\ K,\ Q^*,\ C^*\right\} \to \left\{B,\ s_B,\ K\left(s_B\right)\right\}. \qquad (24)$$

Задача визначення ефективності варіантів і вибору рішень $Task_6^2$ полягає в оцінюванні варіантів побудови мережі $s \subseteq S^*$ за множиною критеріїв K та виборі найкращого з них $s^\circ = arg\ \underset{s}{opt} K\left(s\right)$. Її розв'язання здійснюється в умовах заданих структурних $\left(E,R\right)$, топологічних G та технологічних A характеристик мережі, а також параметрів елементів та зв'язків B.

Формально задачу $Task_6^2$ можна подати в такому вигляді:

$$Task_6^2 :\ \left\{ObjS,\ Q^*,\ C^*,\ S^*,\ K\right\} \to \left\{s^\circ,\ K\left(s^\circ\right)\right\}. \qquad (25)$$

Подальша декомпозиція задач мікрорівня $Task_i^2 = \left\{Task_{ij}^2\right\},\ j = \overline{1, j_i}$ (де j_i – кількість підзадач задачі $Task_i^2$) приводить до комплексу задач синтезу елементів, елементарних зв'язків та елементів технологій функціонування мережі ГЦСК. У процесі її системного проєктування розв'язки з цього комплексу задач можуть бути знайдені раніше та використовуватися як вихідні дані (обмеження) у вигляді множин припустимих значень їх функціональних та вартісних характеристик B^*.

Процес оптимізації мережі ГЦСК, окрім перерахованих, може включати комплексні задачі, пов'язані з її специфікою або використовуваною методологією синтезу, а також комплекси задач мікрорівня, наприклад, структурно-топологічного, структурно-технологічного, структурно-параметричного синтезу.

Висновки. Для побудови технології системної оптимізації ГЦСК необхідна розробка комплексу моделей визначених задач (11) з урахуванням їх взаємозв'язку за вхідними та вихідними даними.

Методологія системологічного аналізу проблеми оптимізації територіально розподілених об'єктів може бути використана для проєктування інформаційних систем, розподілених систем обслуговування і великомасштабного моніторингу. Практичне застосування отриманих результатів для розв'язання проблеми оптимізації мережі ГЦСК дозволить скоротити терміни вирішення завдань проєктування та планування її розвитку, скоротити витрати на її модернізацію або реінжиніринг за рахунок підвищення якості рішень та на цій основі покращити функціональні характеристики мережі.

СПИСОК ЛІТЕРАТУРИ

1. Управление развитием крупномасштабных систем. Современные проблемы / С. Н. Васильев, А. А. Макаров, В. Л. Макаров и др.; под ред А. Д. Цвиркуна. Москва : Изд-во физ.-мат. литературы, 2015. 477 с.

2. Безрук В. М., Чеботарева Д. В., Скорик Ю. В. Многокритериальный анализ и выбор средств телекоммуникаций. Харьков : ФОП Коряк С. Ф., 2017. 268 с.

3. Інформаційні системи та мережі військ. Ч. 1 / В. І. Ткаченко, Є. Б. Смірнов,

І. О. Романенко та ін.; за ред. І. В. Рубана. Харків : ХУПС, 2013. 328 с.
4. Zhivitskaya H. Topological properties and methodology of research of complex logistic systems efficiency // ECONTECHMOD. 2014. Vol. 3 (3). P. 23–32.
5. Петров Э. Г., Писклакова В. П., Бескоровайный В. В. Территориально распределенные системы обслуживания. Киев : Техника, 1992. 208 с.
6. Бескоровайный В. В. Системологический анализ проблемы структурного синтеза территориально распределенных систем // Автоматизированные системы управления и приборы автоматики. 2002. Вып. 120. С. 29–37.
7. Бескоровайный В. В., Подоляка К. Е. Разработка системологической модели проблемы структурно-топологического реинжиниринга систем крупномасштабного мониторинга // Восточно-Европейский журнал передовых технологий. 2015. № 3 (75). С. 37–42.
8. Beskorovainyi V., Imanhulova Z. Technology of large-scale objects system optimization // ECONTECHMOD. 2017. Vol. 6 (4). P. 3–8.
9. Цвиркун А. Д., Акинфиев В. К. Структура многоуровневых и крупномасштабных систем. Синтез и планирование развития. Москва : Наука, 1993. 160 с.
10. Тимченко А. А. Основи системного проектування та аналізу складних об'єктів : у 2 кн. Кн. 1. Основи САПР та системного проектування складних об'єктів / За ред. В. І. Бикова. Київ : Либідь, 2000. 272 с.
11. Beskorovainyi V., Podoliaka K. Reengineering the topological structure of large-scale monitoring systems // ECONTECHMOD. 2015. Vol. 4 (3). P. 13–18.
12. Method of system design of the network of means of special control / V. Bezkorovayny, O. Solonets, K. Kulagin and other // Advanced Information Systems. 2017. Vol. 1, No. 2. P. 15–20.
13. Справочник по функционально-стоимостному анализу / А. П. Ковалев, Н. К. Моисеева, В. В. Сысун и др.; под ред. М. Г. Карпунина, Б. И. Майданчика. Москва : Финансы и статистика, 1988. 431 с.

Подано 29.12.2018

В. В. Безкоровайный, Ю. А. Гордиенко, А. В. Кошель, К. К. Кулагин, А. И. Солонец

СИСТЕМОЛОГИЧЕСКИЙ АНАЛИЗ ПРОБЛЕМЫ ОПТИМИЗАЦИИ СЕТИ ОБЪЕКТОВ ГЛАВНОГО ЦЕНТРА СПЕЦИАЛЬНОГО КОНТРОЛЯ

Структурные, стоимостные и функциональные характеристики распределённых систем много в чем определяются топологией ее подсистем и элементов, которая, в свою очередь, определяет топологию коммуникационных связей, реализующих обмен между элементами и подсистемами ресурсами и информацией. Это характерно для многих современных технических, организационно-технических и социально-экономических систем.

В статье проанализированы факторы, которые определяют эффективность сети объектов Главного центра специального контроля как территориально распределенной системы, формализированы ее структурное описание и целевое применение. Сформулирована проблема оптимизации данной сети объектов, которая включает комплексы задач выбора структуры, топологии, технологии функционирования, параметров элементов и связей, всесторонней оценки и выбора вариантов на разных этапах ее жизненного цикла. Определена целесообразность построения методологии оптимизации сети объектов Главного центра специального контроля на идеях

агрегативно-декомпозиционного и блочно-иерархического подходов. Предложена трехуровневая схема декомпозиции проблемы оптимизации сети, которая включает множество задач ее проектирования, планирования развития, адаптации и реинжиниринга. Установлены состав и схема взаимосвязи с входящими и исходящими данными задач системного проектирования сети. Практическое применение полученных результатов для решения проблемы оптимизации сети объектов Главного центра специального контроля позволит сократить сроки решения задач проектирования и планирования ее развития, уменьшить расходы на ее модернизацию или реинжиниринг, а за счет совместного решения задач – повысить качество решений и на этой основе улучшить функциональные характеристики сети. Методология системологического анализа проблемы оптимизации территориально распределенных объектов может быть использована при проектировании информационных систем, распределенных систем обслуживания и многомасштабного мониторинга.

Ключевые слова: *сеть; оптимизация; реинжиниринг; специальный контроль.*

V. V. Bezkorovayny, Yu. O. Gordienko, A. V. Koshel, K. K. Kulagin, O. I. Solonets

SYSTEMOMOLOGICAL ANALYSIS OF THE PROBLEM OF OPTIMIZING THE NETWORK OF MAIN CENTER OF THE SPECIAL MONITORING OBJECTS

Structural, cost and functional characteristics of distributed systems are largely determined by the topology of their subsystems and elements. In its turn the topology of subsystems and elements determines the topology of communication links, providing the exchange of resources and information between elements and subsystems. It is common for many modern technical, organizational and technical, and socio-economic systems.

The article analyzes the factors, which determine the efficiency of the network of Main Center of the Special Monitoring objects as a territorially distributed system, formalizes its structural description and designation purpose. It formulates the problem of optimizing the network of Main Center of the Special Monitoring objects that includes complexes of tasks, which deal with the choice of structure, topology, technology of functioning, parameters of elements and connections, comprehensive assessment and choice of options at various stages of the network life cycle. The article determines the expediency of developing a methodology for optimizing the network of the objects of Main Center of the Special Monitoring on the ideas of aggregation-decomposition and block-hierarchical approaches. It suggests the three-level scheme for decomposition of the network optimization problem; that scheme includes the sets of tasks for the network design, evolution planning, adaptation and reengineering. In the article the composition and scheme of interconnections with input and output data of the tasks of network system design are determined. It is concluded that practical application of the obtained results for solution of the problem of optimizing the network of Main Center of the Special Monitoring objects will reduce the time expenditures inevitable in solution of the tasks of the network design and its development planning; it will also reduce the expenses for its modernization or reengineering, through the joint solution of tasks it will improve the quality of solutions and enhance on that basis the network's functional characteristics. The methodology of systemologic analysis of the problem dealing with optimization of geographically distributed objects can generally be used in the design of any information systems, distributed service systems and large-scale monitoring.

Keywords: *network; optimizing; reengineering; special monitoring.*

УДК 659.21 DOI: 10.46972/2076-1546.2019.16.06

І. О. Орищук, Г. Д. Носова, Л. М. Марищук

ОСНОВНІ ПРИНЦИПИ СТВОРЕННЯ ЕФЕКТИВНОГО ВІЗУАЛЬНОГО ПОВІДОМЛЕННЯ

Стаття присвячена визначенню основних принципів створення візуального повідомлення, дотримання яких сприятиме підвищенню ефективності його впливу на цільову аудиторію. В умовах ведення Росією гібридної війни проти України питання контрдій актуальні як ніколи. Зважаючи на світові дослідження з психології, можна стверджувати, що ефективність сприйняття інформації залежить, зокрема, від домінуючого каналу сприйняття (аудіального, візуального, кінестетичного). Проте результати низки психологічних дослідів у галузі візуального сприйняття показали, що краще зрозуміти, запам'ятати та відтворити ту інформацію, яку ми отримуємо через свої зорові канали. Сучасні дослідження соціальних проблем приводять до розуміння: світ став візуальним. Людина нашого часу знаходиться під постійним впливом візуального контенту. Тож донесення до свідомості необхідної інформації ефективно здійснювати через цей канал. Таким чином, саме візуальне повідомлення є дієвим інструментом як контрпропаганди, так й інформування населення в інтересах діяльності Збройних Сил України. Результат проведених наукових досліджень ґрунтується на вивченні особливостей зорового сприйняття інформації про навколишній світ та пов'язаних із цим можливостей щодо використання двовимірного простору в інтересах створення продукції психологічного впливу. Було проаналізовано дію кольору на підсвідомість людини, емоціогенну структуру колірних комбінацій, психологічні ефекти символьного кодування інформації, загальні правила композиції, приклади успішного графічного маркетингу. Для формування практичних рекомендацій з реалізації запропонованих принципів було враховано загальні видавничі підходи до створення друкованої візуальної продукції, технологічні особливості різних типів носіїв, ефективність каналів розповсюдження продукції психологічного впливу та результати аналізу цільової аудиторії.

Ключові слова: *візуальне повідомлення; маркетинг; психологічний вплив; цільова аудиторія.*

Постановка проблеми в загальному вигляді. Психологічні особливості візуального сприйняття людиною навколишнього світу покладено в основу багатьох сфер її діяльності. На цих механізмах базується більшість видів мистецтва та методів навчання, їх насамперед враховують під час виробництва та продажу товарів і послуг масового вжитку, в економіці, політиці тощо. Розуміння процесу візуального сприйняття є основним у ході формування новин чи подання інформації будь-якого змісту.

Для сучасних українських реалій, коли наша держава перебуває в епіцентрі гібридних атак агресивного та непередбачуваного противника, яким є Росія, питання безпеки та протидії негативним інформаційно-психологічним впливам стають більш ніж актуальними. Засилля ворожої пропаганди в зоні ведення бойових дій на сході України та в анексованому Криму, активні намагання порушити крихку стабільність зсередини через

розповсюдження у форматі листівок, плакатів, рекламних банерів, повідомлень у друкованих та інтернет-виданнях по всій території держави маніпулятивних впливів вимагають від нас чіткого розуміння шляхів та способів протидії агресору на інформаційній арені. Для ефективної боротьби першочерговим завданням є вивчення усіх особливостей візуального сприйняття та методів "правильного" подання інформації.

Аналіз останніх досліджень та публікацій. У наш час проблемам створення ефективного візуального повідомлення (ВП) присвячено значну кількість наукових досліджень і публікацій. Так, автори [1–3] спираються на вивчення процесів та механізмів візуального сприйняття людини як здатності до осмислення образів, що дозволяє інтерпретувати сутність інформації, отриманої завдяки нашому зору. Цей підхід дає змогу зрозуміти психологічні особливості інтерпретації того, що ми бачимо, та зрештою допомагає на етапі проєктування продукції. Однак використання лише його не забезпечує всебічного охоплення складного та багатофакторного процесу, звужуючи можливості з виготовлення дійсно ефективного візуального повідомлення.

Фахівці маркетингового дизайну [4–8], поширюючи зміст повідомлення, загострюють увагу на встановленні єдності (спільності) його сприйняття з товаром, запропонованим користувачу, створенні комунікаційного каналу, за допомогою якого відбувається переміщення повідомлення від відправника до одержувача. Як найбільш поширена форма неособистісної комунікації розглядається реклама, діяльність якої в Україні регламентується законодавством [9] і визначається як "спеціальна інформація про осіб чи продукцію, яка розповсюджується в будь-якій формі й у будь-який спосіб з метою прямого або опосередкованого одержання зиску". Іншими словами, спеціальна інформація, що міститься в рекламному повідомленні, повинна вплинути на поведінку цільової аудиторії (ЦА). Найбільш поширеною формою такого впливу є передача одержувачу ВП.

Формулювання завдання дослідження. На сьогодні ВП залишається чи не найпершим дієвим інструментом упровадження потрібного наративу в зоні проведення операції Об'єднаних сил. Підготовка такого повідомлення, ефект від якого буде максимальним, вимагає розуміння усіх складових цієї роботи. Отже, метою та завданням статті є: розглянути основні принципи розробки ефективного ВП, визначити фактори впливу на його сприйняття ЦА та надати деякі рекомендації за визначеним напрямком.

Виклад основного матеріалу. Основою ефективного ВП є розумне та збалансоване застосування усіх важелів впливу на якість сприйняття людиною (ЦА) інформації. Усі повідомлення можна умовно поділити на дві групи: вербальні та невербальні. Схема на рис. 1 показує, які саме важелі належать кожній групі.

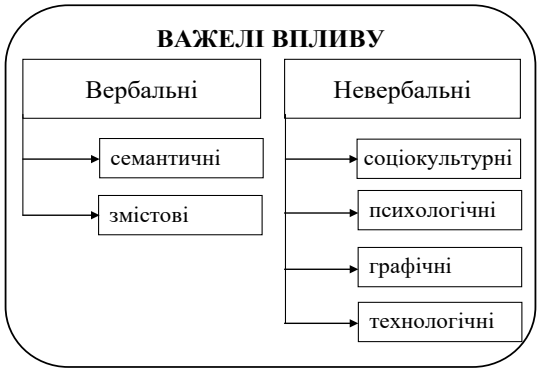


Рис. 1. Важелі впливу на якість сприйняття ВП

Поділ на групи є досить умовним, адже взаємозв'язок між усіма елементами окремо та в цілому досить тісний. Це унеможливлює виділення одного з них як більш вагомого. Розробник ВП повинен однаково уважно ставитися до використання кожного з цих елементів для отримання продукту, який найбільш ефективно "спрацює".

Фахівці з візуального маркетингу наголошують [10]: "Сучасний користувач бажає отримувати якісний контент, але ще більше, що він матиме доступний та зрозумілий формат". Широкі можливості з втілення зазначеного підходу надає створення друкованої продукції. Зрозуміло, що цей процес трудомісткий та потребує урахування численної кількості різноманітних факторів, зокрема, глибокого вивчення ЦА, врахування її психологічних і соціально-психологічних характеристик, групової належності, національної та релігійної специфіки, морально-психологічного стану, соціально-політичної ситуації тощо. Однак виділити загальні принципи створення якісного ВП усе ж таки можливо. Для цього насамперед доцільно визначити фактори впливу на його ефективність, до яких, зокрема, належать: психологічні, графічні, колірні, технологічні та фактори взаємодії (рис. 2).

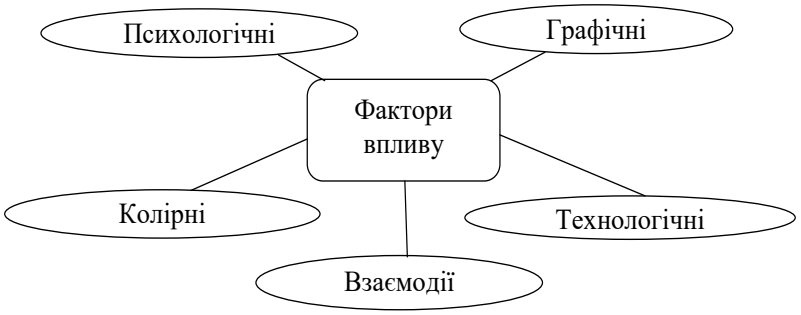


Рис. 2. Фактори впливу на ефективність візуального повідомлення

Серед психологічних факторів виділяють:

систему цінностей суспільства (ЦА, об'єкта впливу);

психологічну толерантність системи цінностей (її стійкість до зовнішніх або внутрішніх деструктивних дій);

індивідуальну (масову) свідомість;

психологічну толерантність свідомості (її стійкість до маніпулятивних впливів і щодо залучення до протиправної діяльності маніпулятивними методами прихованого примусу особистості);

психічне здоров'я;

толерантність психічного здоров'я (його стійкість до зовнішніх чи внутрішніх деструктивних дій) [11].

Колірні фактори впливу безпосередньо ґрунтуються на механізмах візуального сприйняття. До них належать такі:

конгруентність кольору;

психологічні особливості кольору [12];

символізм кольору для визначеної ЦА;

колірна гармонія.

ВП саме по собі можна визначити як думку (слово, образ тощо), вираження якої ми можемо бачити безпосередньо – зафіксоване у вигляді символів, знаків, картинок і т. ін. Отже, врахування графічних факторів впливу на ефективність ВП є дуже важливим завданням для розробника, до них належать: кодові засоби (знаки, предмети, символи) та порядок їх застосування; графічне оформлення слова (тип, розмір, форма, ритм, художній вигляд шрифту); грамотність; зручність читання (шрифтова композиція, чіткість шрифту, зрозумілість).

Технологічні фактори враховуються з огляду на порядок виготовлення готового зразка продукції і включають:

урахування видавничих принципів (відповідність розміру форматові);

якість характеристики носія (відповідність якості контенту носієві);

дотримання правил композиції, балансу.

Узгодженість, гармонійність усіх елементів ВП – запорука того, що закладений у нього генеральний меседж досягне своєї мети. Забезпечення потрібного ефекту неможливе без урахування факторів взаємодії окремих елементів один з одним та з органами чуттів споживача продукції (ЦА). Тут слід врахувати:

управління напрямом погляду;

дотримання балансу графічних елементів та засобів їх відображення.

Якісне ефективне ВП – це кінцевий продукт, побудований на основі ґрунтовного аналізу ЦА для досягнення чітко визначеної мети з урахуванням усіх можливих факторів впливу. Реалізація цього твердження неможлива без дотримання під час його створення певних принципів. Розглянемо їх.

Візуальна помітність. Повідомлення має бути візуально помітним, для цього розмір, колірна гама, ритмічність сполучення елементів, спосіб подання змісту, загальна експозиція повинні бути узгодженими за стилем, не мати розбіжностей, відповідати загальній меті.

Візуальна риторика простору повторює риторику ідеологічну.

Ідеальна змістовна частина. Мета якісного копірайтингу, або створення ідеального тексту, полягає в тому, аби "за допомогою художніх засобів та знання психотехнологій глибинного впливу через медіа на суспільне несвідоме викликати в потенційної аудиторії послідовність емоцій, відчуттів і переживань, що в результаті сформують бажання стати споживачем певної інформаційної продукції" [13, 14]. При цьому під час розробки змістовної частини доцільно керуватися формулою AIDMA (рис. 3), що є модифікацією відомої моделі AIDA, запропонованої Е. Левісом ще в XIX столітті. Вона описує ідеальний текст як такий, що має викликати спочатку увагу, потім інтерес, бажання та зрештою дію.

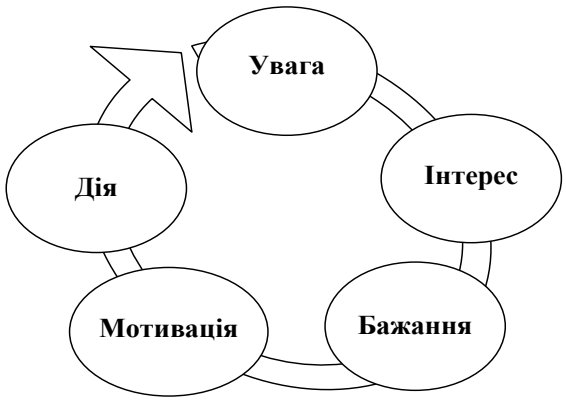


Рис. 3. Модель AIDMA

Користуючись загальними *видавничими принципами*, слід обов'язково враховувати призначення продукту та ЦА. Вибирати тип, форму, розмір, вагу носія інформації треба так, щоб повідомлення можливо було легко розповсюдити з найбільшою ймовірністю його доведення до визначеної ЦА. На якість друкованої продукції значно впливають фізичні характеристики паперу, такі як: форма, текстура, якість, розмір та маса. Якість і текстура впливають на зручність читання і правильне сприйняття кольору. Висока якість паперу потрібна для правильної передачі кольорів, вона впливає на довговічність друкованої продукції. Основними показниками, від яких залежить щільність і розмір паперу, є: довжина і структура повідомлення, засоби розповсюдження, можливості засобів друку, доступний матеріал.

У разі виготовлення друкованої візуальної продукції, тобто розміщення ВП на носії (папір, плівка, нестандартні носії тощо), необхідно оптимально вибирати між якістю і вартістю виготовлення. Основним правилом є: ВП високої якості не повинно бути розміщене на носіях низької якості й довговічності.

Висновки. Створення ефективного ВП є багатофакторним, багатокритерійним завданням, яке потребує від розробника широких знань у різних галузях життя, якісного вивчення ЦА, уваги до деталей, креативного мислення. Дотримання сформульованих у статті принципів дозволить створити такий продукт, який стане ефективним інструментом підтримки інформаційної кампанії, психологічної операції (акції) тощо. Подальші дослідження цієї актуальної наукової проблеми необхідно спрямувати на удосконалення методології практичного застосування виявлених закономірностей узгодження різних засобів кодування інформації у ВП для підвищення ефективності його впливу на ЦА.

СПИСОК ЛІТЕРАТУРИ

1. Котлер Ф., Вероника В., Сондерс Д., Армстронг Г. Основы маркетинга. 4-е изд. Москва : "Вильямс", 2007. 1200 с.

2. Арнхейм Р. Искусство и визуальное восприятие / Пер. с англ. В. Н. Самохина, общ. ред. В. П. Шестакова. Москва : "Прогресс", 1974. 393 с.

3. Гибсон Дж. Экологический подход к зрительному восприятию / Пер. с англ. Т. М. Сокольской, общ. ред. А. Д. Логвиненко. Москва : Прогресс, 1988. 461 с.

4. Рижова І. С. Філософія дизайну: теоретико-методологічні засади : монографія. Запоріжжя : ЗНТУ, 2006. 540 с.

5. Білодід Ю. М., Поліщук О. П. Основи дизайну : навч. посіб. Київ : Парапан, 2004. 240 с.

6. Загородній А. Г., Вознюк Г. Л., Комарницький І. М. Торгівля, маркетинг, реклама : термінол. словник. Львів : Львів. політехніка, 2011. 312 с.

7. Палига Є. М. Основи сучасного маркетингу: навч. посіб. Львів, 2007. 236 с.

8. Липчук В. В., Дудяк Р. П., Бугіль С. Я., Янишин Я. С. Маркетинг : навч. посіб. Львів : "Магнолія 2006", 2012. 456 с.

9. Про рекламу : Закон України від 03.06.1996 № 270/96-ВР (зі змінами і доповненнями) // База даних "Законодавство України" / Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80 (дата звернення: 21.09.2018).

10. Зрительное восприятие // Сайт компанії CogniFit. URL: https://www.cognifit.com/ru/science/cognitive-skills/visual-perception (дата звернення: 13.12.2018).
11. Грачев Г., Мельник И. Манипулирование личностью: Организация, способы и технологии информационно-психологического воздействия. Москва, 2002. 153 с.
12. Люшер М. Цветовой тест Люшера. Москва : Сова, 2005. 192 с.
13. Зеленін В. В. Основи міфодизайну: психотехнології керування медіареальністю. Київ : Гнозіс, 2017. 168 с.
14. Зеленин В. В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандистської війни : навч. посіб. Київ : "Люта справа", 2015. Т. 1. 384 с.

Подано 29.12.2018

И. А. Орищук, А. Д. Носова, Л. М. Марищук

ОСНОВНЫЕ ПРИНЦИПЫ СОЗДАНИЯ ЭФФЕКТИВНОГО ВИЗУАЛЬНОГО СООБЩЕНИЯ

Статья посвящена определению основных принципов создания визуального сообщения, следование которым способствует повышению эффективности его влияния на целевую аудиторию. В условиях ведения Россией гибридной войны против Украины, вопросы контрдействий актуальны как никогда. Учитывая мировые исследования по психологии, можно утверждать, что эффективность восприятия информации зависит, в частности, от доминирующего канала восприятия (аудиального, визуального, кинестетического). Однако результаты серии психологических опытов по вопросам визуального восприятия показали, что лучше понимать, запоминать и воспроизводить ту информацию, которую мы получаем через свои зрительные каналы. Современные исследования социальных проблем приводят к пониманию: мир стал визуальным. Человек нашего времени находится под постоянным влиянием визуального контента. Поэтому донесение до сознания необходимой информации эффективно осуществлять через этот канал. Таким образом, именно визуальное сообщение является действенным инструментом как контрпропаганды, так и информирования населения в интересах деятельности Вооруженных Сил Украины. Результат проведенных научных исследований опирается на изучение особенностей зрительного восприятия информации об окружающем мире и связанных с этим возможностей по использованию двумерного пространства в интересах создания продукции психологического влияния. Кроме того, был проведен анализ психологического воздействия цвета на подсознание человека, эмоциогенной структуры цветовых комбинаций, психологических эффектов символьного кодирования информации, общих правил композиции, примеров успешного графического маркетинга. При формировании практических рекомендаций по реализации предложенных принципов были учтены общие издательские подходы к созданию печатной визуальной продукции, технологические особенности разных типов носителей, эффективность каналов распространения продукции психологического влияния и результаты анализа целевой аудитории.

Ключевые слова: *визуальное сообщение; маркетинг; психологическое влияние; целевая аудитория.*

I. O. Oryshchuk, A. D. Nosova, L. M. Maryshchuk

BASIC PRINCIPLES FOR CREATING AN EFFECTIVE VISUAL MESSAGE

The article is devoted to the definition of the basic principles of creating a visual message, the adherence to which contributes to the effectiveness of its influence on the target audience. In the context of Russia's hybrid war against Ukraine, counter-terrorism issues are more urgent than ever. In light of world research in psychology, the effectiveness of perceiving information depends, in particular, on the dominant channel of perception (audio, visual, kinesthetic). However, the results of a number of psychological experiments in the field of visual perception have shown that it is better to understand, memorize and reproduce the information we receive through our visual channels. Modern research of social problems leads to understanding - the world has become visual. Man of our time is under constant influence of visual content. So reporting to the consciousness of the necessary information effectively through this channel. Thus, the very visual message is an effective tool for counterpropaganda and for informing the population in the interests of the Armed Forces of Ukraine. The result of the research is based on the study of the peculiarities of the visual perception of information about the world and, related to this, the possibilities of using two-dimensional space in the interests of creating products of psychological influence. In addition, an analysis was conducted of the psychological effect of color on the human subconscious, the emotiogenic structure of color combinations, the psychological effects of symbolic coding of information, general rules of composition, examples of successful graphic marketing. In forming practical recommendations for the implementation of the proposed principles, general publishing approaches to the creation of printed visual products, the technological features of different types of media, the effectiveness of distribution channels for products of psychological influence and the results of the analysis of the target audience were taken into account.

Keywords: *visual message; marketing; psychological influence; target audience.*

ISSN 2076-1546

УДК 004.021 DOI: 10.46972/2076-1546.2019.16.07

М. П. Романчук

ОБҐРУНТУВАННЯ ТИПУ ФРЕЙМВОРКІВ ГЛИБОКОГО НАВЧАННЯ ДЛЯ ОБРОБЛЕННЯ ДАНИХ ДИСТАНЦІЙНОГО ЗОНДУВАННЯ ЗЕМЛІ

Важливим завданням у ході обробки даних дистанційного зондування Землі є автоматизація процесу дешифрування аерокосмічних знімків, зокрема виявлення та розпізнавання об'єктів у військовому дешифруванні. У статті розглянуто напрями автоматизації дешифрування знімків та виділено з них перспективний, що ґрунтується на використанні нейронних мереж глибокого навчання. Також проаналізовано технічні завдання, які виникають у ході створення алгоритмів та розгортання навчених моделей на різноманітних мобільних пристроях.

З'ясовано важливу роль програмних каркасів глибокого навчання в процесі тренування моделей нейромереж, метою яких є полегшення розробки та розгортання. Проаналізовано зміни популярності програмних каркасів протягом останніх років та акцентовано на потребі аналізу їх можливостей, що динамічно змінюються. Досліджено найпоширеніші програмні фреймворки для втілення підходів глибокого навчання, їх переваги та недоліки щодо розв'язання завдань тематичного дешифрування на доступних обчислювальних ресурсах. Розглянуто типи обчислювального графа, які використовують програмні каркаси глибокого навчання, та мови програмування, за допомогою яких можна створювати та розгортати моделі нейромереж. Здійснено аналіз фреймворків за обраними критеріями: розподілене виконання, оптимізація архітектури, відображення процесу навчання, спільна підтримка та портативність. У результаті виділено програмний каркас, який слід використовувати для проведення досліджень, та зроблено висновок про переважний фреймворк у промисловому використанні в ході глибокого навчання нейронної мережі для оброблення даних дистанційного зондування Землі.

Ключові слова: *машинне навчання; нейронні мережі глибокого навчання; обчислювальний граф; автоматизація дешифрування; аерокосмічні знімки; фреймворк; виявлення об'єктів; дистанційне зондування Землі.*

Постановка проблеми в загальному вигляді. Досвід локальних війн та збройних конфліктів останніх десятиліть доводить, що однією з основних тенденцій сучасного розвитку військової справи є інформатизація боротьби. Підвищення рівня інформатизації в державних органах, які здійснюють повноваження у сфері національної безпеки та оборони, передбачається досягти, зокрема, за рахунок моніторингу земної поверхні за результатами дистанційного зондування.

Прийняття рішень посадовими особами залежить від оперативності й достовірності оброблення даних дистанційного зондування Землі (ДЗЗ), а саме дешифрування знімків. Усі завдання дешифрування аерокосмічних знімків можна розділити на дві групи:

щодо одержання узагальненої інформації про земну поверхню;

щодо визначення наявності об'єктів на ній та їх характеристик.

Залежно від призначення і завдань, розв'язуваних у процесі дешифрування знімків, розрізняють два види дешифрування: загальногеографічне і галузеве. Найважливішим різновидом останнього є військове дешифрування знімків.

Військовим дешифруванням називається процес виявлення, розпізнавання й інтерпретації розташованих на місцевості об'єктів за їх зображеннями на знімках, а також визначення їх кількісних і якісних характеристик [1], що зазвичай здійснюється в ручному режимі дешифрувальником і має низку недоліків, а саме: низьку оперативність дешифрування, високі вимоги до підготовки спеціалістів, а звідси і вартість дешифрування, суб'єктивність тощо. Тому актуальним завданням є здійснення автоматизації процесу дешифрування аерокосмічних знімків.

Аналіз останніх досліджень і публікацій. Об'єкти на аерокосмічних знімках вирізняються за дешифрувальними ознаками, які поділяються на прямі та непрямі [1]. До прямих належить форма, розмір, колір, тон та тінь, а також складно об'єднувальна ознака – малюнок зображення. Непрямими ознаками є розміщення об'єкта, його географічне сусідство, сліди взаємодії з навколишнім середовищем.

Автоматизоване дешифрування знімків передбачає оброблення даних у цифровому вигляді з використанням обчислювальних засобів із відповідним програмним забезпеченням. Таке програмне забезпечення створюється на основі вирішення завдання «розпізнавання образів», що потребує своєрідного «банка пам'яті», де зібрані характеристики природних та штучних об'єктів.

Перспективні автоматичні способи дешифрування аерокосмічних знімків використовують машинне навчання (англ. ML) і нейронні мережі. Застосування останніх ґрунтується на самонавчанні з використанням типових образів об'єктів розпізнавання та принципів багатошаровості. У базі даних знаходяться еталони об'єктів у всіх можливих ситуаціях, а кожен шар нейронної мережі працює із зображенням на своєму рівні абстракції, деякі шари визначають межі об'єктів, що базується на перепадах контрасту, інші – форму, або колір об'єктів тощо. Процес самонавчання мережі формує машинне уявлення об'єкта.

Чим більше вхідних даних – тим з більшою ймовірністю буде розпізнаний об'єкт на знімку, однак важливим питанням є організація процесу навчання нейронної мережі: реалізація алгоритмів на обчислювальних засобах.

Глибоке навчання (англ. DL) [2] – це набір здатних навчатися алгоритмів, що моделюють абстракції високого рівня в даних з використанням архітектури та складаються з декількох нелінійних перетворень. Створення алгоритмів та розгортання навчених моделей є достатньо важким завданням для вчених та інженерів з обробки даних. Для стандартизації процесу розробки програмних продуктів створено низку бібліотек або фреймворків DL, метою яких є полегшення розробки складних систем. Проте існують обмеження, що задають правила створення структури проєкту та написання коду. Наявні фреймворки глибокого навчання посилили загальну масштабність можливості досліджень у рамках цієї сфери, здійснили перехід до розробки моделей ML, що вже працюють на мобільних пристроях. Нові фреймворки та методи дозволяють розробити інструменти, що можуть запропонувати кращий рівень абстракції, а також спростити програмування. Можливості фреймворків динамічно змінюються, що потребує їх аналізу.

У табл. 1 наведено порівняння наукових статей в електронному репозиторії arXiv (cs.AI, cs.LG, cs.CV, cs.CL, cs.NE, stat.ML), у яких згадуються фреймворки, використовувані в сфері DL. Порівняння було проведено в повному тексті із загальною кількістю поданих документів, розміщених у січні – вересні 2018 року.

Таблиця 1

Загальна кількість розміщених статей із машинного навчання в arXiv

Фреймворк DL	Розміщено за період	% статей
Tensorflow	131	44,41
Keras	27	9,15
PyTorch	51	17,29
MxNet	27	9,15
Caffe	19	6,44
Caffe2	3	1,02
CNTK	10	3,39
Theano	10	3,39
Torch	10	3,39

Так, 44% усіх документів, поданих у січні – вересні 2018 року, згадують TensorFlow.

На рис. 1 показано, як із часом змінювалася популярність фреймворків (у відсотках) у пошукових запитах Google.

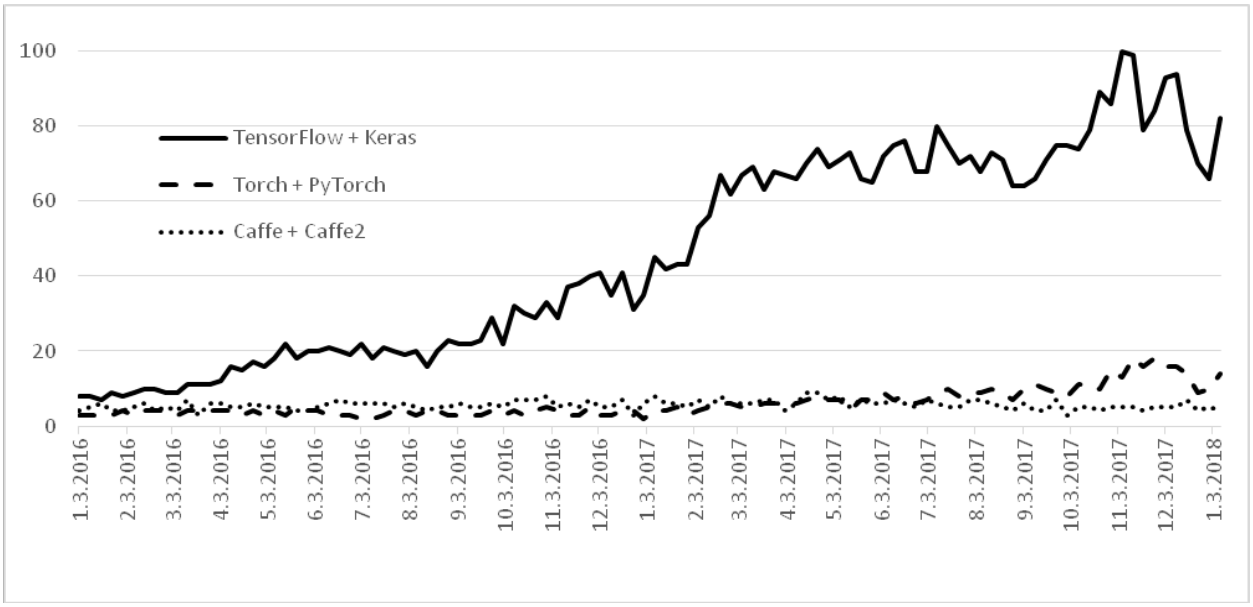


Рис. 1. Динаміка зміни популярності фреймворків

З рис. 1 видно, що Theano широко використовувався великий проміжок часу, але його зростання дещо сповільнилося. Caffe швидко зріс в 2014 році, але останні роки його випередив TensorFlow, який є продовженням Theano. Torch (з недавнього часу його продовженням є PyTorch) також зростає повільно і стабільно.

Формулювання завдання дослідження. Досить складно навіть для досвідчених дослідників та розробників визначити з усього набору фреймворків DL найбільш придатні для вирішення завдань на доступних обчислювальних ресурсах. Кожен фреймворк

побудований іншим способом для різних цілей. Розглянемо основні, щоб дати уявлення про те, які з них будуть кращими для автоматизованого розпізнавання зображень на аерокосмічних знімках.

Отже, метою статті є аналіз переваг та недоліків фреймворків глибокого навчання з метою визначення переважного у завданні виявлення і розпізнавання об'єктів за даними ДЗЗ.

Виклад основного матеріалу. Перш за все необхідно розглянути загальні риси найпоширеніших програмних каркасів.

Фреймворк **TensorFlow** розроблений компанією Google Brain для здійснення досліджень ML та DL. Він використовує статичний обчислювальний граф, який створюється перш ніж модель буде працювати [3–8]. TensorFlow доступний як на стаціонарних комп'ютерах, так і на мобільних пристроях, він дозволяє розробляти моделі за допомогою мов програмування Python, C++ та R, також надає прикладний програмний інтерфейс (англ. API) для їх використання в .NET мовами програмування Java, C, Go, JavaScript. TensorFlow – фреймворк із низьким рівнем програмування, що дозволило на його основі створити низку інших фреймворків, які мають на меті забезпечити шари абстракції високого рівня (Keras, Sonnet, TFLearn тощо). У TensorFlow можна визначити: планувальники, які є вхідними вузлами в обчислювальному графі, наприклад, вхідні дані; змінні – це значення, що існують в обчислювальному графі, наприклад, ваги та зміщення. На сьогодні TensorFlow має обмежену підтримку динамічних входів через Tensorflow Fold.

Фреймворк **Keras**, написаний на Python, є API для побудови нейронних мереж на високому рівні [9]. Його можна використовувати додатково до TensorFlow, Theano або CNTK. Keras призначений для прискорення створення моделі нейромережі. Він здійснює модульне виконання: модель розглядається як послідовність чи як граф автономних, повністю сконфігурованих модулів, які можна з'єднувати разом із мінімальними обмеженнями. Нові модулі легко додаються у вигляді нових класів та функцій.

Фреймворк **PyTorch,** розроблений компанією Facebook, використовує динамічний обчислювальний граф [10], який передбачає побудову нового графа на кожному прохідному етапі. PyTorch має об'єктно-орієнтований підхід, що також дозволяє легко розширювати його функціональні можливості, визначаючи власні класи.

Три рівні абстракції PyTorch полегшують його використання. Тензор у PyTorch – це імперативний nd-масив, подібний до numpy, що має здатність працювати на графічному процесорі (англ. GPU). Змінна є вузлом в обчислювальному графі, який дуже схожий на тензор, змінну і заповнювач у TensorFlow. Модуль – нейронний шар, який може зберігати навчені ваги, що можна використовувати для створення власних класів нейронних мереж.

Фреймворк **MXNet**, розроблений компанією Apache Software Foundation, підтримується компаніями Amazon, Microsoft. Він використовує мови програмування Python та C++, а також JavaScript, R і Go. MXNet здатний масштабувати і працювати з безліччю GPU за допомогою постпроцесорного компілятора, написаного на C++ і Compute Unified Device Architecture (CUDA), що робить його незамінним для промислового використання. Він забезпечує високу продуктивність і відмінну масштабованість, має гарні навички класифікації. Незважаючи на ці переваги, MXNet має невелику сферу застосування та дуже обмежену до використання документацію.

MXNet підтримує мережі з довгою короткотерміновою пам'яттю (англ. LTSM) разом із рекурентними (англ. RNN) та згортковими (англ. CNN) нейронними мережами.

У жовтні 2017 року Amazon Web Services та Microsoft випустили новий фреймворк DL, який називається Gluon та є обгорткою MXNet, незабаром він також включатиме CNTK у Microsoft. Розробники стверджують, що інтерфейс Gluon спрощує розробку моделей DL, не відмовляючись від швидкості навчання. Він пропонує простоту кодування та більшу гнучкість, крім динамічних графів і високої продуктивності.

Фреймворк **Caffe** підтримується інтерфейсами C, C++, Python та MATLAB, а також інтерфейсом командного рядка. Він добре відомий своєю швидкістю, масштабованістю і його застосуванням у моделюванні CNN. Перевага від використання C++ у Caffe (постачається з інтерфейсом Python) – це можливість доступу до відкритих мереж DL мережного сховища Caffe Model Zoo, які попередньо підготовлені та можуть бути використані одразу.

Caffe є популярним фреймворком глибокого навчання для обробки зображень. Проте він не підтримує дрібнозернисті мережеві шари, як TensorFlow або CNTK. Інтерфейс Python мало документований, вимагає написання власного коду C++/CUDA для GPU, що не дуже добре для RNN, і є занадто громіздким для великих нейронних мереж. Caffe в даний час широко не застосовується для наукових досліджень, але може бути затребуваним для промислового використання.

Фреймворк **Caffe2**, розроблений Facebook, є наступником Caffe. Це легкий модульний фреймворк, побудований для досягнення успіху на мобільних пристроях й у виробництві. Він використовує статичні графи, подібні до TensorFlow, і має кращий інтерфейс Python порівняно з Caffe. Моделі можна навчати в Python, серіалізувати та потім розгортати без нього. Caffe2 може бути використаний з іншими системами через ONNX, наприклад PyTorch, для ефективного розгортання навчених моделей.

Фреймворк **CNTK**, розроблений компанією Microsoft, використовує статичний обчислювальний граф, подібний до TensorFlow. Він включає в себе CNN та RNN моделі. CNTK пропонує Python API над C++ кодом. Основна перевага фреймворка полягає в можливості легко створювати моделі для програмних продуктів, пов'язаних із вирішенням завдань обробки зображень. За підтримки Microsoft це також дозволяє легко інтегрувати отримані реалізації з Azure Cloud-сервісами.

Є критичні зауваження до CNTK щодо ліцензування, оскільки Microsoft не прийняла такі ліцензії відкритого коду, як: GPL, ASF або MIT. Також відомо, що він забезпечує більш високу продуктивність та масштабованість порівняно з наборами інструментів Theano або TensorFlow під час роботи на декількох обчислювальних машинах.

У порівнянні з Caffe, коли мова йде про розробку нових складних типів шарів, у разі використання CNTK користувачам не потрібно їх реалізовувати мовою низького рівня через відмінну деталізацію будівельних блоків.

Фреймворк **Theano** розроблений у 2007 році Йошуа Бенжіо та дослідницькою групою в Монреальському інституті алгоритмів навчання (MILA), у якому TensorFlow запозичив багато ідей [10, 11]. Theano є бібліотекою Python, надзвичайно швидкою та потужною, але його критикують за те, що це глибоке навчальне середовище низького рівня. Активна розробка в рамках програми була припинена з версії 1.0. Група компаній Theano оголосила в 2017 році, що після оприлюднення останньої версії подальшого розвитку не буде.

Фреймворк **Torch** пропонує широку підтримку алгоритмів ML. До введення TensorFlow і PyTorch він був головним конкурентом Theano. Даний фреймворк має основні переваги, характерні PyTorch: використання динамічних графів та розширення можливостей. Хоча він краще розвинутий порівняно з PyTorch, один з основних недоліків його полягає у використанні мови програмування Lua. Torch використовує CUDA разом із бібліотеками C/C++ і в основному був створений для масштабування розроблених моделей та забезпечення загальної гнучкості.

Розглянемо критерії відбору, за якими буде здійснено порівняння та аналіз основних фреймворків.

1. Розподілене виконання як спосіб розв'язання трудомістких обчислювальних завдань із використанням двох і більше комп'ютерів, об'єднаних у мережу.

Розподілене виконання підтримується більшістю фреймворків: TensorFlow та PyTorch побудовані з його використанням, обчислювальний граф може бути розподілений у кластері. CNTK має розподілений модуль для використання декількох графічних процесорів та машин, однак, як згадувалося раніше, існують деякі застереження щодо ліцензування. MXNet також може розподіляти навчання, проте відстає від інших фреймворків, у документації відсутній достатній опис. Caffe2 включає в себе вбудоване розподілене навчання, яке використовує Gloo. Torch, Caffe і Theano не мають вбудованої підтримки для даного виконання завдань.

2. Оптимізація архітектури фреймворка. Усі фреймворки оптимізовані для роботи на центральному процесорі (англ. CPU або GPU), більшість з них мають можливість переключатися між процесорами.

У TensorFlow існують окремі пакети для версій, що підтримуються центральним і графічним процесорами. TensorFlow намагається з'ясувати, який пристрій використовувати залежно від операції та наявних ресурсів, а також у якому об’ємі.

У PyTorch обидві версії, що підтримуються центральним і графічним процесорами, знаходяться в одному пакеті, тому необхідно чітко визначити, на якому процесорі він повинен працювати. Існує можливість легко переносити змінні на пристрої та з них. Наприклад, якщо в GPU визначено тензор, тоді будь-які наступні операції на ньому будуть відбуватися на GPU, поки тензор не буде переданий назад CPU.

Більшість фреймворків використовують GPU Nvidia і покладаються на бібліотеки CUDA і cudNN для виконання таких обчислень, як згортки та операції над матрицями. Продуктивність може відрізняється залежно від інших чинників, наприклад розміру мережі.

Через проблеми з продуктивністю OpenGL більшість фреймворків не мають жодної підтримки для GPU за межами Nvidia. Спостерігається постійний прогрес для підтримки більшості фреймворків для обчислень на CPU, зокрема HIP від компанії AMD і MKL-DNN від компанії Intel.

3. Візуалізація. TensorFlow постачається з комплектом інструментів візуалізації, який називається TensorBoard, що дозволяє відображати тренувальний процес, конвергенцію тощо. Він використовує результати обчислень, які записуються на диск. Коли проводиться експеримент, то зберігаються підсумкові дані для певного запуску з диска. TensorBoard

може потім візуалізувати ці дані, наприклад, ви можете виконати кілька тестів для пошуку гіперпараметрів, запустити TensorBoard і одночасно порівнювати всі моделі. Це можливо робити це під час процесу навчання, оскільки TensorBoard періодично оновлюється. Отже, можна повторно візуалізувати будь-який процес будь-коли, якщо зберігати дані. TensorFlow та Keras також надається можливість використовувати метод history та стандартну бібліотеку matplotlib для аналізу результатів обчислень.

PyTorch і Torch можуть використовувати пакет visdom із Facebook для візуалізації. Інші фреймворки забезпечують мінімальні інструменти візуалізації або покладаються на бібліотеки з відкритими кодами, наприклад, graphviz та matplotlib.

Оскільки TensorBoard є бібліотекою з відкритим вихідним кодом, вона дозволяє використовувати будь-які фреймворки, у тому числі PyTorch і CNTK.

4. Спільна підтримка. TensorFlow переважає всі фреймворки, на думку розробників, оскільки він підтримується компанією Google, що полегшує доступ до його використання через сервіс Google Cloud TPU, Colaboratory. Навколо TensorFlow утворилася велика спільнота розробників із різними фреймворками, наприклад, Keras, що полегшують розробку в TensorFlow. Він використовується компанією Google у своїх продуктах та її дослідницьких групах: Google Brain і DeepMind, а також AirBnb, Dropbox, SAP, eBay тощо. Даний фреймворк також має найбільш повну документацію, підручники та книги.

PyTorch в основному застосовується дослідниками завдяки згаданим вище перевагам. Він розробляється та використовується Facebook, Twitter, NVIDIA, Salesforce, Uber, Stanford, CMU, NYU та іншими. Хоча в нього менша спільнота порівняно з TensorFlow, він має активну дошку обговорень Slack. PyTorch також має детальну документацію, офіційні підручники та книги.

CNTK підтримує переважно Microsoft. Загалом його використовують для розгортання розробниками додатків у середовищі Windows, які хотіли б включити моделі машинного навчання в прикладні та мобільні додатки.

MXNet має дошку для обговорень та список розсилки для спільноти. На сьогоднішній день Amazon значно підтримав його та інтегрував в AWS. Існує також деяка підтримка від Microsoft із введенням надбудови високого рівня Gluon, оскільки вона підтримуватиме CNTK як серверний додаток. На сьогодні покращується ситуація з документацією та підручниками.

5. Портативність. Усі фреймворки мають можливість зберігати та завантажувати конфігурацію моделі, а також вивчені параметри. Це можна зробити за допомогою Open Neural Network Exchange (ONNX), де збережена модель може бути використана в іншій структурі для висновку. Наприклад, моделі PyTorch можуть бути збережені за допомогою ONNX для розгортання на Caffe2 або CNTK. Це також дозволяє інтегрувати їх на мобільні пристрої. ONNX використовується за замовчуванням у PyTorch, Caffe2, CNTK та MXNet. Хоча TensorFlow ще не підтримує ONNX, конвертери з відкритим кодом доступні для того, щоб застосувати деяку частину цієї функції до моделі TensorFlow.

Проведене порівняння фреймворків глибокого навчання відображено в табл. 2, де наявність і кількість хрестиків позначає більш високий рівень визначеного критерію у фреймворка.

Таблиця 2

Порівняння фреймворків глибокого навчання

Критерій / Фреймворк	Розподілене виконання	Оптимізація архітектури	Візуалізація	Спільна підтримка	Портативність
TensorFlow	XX	XX	XX	XX	XX
Keras	X	XX	XX	XX	XX
PyTorch	XX	XX	XX	XX	XX
CNTK	XX	XX	X	-	XX
MXNet	X	XX	X	-	XX
Torch	-	XX	X	X	X
Caffe2	XX	XX	-	-	XX
Caffe	-	XX	X	X	X
Theano	-	XX	X	X	X

Результати аналізу характеристик найпоширеніших фреймворків показали, що недоцільно розпочинати нові проєкти на базі Torch, Theano та Caffe, тому що вони вже не оновлюються. Це стосується не функціонала та продуктивності фреймворків, а лише відсутності активного розвитку й підтримки. У зв'язку з чим розробники використовують TensorFlow, PyTorch, MXNet, CNTK і Caffe2, хоча існують застереження щодо CNTK.

Включення сумісності дає змогу швидше отримувати реалізації у виробництві. ONNX дозволяє моделювати навчання в одній системі та переносити на іншу для проведення аналізу. Моделі ONNX у даний час підтримуються в Caffe2, CNTK, MXNet та PyTorch, а також є можливість їх підключення для багатьох інших загальних структур і бібліотек. Це дозволяє користувачам більш легко переміщувати моделі між різними фреймворками.

PyTorch і TensorFlow найкраще підходять для процесу розробки та загального дослідження на низькому рівні. Вони є основою глибокого навчання із застосуванням Python. PyTorch краще підходить для проведення досліджень, оскільки простий у використанні та ґрунтується на динамічному обчислювальному графі. Переваги TensorFlow, в основному, пов'язані з його широким застосуванням, підтримкою спільнотою розробників, що дозволяє створювати програмний код для промислового використання.

Тому в системі автоматизованого дешифрування аерокосмічних знімків з метою виявлення та розпізнавання об'єктів доцільно використовувати TensorFlow як фреймворк глибокого навчання.

Висновки. Розвиток інформаційних технологій дозволяє значно збільшити кількість і якість інформації, яка використовується в інтересах сектора безпеки держави. Однак оперативність її надходження потребує автоматизації оброблення даних моніторингу, у тому числі й військового дешифрування даних ДЗЗ.

У процесі автоматизованого дешифрування аерознімків з метою виявлення та розпізнавання точкових об'єктів застосовують елементи штучного інтелекту

з використанням моделей нейромереж глибокого навчання. У процесі тренування моделей важливу роль відіграють фреймворки (програмні каркаси) глибокого навчання, метою яких є полегшення розробки та розгортання. Для побудови ефективної автоматизованої системи дешифрування необхідно обґрунтувати вибір типу фреймворка. Порівняння їх властивостей здійснювалося за такими критеріями: розподілене виконання, оптимізація архітектури, візуалізація, спільна підтримка та портативність.

Результати аналізу характеристик програмних каркасів за визначеними критеріями показали, що переважним є використання фреймворка TensorFlow для навчання нейронної мережі з метою подальшого оброблення даних ДЗЗ.

СПИСОК ЛІТЕРАТУРИ

1. Карпович И. Н. Военное дешифрирование аэроснимков : Учебник. Москва : Воениздат, 1990. 544 с.
2. Гудфеллоу Я., Бенджио Й., Курвиль А. Глубокое обучение. Москва : ДМК Пресс, 2018. 652 с.
3. TensorFlow: Large-scale machine learning on heterogeneous systems / Martın Abadi, Ashish Agarwal, Paul Barham et al. URL: https://arxiv.org/abs/1603.04467 (last accessed: 20.01.2019).
4. Hope T., Yehezkel S., Lieder I. Learning TensorFlow. Sebastopol : O'Reilly Media, 2017. 242 p.
5. McClure N. TensorFlow Machine Learning Cookbook. Birmingham : Packt Publishing Ltd, 2017. 370 p.
6. Warden P. Building Mobile Applications with TensorFlow. Birmingham : Packt Publishing Ltd, 2017. 238 p.
7. Géron A. Hands-On Machine Learning with Scikit-Learn and TensorFlow. Sebastopol : O'Reilly Media, 2017. 751 p.
8. Karim R. TensorFlow: Powerful Predictive Analytics with TensorFlow. Birmingham : Packt Publishing Ltd, 2018. 165 p.
9. Джулли А., Пал С. Библиотека Keras – инструмент глубокого обучения. Реализация нейронных сетей с помощью библиотек Theano и TensorFlow. Москва : ДМК Пресс, 2018. 294 с.
10. Deep learning with dynamic computation graphs / Moshe Looks, Marcello Herreshoff, DeLesley Hutchins & Peter Norvig Google Inc. URL: https://arxiv.org/abs/1702.02181 (last accessed: 20.01.2019).
11. Theano Development Team. Theano: A Python framework for fast computation of mathematical expressions. URL: https://arxiv.org/abs/1605.02688 (last accessed: 20.01.2019).
12. Рашка С. Python и машинное обучение. Москва : ДМК Пресс, 2017. 418 с.
13. Bengio Y. Learning deep architectures for AI. Foundations and trends in Machine Learning. 2009. № 1. P. 1–127.

Подано 29.03.2019

Н. П. Романчук

ОБОСНОВАНИЕ ТИПА ФРЕЙМВОРКОВ ГЛУБОКОГО ОБУЧЕНИЯ ПРИ ОБРАБОТКЕ ДАННЫХ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

Важной задачей в ходе обработки данных дистанционного зондирования Земли является автоматизация процесса дешифрирования аэрокосмических снимков, в том числе выявление и распознавание объектов в военном дешифрировании. В статье рассмотрены направления автоматизации дешифрирования снимков и выделено из них перспективное, основанное на использовании нейронных сетей глубокого обучения. Также

проанализированы технические задачи, возникающие при создании алгоритмов и развертывании обученных моделей на различных мобильных устройствах.

Отмечена важная роль программных каркасов глубокого обучения в процессе тренировки моделей нейросетей, целью которых является облегчение разработки и развертывания. Проанализированы изменения популярности программных каркасов в последние годы и акцентировано внимание на необходимости анализа их динамично изменяющихся возможностей. Исследованы распространенные программные фреймворки для воплощения подходов глубокого обучения, их преимущества и недостатки по решению задач тематического дешифрирования на доступных вычислительных ресурсах. Рассмотрены типы вычислительного графа, использующие программные каркасы глубокого обучения, и языки программирования, с помощью которых можно создавать и развертывать модели нейронных сетей. Осуществлен анализ фреймворков по выбранным критериям: распределенное выполнение, оптимизация архитектуры, отражение процесса обучения, совместная поддержка и портативность. В результате выделен фреймворк, который следует использовать при проведении исследований, и сделан вывод о преимущественном фреймворке в промышленном использовании в ходе глубокого обучения нейронной сети для обработки данных дистанционного зондирования Земли.

Ключевые слова: *машинное обучение; нейронные сети глубокого обучения; вычислительный граф; автоматизация дешифрирования; аэрокосмические снимки; фреймворк; выявление объектов; дистанционное зондирование Земли.*

M. P. Romanchuk

THE REASON OF THE FIREWORK TYPE OF DEPTH EDUCATION IN PROCESSING THE DATA OF REMOTE SURFACES OF THE EARTH

An important task in the processing of Earth remote sensing data is the automation of the decoding process of aerospace images, in particular the detection and recognition of objects in military decoding. In the article the directions of automation of decryption of photos are considered and promising from them is selected, which is based on the use of neural networks of deep learning, and also analyzed the technical problems that arise during the creation of algorithms and the deployment of trained models on a variety of mobile devices.

The important role of deep-instruction software frameworks in the process of training of neural network models is aimed at facilitating development and deployment. The changes in the popularity of software frameworks in recent years have been analyzed and the need to analyze their dynamically changing capabilities has been analyzed. The most widely used software frameworks for the implementation of deep learning approaches, their advantages and disadvantages for solving tasks of thematic decryption on accessible computational resources are explored. The types of computational graphs, which use the software of deep learning, and programming languages, with the help of which it is allowed to create and deploy models of neural networks are considered. The analysis of the frameworks according to selected criteria was performed: distributed execution, architecture optimization, reflection of the learning process, joint support and portability. As a result, the software framework to be used in conducting research is highlighted, and the conclusion is drawn about the predominant framework for industrial use in the course of in-depth training of the neural network for the processing of Earth remote sensing data.

Keywords: *machine learning; neural networks of deep learning; computing graph, decoding automation; aerospace images; frameworks; object detection; remote sensing of the Earth.*

ISSN 2076-1546

УДК 621.396 DOI: 10.46972/2076-1546.2019.16.08

О. Л. Сидорчук

МЕТОД ВИЗНАЧЕННЯ ЕЛЕКТРОМАГНІТНОГО ПОЛЯ, РОЗСІЯНОГО ВІД РУПОРНОГО ОПРОМІНЮВАЧА, ЩО РОЗТАШОВАНИЙ У ФОКУСІ ПАРАБОЛОЇДА ОБЕРТАННЯ АНТЕННОЇ СИСТЕМИ СТАНЦІЙ НАЗЕМНОЇ РОЗВІДКИ

У статті запропоновано вдосконалений математичний апарат для дослідження електромагнітного поля, розсіяного антенною системою з рупорним опромінювачем пірамідальної форми, розташованим у фокусі параболоїда обертання, на прикладі станцій наземної розвідки типу ПСНР «Кредо» (1РЛ133).

Удосконалення апарату полягає в застосуванні нового методу визначення розсіяного електромагнітного поля, перевипроміненого рупорним опромінювачем, що розташований у фокусі параболоїда обертання антенної системи, за нормальної поляризації падаючої плоскої хвилі до площини її падіння та збігу поляризації хвилі й площини її падіння як суперпозиції довільного падіння.

Окреслене завдання має дві складові: визначення електромагнітного поля в площині фокуса параболоїда обертання в разі довільного падіння на нього плоскої електромагнітної хвилі та знаходження електромагнітного поля, розсіяного від рупорного опромінювача колової поляризації, розміщеного в площині фокуса параболоїда обертання за умови довільного падіння на нього плоскої електромагнітної хвилі.

Надані в статті матеріали та отримані автором раніше результати об'єднує випадок довільного падіння електромагнітної хвилі, що є суперпозицією двох ортогональних варіантів її падіння. Розрахунки за новим методом дозволять оцінювати вплив різноманітних елементів, розміщених у площині фокуса, на розсіяння антенних систем в цілому за будь-якого випадку падіння хвилі на дзеркало.

Побудова радіолокаційних станцій на основі розрахованої за новим методом параболічної антени дозволить отримати значні переваги над традиційними однополяризаційними радіолокаційними станціями в разі виявлення об'єктів із малою ефективною поверхнею розсіювання і виділення їх інформативних ознак.

Ключові слова: *параболоїд обертання; дзеркальна антена; малогабаритний рупорний випромінювач; покращення поляризаційних характеристик; дифракція електромагнітної хвилі; зменшення ефективної поверхні розсіювання.*

Постановка проблеми в загальному вигляді. Сучасні радіоелектронні засоби (РЕЗ) зразків озброєння та військової техніки (ОВТ) постійно вимагають досліджень щодо підвищення ефективності їх застосування [1–3]. Особливості функціонування таких засобів найчастіше визначають їх антенні системи, які і потребують досліджень щодо удосконалення.

Параметри антенних систем значною мірою впливають на якісні показники функціонування РЕЗ різного призначення [3]. В останні роки таке удосконалення здійснюється головним чином не шляхом створення принципово нових антенних систем, а шляхом покращення характеристик спрямованості, узгодження, поляризації, розрізнювальної здатності та зменшення ефективної поверхні розсіювання (ЕПР) наявних.

Розглянемо це на прикладі радіолокаційної станції (РЛС) наземної розвідки типу ПСНР “Кредо” (1РЛ133) [4–7]. Основною її складовою є однополяризаційна антенна система, яка має дзеркальний параболоїд обертання та опромінювач пірамідальної форми.

Антени з дзеркалами у вигляді параболоїда обертання, зрізаного параболоїда, параболічного циліндра і вирізки з параболоїда обертання (зазвичай з контуром овальної форми) (рис. 1, 2) набули найбільшого поширення в сучасних радіотехнічних системах РЕЗ ОВТ. Широке застосування таких антен пояснюється можливістю формування найрізноманітніших діаграм спрямованості за відносної простоти конструкції, досить високого коефіцієнта корисної дії та малої шумової температури.

Розглянемо звичайну параболічну систему (рис. 3), що складається з двох елементів: металевого дзеркала параболічного профілю й опромінювача, розміщеного у фокусі дзеркала. Принцип роботи антени ґрунтується на тому, що сума відстаней від фокуса F до дзеркала і від дзеркала до апертури є величиною постійною $\left(FA + AA' = FD + DD'\right)$. Відповідно, якщо у фокусі розташовано джерело сферичної хвилі, то після відбиття від дзеркала вона перетворюється в плоску, а випромінювальний розкрив антени збуджується синфазно.

Рис. 1. Модернізована РЛС «Кредо-М» у складі БРМ-3К

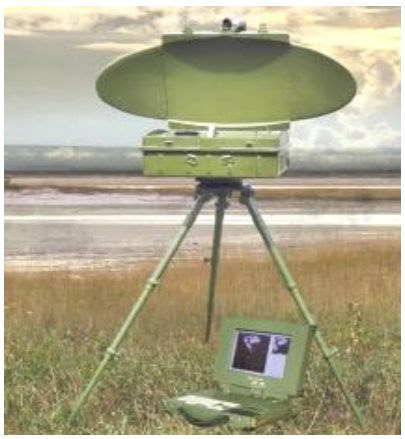


Рис. 2. РЛС наземної розвідки ПСНР-8 «Кредо-М1»

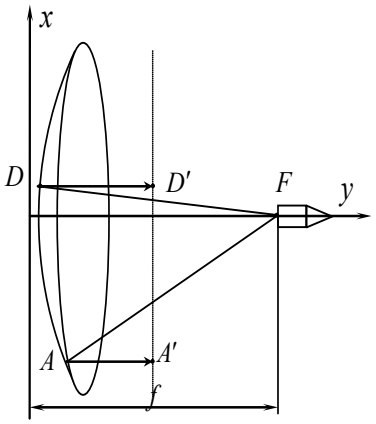


Рис. 3. Дзеркальна антена параболічного профілю

За допомогою параболоїда обертання, що виконує роль дзеркала, можна досягти такої діаграми спрямованості з високим ступенем спрямованості, коли ширина головної пелюстки за рівнем половинної потужності є однаковою в E і H площинах. Недоліком таких систем є значні втрати електромагнітної енергії, що визначаються коефіцієнтом використання поверхні антени.

Числове значення коефіцієнта використання поверхні розкриву знаходять не тільки за законом розподілу амплітуди по полю розкриву антени, але й за іншими факторами, зумовленими конструкцією антени (витік частини потужності опромінювача за краї дзеркала, затінення частини розкриву антени опромінювачем, інтерференція поля антени й поля опромінювача, неточність суміщення фазового центру опромінювача з фокусом дзеркала тощо). Повний коефіцієнт використання параболічної антени зі звичайним, наприклад, рупорним опромінювачем на практиці не перевищує 0,5–0,6 [8]. Тому побудова таких конструкцій потребує нових математичних методів розрахунку щодо зменшення розсіяного електромагнітного поля антени, а отже, і зменшення втрат.

Визначення електромагнітного поля, розсіяного від антени, яка розташована у фокусі параболоїда обертання, з погляду класичної фізичної теорії розсіяння і дифракції хвиль на перешкодах, уже давно належить до вивчених у тому сенсі, що відомі диференціальні рівняння. Для того, щоб повністю знайти дифраговане поле, потрібно лише знайти розв'язок рівняння, що відповідає граничним умовам та конкретному джерелу й перешкоді. Однак практично це дуже складна задача, навіть за простих та ідеалізованих умов.

Відомі наближені математичні методи розв'язку таких задач, що досить добре слугують для вивчення оптичних явищ, пов'язаних із розсіюванням і дифракцією, мало придатні для розв'язання загальних електродинамічних задач, особливо для радіолокаційних РЕЗ. Доведення інформації, яка утримується в неявному вигляді у хвилевому рівнянні та відповідних граничних умовах, до чисел і графіків потребує нових математичних й експериментальних методів.

Аналіз останніх досліджень і публікацій. Задача визначення розсіяного поля від рупорного опромінювача, розташованого у фокусі параболоїдного дзеркала, належить до області дифракції електромагнітних хвиль на двох тілах, причому одне з яких більше за інше. Подібні завдання вирішувалися в різних працях. У роботі [9] наведено розв'язок двомірної задачі розсіювання електромагнітної хвилі на малорозмірному імпедансному циліндрі, розташованому на фоні великого імпедансного рефлектора. Отримано систему лінійних інтегральних рівнянь Фредгольма 1-го роду відносно невідомих коефіцієнтів розкладання, яку можна розв'язати методом редукції. У [10] розглянуто задачу про випромінювання лінійної структури, розташованої поблизу ідеально-провідного екрана, що зводиться до двомірної системи рівнянь Фредгольма 1-го роду.

У роботі [11] досліджено дифракцію на провідній кулі у фокусі в разі падіння на нього плоскої електромагнітної хвилі. Поле в області фокуса визначено методом геометричної оптики, а дифракційне поле кулі – методом розкладу за мультиполями.

У [12] розглянуто задачу визначення поля в області параболоїда обертання і дифракційного поля дзеркальної антени з рупорним опромінювачем. Поле в площині фокуса оцінювалося методом хвильової оптики, а дифракційне поле дзеркальної антени визначалося в такій послідовності: після визначення поля в області фокуса знаходилося поле, перевідбите від рупорного опромінювача, яке, падаючи знову на дзеркало, створювало перевідбите поле вже від усієї антени в дальній зоні.

У [13] проаналізовано поле в області фокуса параболоїда обертання в разі падіння на нього плоскої електромагнітної хвилі, причому розглядався випадок прямого падіння плоскої хвилі. Довільне падіння електромагнітної хвилі в [13] залишилося поза увагою.

Дослідження перевипроміненого електромагнітного поля на рупорному опромінювачі станції наземної розвідки ПСНР-5 "Кредо" (1РЛ133) описані в [5–7, 15]. Вони стосувалися довільного падіння плоскої електромагнітної хвилі на розкрив пірамідального рупора, проте не розглядався випадок довільного падіння для рупорного опромінювача, розташованого у фокусі параболоїда обертання. Такі дослідження необхідні для удосконалення або проєктування нової параболічної антени з покращенням її характеристик спрямованості, узгодженості, поляризаційних параметрів та зменшення ЕПР, що зумовлює необхідність оцінювання її розсіювальних властивостей.

Отже, **метою статті** є розв'язання задачі розсіювання від рупорної антени, розміщеної

в площині фокуса параболоїда обертання в разі довільного падіння на нього плоскої електромагнітної хвилі.

Поставлене завдання включає в себе дві задачі:

а) визначення поля в площині фокуса параболоїда обертання в разі довільного падіння на нього плоскої електромагнітної хвилі;

б) визначення розсіяного поля від рупорного опромінювача, розміщеного в площині фокуса параболоїда обертання в разі довільного падіння на нього плоскої електромагнітної хвилі.

Перша задача має і самостійне значення, оскільки дозволяє оцінювати вплив різноманітних елементів, розміщених у площині фокуса, на розсіяння антени в цілому в разі косого падіння хвилі на дзеркало.

Виклад основного матеріалу. Нехай на розкрив параболоїда обертання з рупорним опромінювачем у площині фокуса (рис. 4) падає плоска електромагнітна хвиля. Необхідно визначити електромагнітне поле, розсіяне від рупорного опромінювача.

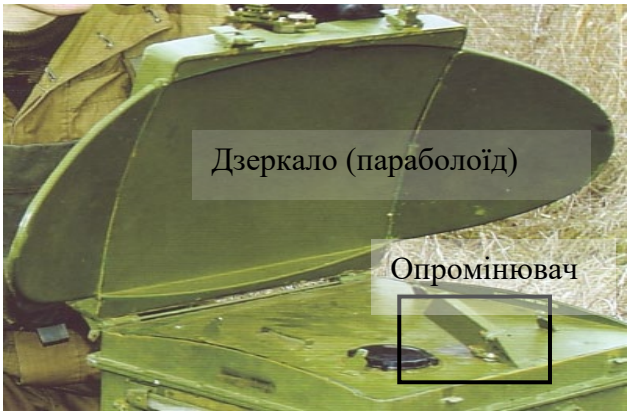


Рис. 4. Станція наземної розвідки ПСНР-5 "Кредо" (1РЛ133)

Загальний випадок довільного падіння плоскої хвилі можна розглянути як суперпозицію двох окремих: хвиля поляризована нормально до площини падіння (рис. 5); хвиля поляризована в площині падіння (рис. 6).

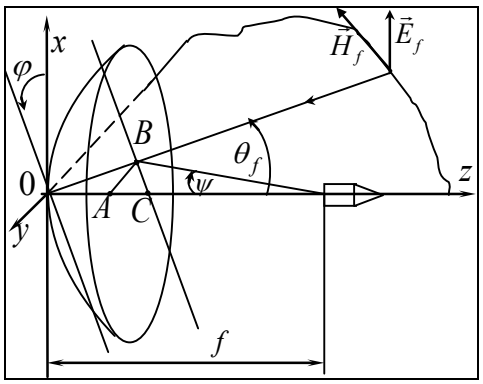


Рис. 5. Падіння плоскої електромагнітної хвилі за її нормальної поляризації до площини падіння ($\varphi_f = 3/2\pi$)

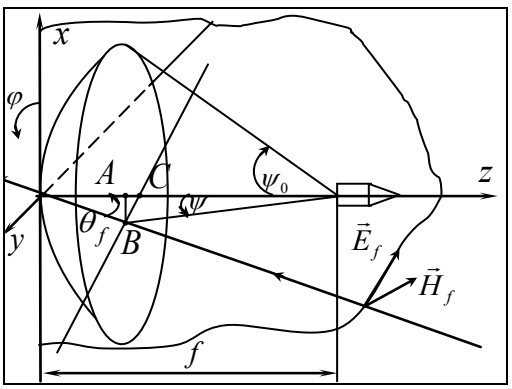


Рис. 6. Падіння плоскої електромагнітної хвилі за умови збігу площини поляризації хвилі та площини її падіння ($\varphi_f = \pi$)

У разі нормальної поляризації падаючої хвилі до площини падіння (див. рис. 1) електричну $\vec{E}_f^{\perp}$ і магнітну $\vec{H}_f^{\perp}$ складові вектора падіння електромагнітної хвилі можна записати як

$$\begin{cases} \vec{E}_f^{\perp} = \vec{e}_x E_0 e^{ikR^{\perp}}; \\ \vec{H}_f^{\perp} = -\left(\vec{e}_z \sin\theta_f + \vec{e}_y \cos\theta_f\right) e^{ikR^{\perp}} \dfrac{E_0}{Z_0}, \end{cases} \tag{1}$$

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.

У разі збігу площини поляризації з площиною падіння (рис. 2) падаюче поле має такий вигляд:

$$\begin{cases} \vec{E}_f^{\square} = \left(\vec{e}_x \cos\theta_f - \vec{e}_z \sin\theta_f\right) E_0 e^{ikR^{\square}}; \\ \vec{H}_f^{\square} = -\vec{e}_y e^{ikR^{\square}} \dfrac{E_0}{Z_0}, \end{cases} \tag{2}$$

де $R^{\perp}$, $R^{\square}$ – відстань від лінії фронту падаючої хвилі до поверхні дзеркала:

$$R^{\perp} = ftg\frac{\psi}{2}\left(tg\frac{\psi}{2} + 2tg\theta_f \sin\varphi\right)\cos\theta_f; \tag{3}$$

$$R^{\square} = ftg\frac{\psi}{2}\left(tg\frac{\psi}{2} + 2tg\theta_f \cos\varphi\right)\cos\theta_f, \tag{4}$$

де ψ – кут, утворений між віссю z і відстанню R від фокуса до параболоїда;

φ – азимутальний кут, відрахований від осі x (рис. 1, 2).

Вектор щільності поверхневого струму на дзеркалі в наближенні фізичної оптики можна визначити за відомою формулою:

$$\vec{\gamma}^{\perp,\square} = 2\left[\vec{n}, \vec{H}_f^{\perp,\square}\right], \tag{5}$$

де $\vec{n}$ – одиничний орт до поверхні параболоїда обертання, що дорівнює

$$\vec{n} = \vec{e}_z \cos\frac{\psi}{2} - \vec{e}_x \sin\frac{\psi}{2}\cos\varphi - \vec{e}_y \sin\frac{\psi}{2}\sin\varphi. \tag{6}$$

Підставляючи (1), (2), (6) у (5), отримаємо

$$j^{\perp,\square} = 2\frac{E_0}{Z_0} e^{ikR^{\perp,\square}}\left(\vec{e}_x a_x^{\perp,\square} + \vec{e}_y a_y^{\perp,\square} + \vec{e}_z a_z^{\perp,\square}\right), \tag{7}$$

де

$$\begin{cases} a_x^{\perp} = \left(sin\frac{\psi}{2} sin\varphi sin\theta_f + cos\frac{\psi}{2} cos\theta_f \right); \\ a_y^{\perp} = -sin\frac{\psi}{2} cos\varphi sin\theta_f; \\ a_z^{\perp} = sin\frac{\psi}{2} cos\varphi sin\theta_f; \end{cases} \tag{8}$$

$$\begin{cases} a_x^{\parallel} = cos\frac{\psi}{2}; \\ a_y^{\parallel} = 0; \\ a_z^{\parallel} = sin\frac{\psi}{2} cos\varphi. \end{cases} \tag{9}$$

Електричну складову електромагнітного поля, утвореного поверхневими струмами (5), можна визначити з виразу [14]

$$\vec{E}^{\perp,\parallel} = \frac{1}{i\omega\varepsilon}\left[grad\ div\vec{A}^{\perp,\parallel} + k^2 \vec{A}^{\perp,\parallel} \right], \tag{10}$$

а магнітну складову – з виразу

$$\vec{H}^{\perp,\parallel} = \frac{i}{\omega\mu} rot\vec{E}, \tag{11}$$

де $\vec{A}^{\perp,\parallel}$ – векторний електричний потенціал, утворений струмами, що течуть по поверхні дзеркала, який визначається як

$$\vec{A}^{\perp,\parallel} = \frac{1}{4\pi}\int\limits_{(S)} \vec{j}^{\perp,\parallel} \frac{e^{-ikr}}{r} ds, \tag{12}$$

де ds – елемент поверхні зі струмами:

$$ds = \frac{2f^2 sin\frac{\psi}{2}}{cos^4\frac{\psi}{2}} d\psi d\varphi, \tag{13}$$

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

$$r = \sqrt{\left(x_2 - x_1\right)^2 + \left(y_2 - y_1\right)^2 + \left(z_2 - z_1\right)^2}. \tag{14}$$

Координати точки інтегрування запишемо як

$$\begin{cases} x_1 = 2\,ftg\dfrac{\psi}{2}\cos\varphi; \\ y_1 = 2\,ftg\dfrac{\psi}{2}\sin\varphi; \\ z_1 = ftg^2\dfrac{\psi}{2}. \end{cases} \tag{15}$$

Амплітуди хвиль у розкриві рупорного опромінювача для випадку збігу поляризації хвилі, що падає, до площини її падіння визначимо з виразів [5]:

$$C^{H||}_{+mn} = \frac{-8E_0\left(1+\cos\theta_f\right)kb_p^2\sin\theta_f\sin^2\dfrac{n\pi}{2}\sqrt{1-\left(\dfrac{m\lambda}{2b_p}\right)^2-\left(\dfrac{n\lambda}{2a_p}\right)^2}}{\left(m\pi\right)^2 N^H_{mn}\cdot Z_0\left(1-\rho^H_{-mn}\rho^H_{+mn}\right)\left(1+\sqrt{1-\left(\dfrac{m\lambda}{2b_p}\right)^2-\left(\dfrac{n\lambda}{2a_p}\right)^2}\right)}\times\frac{f_{-m}\left(\theta_f\right)}{\left(1-\left(\dfrac{kb_p}{m\pi}\sin\theta_f\right)^2\right)}, \tag{16}$$

$$C^{E||}_{+mn} = \frac{8E_0\left(f_{-m}\left(\theta_f\right)\right)\left(1+\cos\theta_f\right)ka_pb_p\sin\theta_f\sin^2\left(\dfrac{n\pi}{2}\right)\sqrt{1-\left(\dfrac{m\lambda}{2b_p}\right)^2-\left(\dfrac{n\lambda}{2a_p}\right)^2}}{mn\pi^2 N^E_{mn}\left(1+\sqrt{1-\left(\dfrac{m\lambda}{2b_p}\right)^2-\left(\dfrac{n\lambda}{2a_p}\right)^2}\right)\left(1-\left(\dfrac{kb_p}{m\pi}\sin\theta_f\right)^2\right)\left(1-\rho^E_{-mn}\rho^E_{+mn}\right)}, \tag{17}$$

де b_p, a_p – розміри розкриву рупорного опромінювача;

k – хвильове число;

λ – довжина хвилі збудженого в рупорі поля;

m,n – кількість стоячих півхвиль, які вкладаються по сторонах a і b поперечного розрізу;

$\rho^H_{-mn}\rho^H_{+mn}$ або $\rho^E_{-mn}\rho^E_{+mn}$ – коефіцієнти відбиття власних функцій від внутрішніх неоднорідностей у рупорі;

$$f_{-m}\left(\theta_f\right) = \cos^2\left(\frac{m\pi}{2}\right)\sin\left(\frac{kb_p}{2}\sin\theta_f\right) - i\sin^2\left(\frac{m\pi}{2}\right)\cos\left(\frac{kb_p}{2}\sin\theta_f\right); \tag{18}$$

N^E_{mn} – норма хвиль електричного типу, що дорівнює

$$N^E_{mn} = \frac{a_pb_p}{2}Z_0\sqrt{1-\left(\frac{m\lambda}{2b_p}\right)^2-\left(\frac{n\lambda}{2a_p}\right)^2}\left\{\left(\frac{m\pi}{b_p}\right)^2+\left(\frac{n\pi}{a_p}\right)^2\right\}. \tag{19}$$

Амплітуди хвиль у розкриві рупорного опромінювача для випадку нормальної поляризації хвилі до площини її падіння визначимо з виразу [5]

$$C_{+mn}^{H_\perp} = 2E_0 \frac{n\pi}{a_p} \frac{\left(1+cos\,\theta_f\right)\sqrt{1-\left(\frac{m\lambda}{2b_p}\right)^2-\left(\frac{n\lambda}{2a_p}\right)^2}}{N_{mn}^H \cdot Z_0\left(1-\rho_{-mn}^H\rho_{+mn}^H\right)\left(1+\sqrt{1-\left(\frac{m\lambda}{2b_p}\right)^2-\left(\frac{n\lambda}{2a_p}\right)^2}\right)}\aleph, \tag{20}$$

де N_{mn}^H – норма хвиль магнітного типу, що дорівнює

$$N_{mn}^H = -\frac{a_p b_p}{2Z_0}\sqrt{1-\left(\frac{m\lambda}{2b_p}\right)^2-\left(\frac{n\lambda}{2a_p}\right)^2}\times$$
$$\times\left\{\left(\frac{m\pi}{b_p}\right)^2\left(1-\frac{sin\,2m\pi}{2m\pi}\right)\left(1+\frac{sin\,2n\pi}{2n\pi}\right)+\left(\frac{n\pi}{a_p}\right)^2\left(1+\frac{sin\,2m\pi}{2m\pi}\right)\left(1-\frac{sin\,2n\pi}{2n\pi}\right)\right\}, \tag{21}$$

$$\aleph = \int_{-\frac{a_p}{2}}^{\frac{a_p}{2}} sin\left(\frac{n\pi}{a_p}\left(y+\frac{a_p}{2}\right)\right)exp\left(-iky\,sin\,\theta_f\right)dy\int_{-\frac{b_p}{2}}^{\frac{b_p}{2}} cos\left(\frac{m\pi}{b_p}\left(x+\frac{b_p}{2}\right)\right)dx. \tag{22}$$

Амплітуди хвиль електричного типу, як з'ясовано в [15], збуджуватися не будуть. Розсіяне рупорним опромінювачем колової поляризації поле визначимо з виразів:

$$\begin{cases} \vec{E}_{xD} \cong \dfrac{\vec{e}_{ep}}{4\pi^2}\displaystyle\int_{-\infty}^{\infty}\int\left[\iint_{S_p}\left\{\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\vec{\varsigma}_{xx}\vec{C}_{-mn}^{H,E}\vec{E}_{mn}^{H,E}\,exp\left(i\left(k_x x+k_y y\right)\right)-\right.\right. \\ \left.\left.-E_{xF\tau}\left(z=0\right)exp\left(i\left(k_x x+k_y y\right)\right)dxdy\right\}exp\left(-i\left(k_x x+k_y y+k_z z\right)\right)dk_x dk_y\right]; \\ \vec{E}_{yD} \cong \dfrac{\vec{e}_{ep}}{4\pi^2}\displaystyle\int_{-\infty}^{\infty}\int\left[\iint_{S_p}\left\{\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}\vec{\varsigma}_{yx}\vec{C}_{-mn}^{H,E}\vec{E}_{mn}^{H,E}\,exp\left(i\left(k_x x+k_y y\right)\right)-\right.\right. \\ \left.\left.-E_{yF\tau}\left(z=0\right)exp\left(i\left(k_x x+k_y y\right)\right)dxdy\right\}exp\left(-i\left(k_x x+k_y y+k_z z\right)\right)dk_x dk_y\right], \end{cases} \tag{23}$$

де $\vec{E}_{xD}$ – поле, розсіяне розкривом опромінювача колової поляризації для x складових;

$\vec{E}_{yD}$ – поле, розсіяне розкривом опромінювача колової поляризації для y складових;

S_p – поверхня інтегрування розкриву опромінювача з внутрішньої сторони;

$\vec{e}_p$ – одиничний вектор напруженості електромагнітного поля;

$\vec{C}_{-mn}^{H,E}$ – амплітуди плоских хвиль, що збуджуються на розкриві;

k_x, k_y, k_z – проекції хвильового вектора на осі x, y, z.

$E_{xF\tau}(z=0)$ або $E_{xF\tau}(z=0)$ – вектори напруженості поля після врахування граничних умов і доповнення інтегрування до нескінченних меж поза поверхнею;

$\vec{\varsigma}_{yx}$ – коефіцієнт відбиття від внутрішніх неоднорідностей опромінювача колової поляризації для y складових;

$\vec{\varsigma}_{xx}$ – коефіцієнт відбиття від внутрішніх неоднорідностей опромінювача колової поляризації для x складових.

Магнітні складові розсіяного поля можна отримати з рівнянь Максвелла.

Якщо площина поляризації хвилі, що падає, збігається з площиною її падіння у площинах $\varphi=\pi$ та $\varphi=3\pi/2$ (рис. 5, 6), то вирази розсіяного поля можуть бути отримані для складових *x* із таких формул:

$$E^{||}_{Fx|_{\varphi=\pi}} \approx \frac{cos\,\theta_f}{\lambda r} e^{-i\left(kr-\pi/2\right)} \left\{ \sum_{m=0}^{\infty}\sum_{n=1}^{\infty} A^{mn}_{x1}\left(k_x=-k\,sin\,\theta\right) A^{mn}_{x2}\left(k_y=0\right) + \right.$$
$$\left. + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} A^{mn}_{x3}\left(k_x=-k\,sin\,\theta\right) A^{mn}_{x4}\left(k_y=0\right) + A^{mn}_{x5}\left(k_x=-k\,sin\,\theta\right) A^{mn}_{x6}\left(k_y=0\right) \right\}, \tag{24}$$

$$E^{||}_{Fx|_{\varphi=3\pi/2}} \approx \frac{cos\,\theta_f}{\lambda r} e^{-i\left(kr-\pi/2\right)} \left\{ \sum_{m=0}^{\infty}\sum_{n=1}^{\infty} A^{mn}_{x1}\left(k_x=0\right) A^{mn}_{x2}\left(k_y=-k\,sin\,\theta\right) + \right.$$
$$\left. + \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} A^{mn}_{x3}\left(k_x=0\right) A^{mn}_{x4}\left(k_y=-k\,sin\,\theta_f\right) + A^{mn}_{x5}\left(k_x=0\right) A^{mn}_{x6}\left(k_y=-k\,sin\,\theta_f\right) \right\}, \tag{25}$$

де вирази для $A^{mn}_{x1}(k_x)$, $A^{mn}_{x2}(k_x)$, $A^{mn}_{x3}(k_x)$, $A^{mn}_{x4}(k_x)$, $A^{mn}_{x5}(k_x)$, $A^{mn}_{x6}(k_x)$ визначаються такий спосіб:

$$A^{mn}_{x1}(k_x) = \frac{-4 f_{+m}(k_x)}{\left(\frac{m\pi}{b_p}\right)^2 - k_x^2} k_x \left(\frac{n\pi}{a_p}\right)^2 C^{H||}_{-mn}\left(1+\rho^{H}_{-mn}\right), \tag{26}$$

$$A^{mn}_{x2}(k_y) = \frac{f_{+n}(k_y)}{\left(\frac{n\pi}{a_p}\right)^2 - k_y^2}, \tag{27}$$

$$A^{mn}_{x3}(k_x) = \frac{4 k_{x k_{zmn}} f_{+m}(k_x)}{\left(\frac{m\pi}{b_p}\right)^2 - k_x^2} \left(\frac{n\pi}{a_p}\right)\left(\frac{m\pi}{b_p}\right) C^{E||}_{-mn}\left(1+\rho^{E}_{-mn}\right), \tag{28}$$

$$A^{mn}_{x4}(k_y) = \frac{f_{+n}(k_y)}{\left(\frac{n\pi}{a_p}\right)^2 - k_y^2}, \tag{29}$$

$$A_{x5}^{mn}\left(k_x\right)=-E_0\cos\theta_f a_p b_p \sin\left(\frac{b_p}{2}\left(k_x-k\sin\theta_{II}\right)\right)\frac{1}{\frac{b_p}{2}\left(k_x-k\sin\theta_f\right)}, \tag{30}$$

$$A_{x6}^{mn}\left(k_y\right)=\sin\left(\frac{a_p}{2}k_y\right)\frac{1}{\frac{a_p}{2}k_y}, \tag{31}$$

$$\left.\begin{aligned} f_{+m}\left(k_x\right)&=\cos^2\left(\frac{m\pi}{2}\right)\sin\left(\frac{k_x b_p}{2}\right)+i\sin^2\left(\frac{m\pi}{2}\right)\cos\left(\frac{k_x b_p}{2}\right)\\ f_{+n}\left(k_y\right)&=\sin^2\left(\frac{n\pi}{2}\right)\cos\left(\frac{k_y a_p}{2}\right)+i\cos^2\left(\frac{n\pi}{2}\right)\sin\left(\frac{k_y a_p}{2}\right)\end{aligned}\right\}. \tag{32}$$

Для випадку нормальної поляризації хвилі до площини падіння вирази для розсіяного поля можуть бути отримані для складових *x* із таких формул:

$$\begin{aligned}\vec{E}_{xPp\tau}^{\perp}=&-\frac{1}{4\pi^2}\int_{-\infty}^{\infty}\frac{b_p\sin\left(\frac{k_x b_p}{2}\right)}{\frac{k_x b_p}{2}}\left(k_x\right)exp\left(-ik_x r\sin\theta\cos\varphi\right)dk_x\times\\ &\times\int_{-\infty}^{\infty}2\sum_{n=1}^{\infty}-C_{+0n}^{H\perp}(1+\vec{\varsigma}_{xx})\cdot\frac{\sin^2\left(\frac{n\pi}{2}\right)\cos\left(\frac{k_y a_p}{2}\right)-i\cos^2\left(\frac{n\pi}{2}\right)\sin\left(\frac{k_y a_p}{2}\right)}{\left(\frac{n\pi}{a_p}\right)^2-\left(k_y\right)^2}+\\ &+E_0 a_p\frac{\sin\left(\frac{a_p}{2}\left(k_y-k\sin\theta_f\right)\right)}{\frac{a_p}{2}\left(k_y-k\sin\theta_f\right)}\Bigg\}exp\left(-irk_x\left(\sin\theta\cos\varphi\right)\right)dk_x;\end{aligned} \tag{33}$$

$$\begin{aligned}\vec{E}_{yPp\tau}^{\perp}=&-\frac{1}{4\pi^2}\int_{-\infty}^{\infty}2\sum_{n=1}^{\infty}-C_{+m0}^{H\perp}(1+\vec{\varsigma}_{yx})\cdot\frac{\sin^2\left(\frac{n\pi}{2}\right)\cos\left(\frac{k_y a_p}{2}\right)-i\cos^2\left(\frac{n\pi}{2}\right)\sin\left(\frac{k_y a_p}{2}\right)}{\left(\frac{n\pi}{a_p}\right)^2-\left(k_y\right)^2}+\\ &+E_0 a_p\frac{\sin\left(\frac{a_p}{2}\left(k_y-k\sin\theta_f\right)\right)}{\frac{a_p}{2}\left(k_y-k\sin\theta_f\right)}\Bigg\}exp\left(-irk_x\left(\sin\theta\cos\varphi\right)\right)dk_x.\end{aligned} \tag{34}$$

Метод проєктування передбачає, що для опромінювача, який приймає і випромінює хвилі колової поляризації, дві складові розсіяного ним поля у площині $\varphi=3\pi/2$ матимуть такий вигляд:

$$\begin{cases} \vec{E}^{\perp}_{x_{P\tau|\varphi=\frac{3\pi}{2}}} \approx \dfrac{k\cos\theta_f}{2\pi r} exp\left(-i\left(kr-\dfrac{\pi}{2}\right)\right)\times \\ \times 2\sum\limits_{n=1}^{\infty}\dot{C}_{m0}\left(1+\dot{\varsigma}_{-xx}\right)\dfrac{sin^2\left(\dfrac{n\pi}{2}\right)cos\left(\dfrac{ka}{2}sin\theta_f\right)+i\,cos^2\left(\dfrac{n\pi}{2}\right)sin\left(\dfrac{ka}{2}sin\theta_f\right)}{1-\left(\dfrac{\left(ka\cdot sin\theta_f\right)}{n\pi}\right)^2}; \\ \vec{E}^{\perp}_{y_{P\tau|\varphi=\frac{3\pi}{2}}} \approx \dfrac{k\cos\theta_f}{2\pi r} exp\left(-i\left(kr-\dfrac{\pi}{2}\right)\right)\times \\ \times 2\sum\limits_{n=1}^{\infty}\dot{C}_{0n}\left(1+\dot{\varsigma}_{-yx}\right)\dfrac{sin^2\left(\dfrac{n\pi}{2}\right)cos\left(\dfrac{ka}{2}sin\theta_f\right)+i\,cos^2\left(\dfrac{n\pi}{2}\right)sin\left(\dfrac{ka}{2}sin\theta_f\right)}{1-\left(\dfrac{\left(ka\cdot sin\theta_f\right)}{n\pi}\right)^2}; \end{cases} \tag{35}$$

$$\begin{cases} \vec{E}^{\perp}_{x\,P\tau|\varphi=\pi} \approx -\dfrac{bk\cos\theta_f}{2\pi r} exp\left(-i\left(kr-\dfrac{\pi}{2}\right)\right)\dfrac{sin\left(\dfrac{kb}{2}sin\theta_f\right)}{\dfrac{kb}{2}sin\theta_f}2\sum\limits_{n=1}^{\infty}\dot{C}_{0n}\left(1+\dot{\varsigma}_{-xx}\right)sin^2\left(\dfrac{n\pi}{2}\right); \\ \vec{E}^{\perp}_{y\,P\tau|\varphi=\pi} \approx -\dfrac{bk\cos\theta_f}{2\pi r} exp\left(-i\left(kr-\dfrac{\pi}{2}\right)\right)\dfrac{sin\left(\dfrac{kb}{2}sin\theta_f\right)}{\dfrac{kb}{2}sin\theta_f}2\sum\limits_{n=1}^{\infty}\dot{C}_{m0}\left(1+\dot{\varsigma}_{-yx}\right)sin^2\left(\dfrac{n\pi}{2}\right). \end{cases} \tag{36}$$

Коефіцієнти $\dot{\varsigma}_{xx}$ та $\dot{\varsigma}_{yx}$ визначено в [5] шляхом розв'язання внутрішньої задачі.

Висновки. У статті вирішено завдання визначення електромагнітного поля, розсіяного від рупорного опромінювача, розміщеного в площині фокуса параболоїда обертання, у разі довільного падіння на нього плоскої електромагнітної хвилі на прикладі антенних систем станцій наземної розвідки типу ПСНР "Кредо" (1РЛ133).

Поставлене завдання має дві складові: визначення електромагнітного поля в площині фокуса параболоїда обертання в разі довільного падіння на нього плоскої електромагнітної хвилі та знаходження електромагнітного поля, розсіяного від рупорного опромінювача колової поляризації, розміщеного в площині фокуса параболоїда обертання за умови довільного падіння на нього плоскої електромагнітної хвилі.

Надані в статті матеріали та отримані автором раніше результати об'єднує умова довільного падіння електромагнітної хвилі, що є суперпозицією двох окремих випадків. Розрахунки за новим методом дозволять оцінювати вплив різноманітних елементів, розміщених у площині фокуса, на розсіювання антенних систем у цілому за будь-яких умов падіння хвилі на дзеркало.

Побудова РЛС на основі розрахованої за новим методом параболічної антени дозволить отримати значні переваги над традиційними однополяризаційними РЛС у разі виявлення об'єктів з малою ЕПР і виділення їх інформативних ознак, а також підвищить якість виявлення цілей на фоні пасивних (метеоутворення, рослинність тощо) і активних перешкод.

Детальний виклад матеріалу дозволяє в ході проєктування на кожному етапі розрахунку провести моделювання для з'ясування можливості підвищити розрізнювальну здатність антенних систем станцій наземної розвідки та зберегти або навіть покращити характеристики їх електромагнітної сумісності та розвідзахищеності.

СПИСОК ЛІТЕРАТУРИ

1. Сидорчук О. Л. Аналіз методів і способів зменшення ефективної поверхні розсіювання антенних систем // Вісник ЖДТУ. Технічні науки. Житомир, 2012. № 2 (61). С. 94–106.
2. Зайцев Н. А., Платов А. В., Потапов В. А. Радиолокационные станции разведки наземных движущихся целей. Современный уровень и основные направления развития // Вестник Концерна ПВО «Алмаз–Антей». 2014. № 1.С. 41–44.
3. Гладышев А. К., Иванкин Е. Ф., Панычев С. Н. Влияние характеристик рассеяния на показатели качества функционирования РЭС // Измерительная техника. 1995. № 2. С. 48–50.
4. Изделие 1РЛ133. Техническое описание. БД 1.400.009 ТО. 1974. 232 с.
5. 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. Житомир : ЖВІ, 2018. Вип. 15, С. 78–93.
6. 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.
7. Sidorchuk O., Tofanchuk O., Kritenko O., Kalenchuk Yu. Methodology improvment of the electromagnetic field amplitude study related to the antenna system risk radio-solid station of land-development "Credo-M1" // Scientific works of Kharkiv National Air Force University. 2017. № 5 (54). С. 102–109.
8. Вуд П. Анализ и проектирование зеркальных антенн / Пер. с англ. под ред. О. П. Фролова. Москва : Радио и связь, 1984. 208 с.
9. Петров Б. М., Юханов Ю. Б. Рассеяние плоской электромагнитной волны на импедансном цилиндре в присутствии большого рефлектора // Рассеяние электромагнитных волн. Таганрог: ТРТИ, 1981. Вып. 3. С. 127.
10. Алашеева Е. А., Блатов И. А., Маслов М. Ю. Решение задачи об излучении линейной структуры, расположенной вблизи идеально проводящего экрана, сводимой к двумерной системе уравнений Фредгольма первого рода // Вестник СамГУ. Естественная серия. Самара, 2010. № 2 (76) С. 43–49.
11. Астахов В. Н. Дифракция на проводящем шаре в поле параболоида антенны // Изв. ЛЭТИ. Научн. труды. 1974. Вып. 155. С. 25–31
12. 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.
13. Астахов В. Н., Степанов В. А. Определение дифракционного поля в области фокуса параболоида вращения // Изв. ЛЭТИ. Научн. труды. 1979. Вып. 245. С. 25–30.
14. Уфимцев П. Я. Основы физической теории дифракции. Москва : Бином, 2009. 352 с.
15.Сидорчук О. Л. Дослідження амплітуд електромагнітного поля, збудженого лінійною решіткою рупорних опромінювачів // Вісник Нац. техн. ун-ту України «КПІ». Серія «Радіотехніка. Радіоапаратобудування». Київ, 2016. № 64. С. 49–58.

Подано 01.04.2019

О. Л. Сидорчук

МЕТОД ОПРЕДЕЛЕНИЯ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ, РАССЕЯННОГО РУПОРНЫМ ОБЛУЧАТЕЛЕМ, КОТОРЫЙ РАЗМЕЩЕН В ФОКУСЕ ПАРАБОЛОИДА ВРАЩЕНИЯ АНТЕННОЙ СИСТЕМЫ СТАНЦИЙ НАЗЕМНОЙ РАЗВЕДКИ

В статье предлагается усовершенствованный математический аппарат для исследования амплитуд электромагнитного поля, рассеянного антенной системой с рупорным облучателем пирамидальной формы, который расположен в фокусе параболоида вращения на примере станций наземной разведки типа ПСНР «Кредо» (1РЛ133).

Усовершенствование аппарата заключается в применении нового метода определения рассеянного электромагнитного поля, переизлученного облучателем, расположенным в фокусе параболоида вращения антенной системы, при нормальной поляризации падающей плоской волны в плоскости ее падения, а также совпадении поляризации волны и плоскости ее падения как суперпозиции произвольного падения.

Поставленная задача включает две составляющие: определение электромагнитного поля в плоскости фокуса параболоида вращения при произвольном падении на него плоской электромагнитной волны и электромагнитного поля, рассеянного от рупорного облучателя круговой поляризации, расположенного в плоскости фокуса параболоида вращения при произвольном падении на него плоской электромагнитной волны.

Предоставленные в статье и полученные автором ранее материалы объединяет случай произвольного падения электромагнитной волны, что является суперпозицией двух случаев: волна поляризована нормально к плоскости падения; совпадения поляризации волны и плоскости ее падения. Расчеты по новому методу позволят оценивать влияние различных элементов, размещенных в плоскости фокуса, на рассеяние антенных систем в целом при любом случае падения волны на зеркало.

Построение радиолокационных станций на основе рассчитанной по новому методу параболической антенны позволит получить значительные преимущества над традиционными однополяризационными радиолокационными станциями при обнаружении объектов с малой эффективной поверхностью рассеивания и выделять их информационные признаки.

Ключевые слова: *параболоид вращения; зеркальная антенна; малогабаритный рупорный облучатель; улучшение поляризационных характеристик; дифракция электромагнитной волны; уменьшение эффективной поверхности рассеивания.*

O. L. Sidorchuk

METHOD FOR DETERMINING AN ELECTROMAGNETIC FIELD, SCATTERED BY A HORSE IRRADIATOR, PLACED IN THE FOCUS OF THE PARABOLOID ROTATION OF AN ANTENNA SYSTEM OF THE GROUND-DEPENDENT STATIONS

The article proposes an improved mathematical apparatus for studying the amplitudes of the electromagnetic field scattered by an antenna system with a horn feed of pyramidal shape, which is located at the focus of the paraboloid of rotation using the Credo-type ground-based intelligence stations (1RL133).

Improvement of the apparatus consists in applying a new method for determining the scattered electromagnetic field reemitted by the irradiator located at the focus of the paraboloid of rotation of the antenna system during normal polarization of the incident plane wave in its plane of incidence, as well as coincidence of the wave and its plane of incidence as a superposition of an arbitrary incidence.

The task includes two components: determination of the electromagnetic field in the plane of the focus of the paraboloid of rotation with an arbitrary plane electromagnetic wave falling on it and finding the electromagnetic field scattered from the circular polarization horn feed of the polarized paraboloid with an arbitrary plane electromagnetic wave falling on it.

The materials presented in the article and previously received by the author combine the case of an arbitrary fall of an electromagnetic wave, which is a superposition of two cases: the wave is polarized normally to the plane of incidence; coincidence of the polarization of the wave and the plane of its fall. Calculations using the new method will allow evaluating the effect of various elements placed in the plane of focus on the scattering of antenna systems as a whole in any case of a wave falling on a mirror.

The construction of radar stations based on a parabolic antenna calculated using a new method will allow one to gain significant advantages over traditional single-polarization radar stations when detecting objects with a small effective dispersion surface and to highlight their information signs.

Keywords: *paraboloid of rotation; mirror antenna; small-sized horn feed; improvement of polarization characteristics; diffraction of an electromagnetic wave; reduction of the effective dispersion surface.*

ISSN 2076-1546

УДК 629. 7.062.2 DOI: 10.46972/2076-1546.2019.16.09

П. В. Фриз

СПОСІБ ВИБОРУ ДОСТУПНИХ КОСМІЧНИХ АПАРАТІВ ЗА УМОВАМИ ГЕОМЕТРИЧНОЇ ВИДИМОСТІ МІЖ НИМИ ТА ЗАДАНИМ РАЙОНОМ ЗЕМЛІ

В умовах бойових дій на сході України особливої актуальності набуває проблема забезпечення військового керівництва інформацією космічного знімання. З огляду на відсутність вітчизняних засобів для вирішення цих завдань, можливим практичним шляхом отримання інформації космічного знімання є її замовлення та придбання в закордонних операторів. Слід зауважити, що ринок цих послуг достатньо розвинутий, тому постає проблема коректного формування замовлень на знімання.

У статті запропоновано оригінальний спосіб вибору доступних іноземних космічних апаратів дистанційного зондування Землі для використання їх цільової інформації в інтересах Збройних Сил України. Він базується на завчасних розрахунках очікуваних коефіцієнтів часового та просторового накриття заданих районів Землі зоною огляду визначених космічних апаратів, порівнянні їх з вимогами замовників цільової інформації та виборі на цій основі найбільш придатних варіантів.

Формалізовано умови видимості заданого району Землі визначеним космічним апаратом у задану календарну дату. При цьому використано апарат логічних функцій геометричної видимості. Крім того, запропоновано математичний апарат для розрахунку площі заданого району знімання в разі її опису багатокутником довільної форми з урахуванням ексцесу цього сферичного багатокутника. Розроблено математичну модель визначення миттєвої площі знімання на сферичній Землі пірамідальною зоною огляду космічного апарата за відхилень візирної осі бортової цільової апаратури за креном.

Запропоновано напрямки подальших досліджень, зокрема визначення фізичних умов спостереження заданих районів знімання.

Ключові слова: *доступні космічні апарати; оптико-електронні спостереження; проекція поля зору; часовий та просторовий коефіцієнти накриття; заданий район Землі; знята сцена; бортова знімальна апаратура.*

Постановка проблеми в загальному вигляді. На нинішньому етапі гостро стоїть проблема всебічного інформаційно-розвідувального забезпечення діяльності Збройних Сил (ЗС) в умовах бойових дій на сході України [1]. При цьому одним із важливих джерел розвідувальної інформації для ЗС є космічні засоби. У нашій державі на сьогодні добре розвинута лише їх наземна інфраструктура, а орбітальні засоби відсутні. Тому відповідно до керівних документів [2, 3] для національних потреб у космічній інформації акцент робиться на використанні цільової інформації (ЦІ) від доступних іноземних космічних апаратів (КА) спостереження, зокрема КА дистанційного зондування Землі (ДЗЗ). Але оскільки ринок космічних інформаційних послуг достатньо об'ємний, то постає проблема раціонального вибору закордонних космічних систем, найбільш придатних для задоволення тих чи інших потреб вітчизняних замовників, у тому числі й ЗС України, з подальшим плануванням їх цільового застосування.

Аналіз останніх досліджень і публікацій. Завдання планування космічних спостережень останнім часом у тій чи іншій мірі розглядалося низкою закордонних [4–8] та вітчизняних авторів [9–11]. Але в цих публікаціях досліджуються здебільшого власні орбітальні групування, коли не стоїть проблема вибору придатних КА з-поміж доступних іноземних. Так, статті [4–7] стосуються розподілу завдань між власними супутниками на основі механізму об'єднання завдань [4], стратегії руху горизонту [5], динамічного планування в режимі реального часу [6], мультиагентного гібридного навчання [7], а в роботі [8] досліджується процес планування тільки передачі ЦІ на власні наземні засоби.

Статті вітчизняних авторів присвячені раціональному плануванню космічного знімання Землі на основі багатокритерійної оптимізації [9], плануванню роботи бортових систем КА з метою використання координатних методів [10], оптимізації обслуговування заявок на отримання ЦІ з КА ДЗЗ [11]. Але в жодній із цитованих публікацій не розглядається процес вибору КА як передмова для планування їх застосування.

В авторських статтях [12–14] наведено здебільшого оригінальний математичний апарат розрахунків параметрів землеогляду, який використовується далі, але вони не розкривають критеріїв прийняття відповідних рішень.

Найбільш повно проблему вибору КА розкрито в роботі [15], у якій запропоновано алгоритм автоматизованого вибору релевантних (придатних за багатьма показниками) КА для оптико-електронного спостереження (ОЕСп) Землі, але в ній не вистачає математичного апарату для розрахунків умов геометричної видимості між КА і заданим районом та правил прийняття раціональних рішень.

Тому **мета статті** полягає в розробці способу вибору доступних іноземних КА ДЗЗ за умовами геометричної видимості між ними та заданим районом Землі (РЗ) для планування їх цільового застосування в інтересах інформаційного забезпечення діяльності ЗС України.

Виклад основного матеріалу. Нехай в орбітальному польоті знаходиться множина доступних КА $\{K_\mu\}$, $\mu = \overline{1,\mathrm{M}}$, $\mathrm{M} \geq 1$, ОЕСп Землі. Відома множина районів на земній поверхні $\{P_m\}$, $m = \overline{1,M}$, $M \geq 1$, яка підлягає космічному моніторингу. У замовників цільової інформації є необхідність отримати якісні космічні знімки з m-го РЗ у певний час доби й року.

Відомо, що для організації космічних ОЕСп необхідно забезпечити *геометричну видимість* між КА і заданим РЗ m, коли на прямій лінії між ними відсутні інші об’єкти, наприклад, частина земної поверхні. А це означає, що потрібно забезпечити повне або часткове геометричне накриття m-го РЗ *смугою огляду* бортової знімальної апаратури (БЗА). При цьому необхідними ознаками накриття можуть бути такі часткові події:

а) перетин *центра* m-го РЗ *трасою КА*;

б) перетин *центра* m-го РЗ *трасою візирної осі* БЗА;

в) перетин *меж* m-го РЗ *трасою КА*;

г) перетин *меж* m-го РЗ *трасою візирної осі* БЗА;

д) повне або часткове *накриття* m-го РЗ *смугою огляду* БЗА;

е) повне або часткове *накриття* m-го РЗ *смугою захоплення* КА тощо.

Такий самий підхід можна застосовувати для планування моментів спостережень за заданими об'єктами в межах заданого району.

Множину можливих ситуацій у ході планування космічних спостережень за заданим РЗ із використанням БЗА оптико-електронного типу наведено в табл. 1.

Таблиця 1

Можливі ситуації в ході планування ОЕСп за заданим РЗ

Параметри РЗ	Атрибути землеогляду КА			
	Траса КА	Траса візирної осі	Смуга огляду	Смуга захоплення
Центр району	0	0	+	++
Заданий об'єкт	0	0	+	++
Межі району	+	+	++	+++
Задана ділянка	+	+	++	+++
Весь район	++	++	+++	++++

Примітка. У табл. 1 цифра 0 означає дуже малу ймовірність події (близьку до нуля), знаки: + − малу ймовірність; ++ − середню ймовірність; +++ − імовірність, вищу середньої; ++++ − високу ймовірність; ++++ − дуже високу ймовірність (близьку до одиниці).

У формалізованому вигляді наявність або відсутність умов видимості m-го РЗ з μ-го КА в задану дату $d \in d^з$ космічного знімання визначимо за допомогою логічної функції геометричної видимості:

$$\Phi_m^{\Gamma}(\mu) = \begin{cases} 1, if \left(K_m^{\tau}(\mu) \geq \overline{K}_m^{\tau}\right) \wedge \left(K_m^{S}(\mu) \geq \overline{K}_m^{S}\right) = 1; \\ 0, if \left(K_m^{\tau}(\mu) \geq \overline{K}_m^{\tau}\right) \wedge \left(K_m^{S}(\mu) \geq \overline{K}_m^{S}\right) = 0, \end{cases} \quad (1)$$

де $K_m^{\tau}(\mu)$ − часовий коефіцієнт накриття m-го РЗ смугою огляду μ-го КА, який повинен бути не менше допустимого $\overline{K}_m^{\tau}$;

$K_m^{S}(\mu)$ – просторовий коефіцієнт накриття m-го РЗ смугою огляду μ-го КА, який повинен бути не менше допустимого $\overline{K}_m^{S}$.

Умови часового накриття m-го РЗ μ-м КА можна подати логічною функцією (рис. 1)

$$\left[\tau_m(\mu) \in \overline{\tau}_m\right] \wedge \left[\tau_m(\mu) \geq \overline{\tau}_m\right] = 1, \quad (2)$$

де

$$\tau_m(\mu) = t_m^{\kappa}(\mu) - t_m^{n}(\mu) \quad (3)$$

− тривалість *очікуваного* інтервалу знімання КА μ;

$$\overline{\tau}_m = \overline{t}_m^{\kappa} - \overline{t}_m^{n} \quad (4)$$

− тривалість *заданого* інтервалу знімання;

$t_m^{\kappa}(\mu)$, $\overline{t}_m^{\kappa}$ − очікуваний та заданий моменти *закінчення* знімання;

$t_m^n(\mu)$, $\bar{t}_m^n$ – очікуваний та заданий моменти *початку* знімання.

Методику розрахунків очікуваних моментів часу буде розроблено в подальшому.

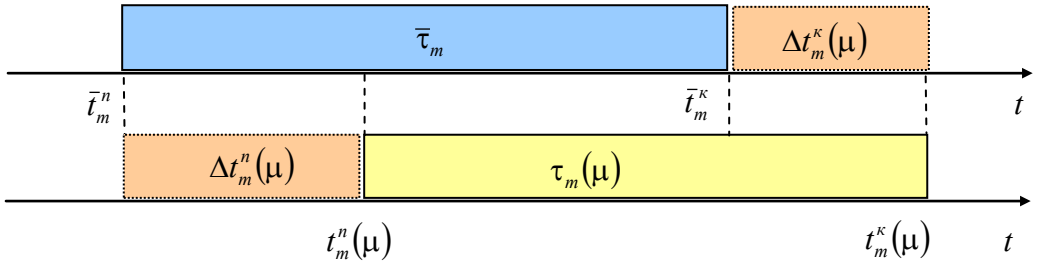


Рис. 1. До положення та тривалості очікуваного та заданого інтервалів знімання

Тоді *часовий коефіцієнт накриття* можна знайти як відношення очікуваного часового інтервалу космічного знімання m-го РЗ μ-м КА $\tau_m(\mu)$ до заданого часу геометричної видимості цього району $\bar{\tau}_m$, прагнучи до його максимізації, тобто

$$K_m^\tau(\mu) = \tau_m(\mu)/\bar{\tau}_m, \; K_m^\tau(\mu) \to max. \tag{5}$$

Від коефіцієнта (5) можна перейти до його нормованих значень за правилом

$$\hat{K}_m^\tau(\mu) = \begin{cases} \tau_m(\mu)/\bar{\tau}_m, if \; \tau_m(\mu) < \bar{\tau}_m; \\ 1, if \; \tau_m(\mu) \geq \bar{\tau}_m. \end{cases} \tag{6}$$

У такому разі коефіцієнт (6) може набувати значень із діапазону

$$0 \leq \hat{K}_m^\tau(\mu) \leq 1. \tag{7}$$

При цьому слід прагнути до забезпечення умови

$$\hat{K}_m^\tau(\mu) \to 1, \tag{8}$$

а вибір придатних КА здійснювати за найбільшими значеннями коефіцієнта (7) із упорядкованої множини його очікуваних значень

$$\hat{K}_m^\tau(1) > \hat{K}_m^\tau(2) > \ldots > \hat{K}_m^\tau(\mu)\ldots, \; \mu = \overline{1,M}. \tag{9}$$

Вимогу $K_m^\tau(\mu) \to max$ у виразі (5) можна інтерпретувати й по-іншому, наприклад, через вимогу мінімізації часу *ненакриття* m-го РЗ μ-м КА, що можна подати такими аналітичними виразами (див. рис. 1):

$$\Delta t_m^n(\mu) = \left| t_m^n(\mu) - \bar{t}_m^n \right| \to 0; \tag{10}$$

$$\Delta t_m^к(\mu) = \left| t_m^к(\mu) - \bar{t}_m^к \right| \to 0; \tag{11}$$

$$\Delta t_m^{\Sigma}(\mu) = \Delta t_m^{n}(\mu) + \Delta t_m^{\kappa}(\mu) \to 0. \tag{12}$$

У такому разі замість (5) слід користуватися протилежним показником – *часовим коефіцієнтом ненакриття* m-го РЗ:

$$K_m^{\Delta t}(\mu) = 1 - K_m^{\tau}(\mu) = \Delta t_m^{\Sigma}(\mu)/\bar{\tau}_m,\ K_m^{\Delta t}(\mu) \to min. \tag{13}$$

Виконання вимог (10)–(13) забезпечує *своєчасність* ОЕСп, економію бортових ресурсів та запобігання отриманню надлишкової ЦІ. У разі невиконання цих вимог визначеними КА слід перевірити на придатність інші апарати та витки орбіти, а також можливість здійснення кутових маневрів вибраних зразків.

Просторовий коефіцієнт накриття $K_m^S(\mu)$ у виразі (1) можна знайти як відношення площі $S_m^*(\mu)$ спостережуваної ділянки m-го РЗ μ-м КА до загальної площі цього району S_m^* (рис. 2), прагнучи до його максимізації, тобто

$$K_m^S(\mu) = S_m^*(\mu)/S_m^*,\ K_m^S(\mu) \to max, \tag{14}$$

де правий верхній індекс $*$ відведений для позначення форми відповідних атрибутів землеогляду – спостережуваної ділянки, усього РЗ тощо.

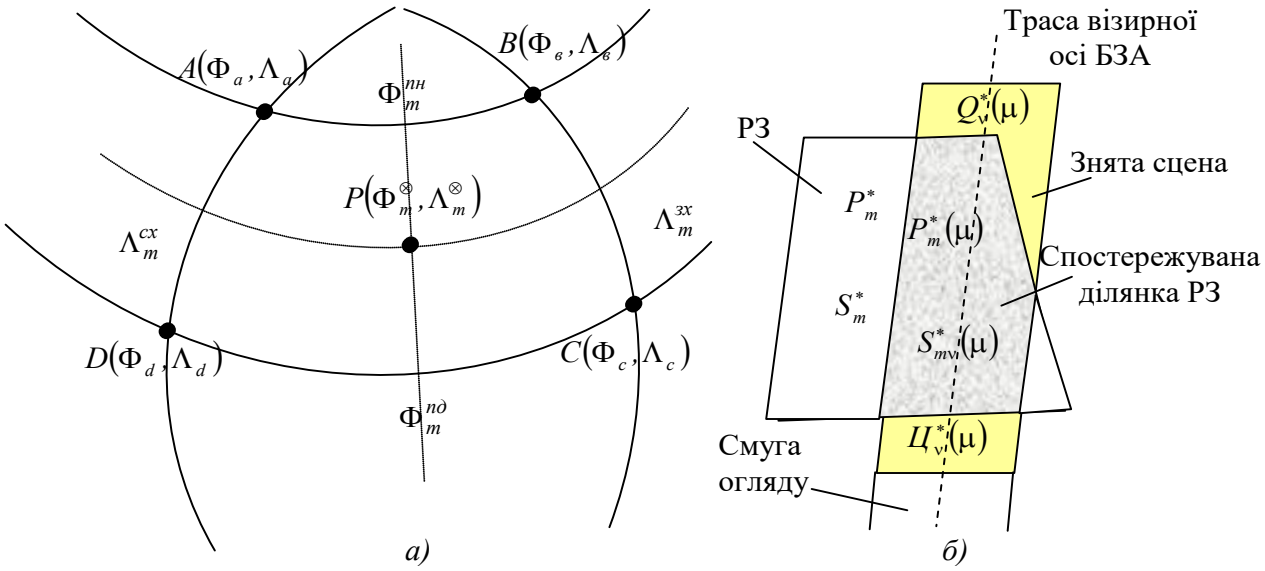


Рис. 2. До поняття просторового коефіцієнта накриття РЗ

Для зручності та з метою запобігання надлишковості від коефіцієнта (14) можна перейти до його нормованих значень

$$\widehat{K}_m^S(\mu) = \begin{cases} S_m(\mu)/S_m, if\ S_m(\mu) < S_m; \\ 1, if\ S_m(\mu) \geq S_m. \end{cases} \tag{15}$$

У такому разі коефіцієнт (15) може набувати значень із діапазону

$$0 \le \widehat{K}_m^S(\mu) \le 1. \tag{16}$$

При цьому слід прагнути до забезпечення умови

$$\widehat{K}_m^S(\mu) \to 1, \tag{17}$$

а вибір придатних КА здійснювати за найбільшими значеннями коефіцієнтів (15) із упорядкованої множини його очікуваних значень

$$\widehat{K}_m^S(1) > \widehat{K}_m^S(2) > ... > \widehat{K}_m^S(\mu)..., \ \mu = \overline{1,\mathrm{M}}. \tag{18}$$

Виконання вимог (10)−(13) забезпечує *своєчасність* ОЕСп, економію бортових ресурсів та запобігання отриманню надлишкової ЦІ. У разі невиконання цих вимог визначеними КА слід перевірити на придатність інші апарати та витки орбіти, а також можливість здійснення кутових маневрів вибраних варіантів.

Для розрахунків ***площі заданого РЗ*** S_m^* у виразі (14) можна скористатися таким підходом [13, 14]. Нехай РЗ має форму сферичної трапеції $ABCD$, сторонами якої є паралелі та меридіани (див. рис. 2). Тоді формально це можна подати як

$$P_m^{\Diamond} = P\left(\Phi_m^{пн}, \Phi_m^{пд}, \Lambda_m^{сх}, \Lambda_m^{зх}\right), \tag{19}$$

де $\Phi_m^{пн}, \Phi_m^{пд}, \Lambda_m^{сх}, \Lambda_m^{зх}$ – географічні межі m-го РЗ (північна та південна широта, східна та західна довгота відповідно).

На практиці в цьому випадку часто обмежуються заданням РЗ через координати тільки двох вершин сферичної трапеції, наприклад, північно-західної $A\left(\Phi_m^{пн}, \Lambda_m^{зх}\right)$ та південно-східної $C\left(\Phi_m^{пд}, \Lambda_m^{сх}\right)$.

Площу такого РЗ можна обчислити за географічними координатами його вершин [14]:

$$S_m^{\Diamond}\left(\Phi_m, \Lambda_m\right) = R_з^2\left(\Lambda_m^{сх} - \Lambda_m^{зх}\right)\left(sin\,\Phi_m^{пн} - sin\,\Phi_m^{пд}\right), \tag{20}$$

де Φ_*^* та Λ_*^* – географічні широта й довгота сторін трапеції в радіанах.

Якщо РЗ має форму багатокутника, то його називають полігоном [14] і описують як

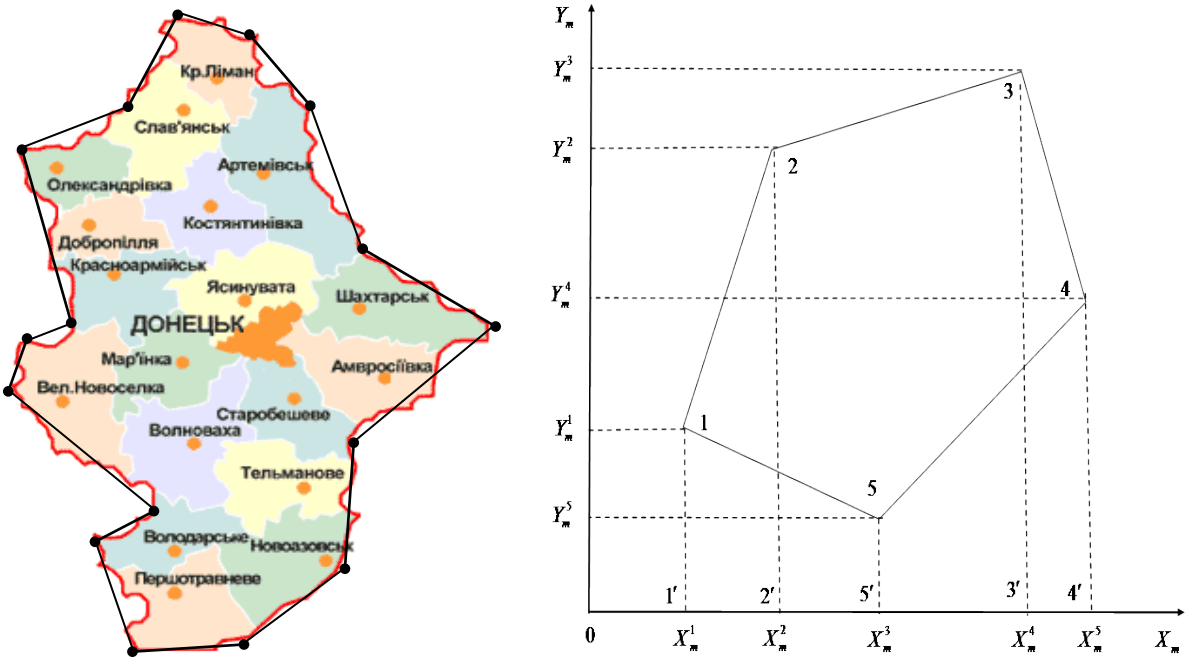
$$P_m^{\Sigma} = P\left[\left(X_m^1, Y_m^1\right), \left(X_m^2, Y_m^2\right), ...\left(X_m^k, Y_m^k\right)\right], \tag{21}$$

де верхніми правими індексами $1, 2, ..., k$ позначені номери вершин багатокутника, а $\left(X_m^k, Y_m^k\right)$ – їх декартові координати.

У разі, коли РЗ має просту форму (коло, трикутник, трапеція тощо) і сферичністю Землі можна нехтувати, то для розрахунку його площі варто скористатися звичайними формулами планіметрії.

Якщо ж РЗ становить собою багатокутник (рис. 3а) довільної форми, то його площу можна знайти через обчислення площ відповідних трапецій [14]. Наприклад, площу

фігури 12345 (рис. 3б) можна обчислити, якщо знайти суму площ трьох "великих" трапецій: 1′122′, 2′233′, 3′344′, – а потім відняти від неї суму площ двох "зайвих" трапецій: 1′155′ і 5′544′.



а) *б)*

Рис. 3. До розрахунків площі РЗ у вигляді багатокутника

При цьому площа будь-якої з трапецій обчислюється через добуток її основи на висоту, а за висоту беруть середню лінію трапеції. Наприклад, площа першої із "великих" трапецій дорівнює

$$S_m^1 = 0{,}5\left(Y_m^1 + Y_m^2\right)\left(X_m^2 - X_m^1\right). \tag{22}$$

Аналогічно для решти "великих" трапецій 2′233′ і 3′344′

$$S_m^2 = 0{,}5\left(Y_m^2 + Y_m^3\right)\left(X_m^3 - X_m^2\right); \tag{23}$$

$$S_m^3 = 0{,}5\left(Y_m^3 + Y_m^4\right)\left(X_m^4 - X_m^3\right). \tag{24}$$

Таким же чином отримаємо площі "зайвих" трапецій: 1′155′ і 5′544′:

$$S_m^4 = 0{,}5\left(Y_m^1 + Y_m^5\right)\left(X_m^5 - X_m^1\right); \tag{25}$$

$$S_m^5 = 0{,}5\left(Y_m^5 + Y_m^4\right)\left(X_m^4 - X_m^5\right). \tag{26}$$

Тоді площа багатокутника 12345 становитиме:

$$S_m^{\Sigma} = S_m^1 + S_m^2 + S_m^3 - S_m^4 - S_m^5. \tag{27}$$

Якщо у вираз (27) підставити формули (22)–(26), то отримаємо подвійну площу цього багатокутника:

$$2S_m^{\Sigma} = \sum \left[X_m^i \left(Y_m^{i+1} - Y_m^{i-1} \right) \right] \text{ або } 2S_m^{\Sigma} = \sum \left[Y_m^i \left(X_m^{i-1} - X_m^{i+1} \right) \right] . \quad (28)$$

Аналогічно можна обчислювати площі земельних ділянок з іншою кількістю сторін, включаючи трикутники і чотирикутники, якщо відомі декартові координати їх вершин.

У випадках, коли необхідно враховувати сферичність Землі, визначають площу полігона через ексцес сферичного багатокутника за формулою [14]

$$\widehat{S}_{\varepsilon}^{\Sigma} = \varepsilon R_з^2 ,$$

де $\varepsilon = 2\pi - \sum_{i=1}^{I} \gamma_i$ – ексцес, тобто сума зовнішніх кутів сферичного багатокутника, що перевищують 2π (рис. 4);

$\gamma_i = \pi - \theta_i$ – кут, що доповнює румб до π;

$\theta_i = \alpha_{i,i-1} - \alpha_{i,i+1}$ – румб (кут між двома напрямками), причому $\theta_i \le 0{,}5\pi$;

$\alpha_{i,i+1}$ – азимут сторони, спрямованої з i-ї вершини в наступну;

$\alpha_{i,i-1}$ – азимут сторони, спрямованої з i-ї вершини в попередню.

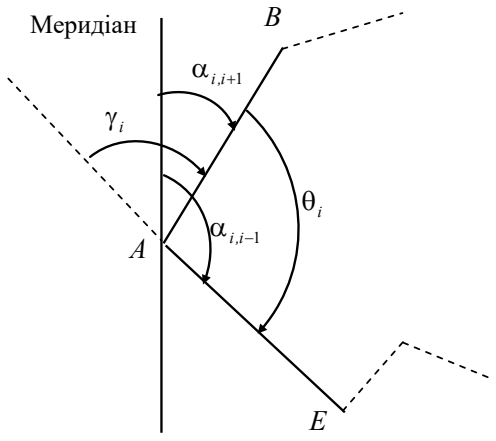


Рис. 4. До вимірювання площі полігона на сферичній Землі

Під *спостережуваною ділянкою* (див. рис. 2б) розумітимемо ту частину РЗ, яка накривається проекцією зони огляду (ПЗО) БЗА μ-го КА за час космічного знімання τ, або, що одне й те ж, смугою огляду БЗА. При цьому, якщо $\tau \approx 0$, то отримаємо *миттєву площу космічного знімання*, яка дорівнює площі ПЗО на земній поверхні $S_{огл}^{*}(\mu)$. Якщо ж $\tau > 0$, то матимемо інтегральну площу – *площу знятої сцени* $S_{огл}^{*}(\mu)$.

Нехай зона огляду μ-го КА є правильною прямокутною пірамідою *KBCFG* (рис. 5а) з кутами при вершині 2α (рис. 5б) і 2β (рис. 5в), візирна вісь БЗА збігається з висотою піраміди *H* і направлена в надир, Земля – *плоска*.

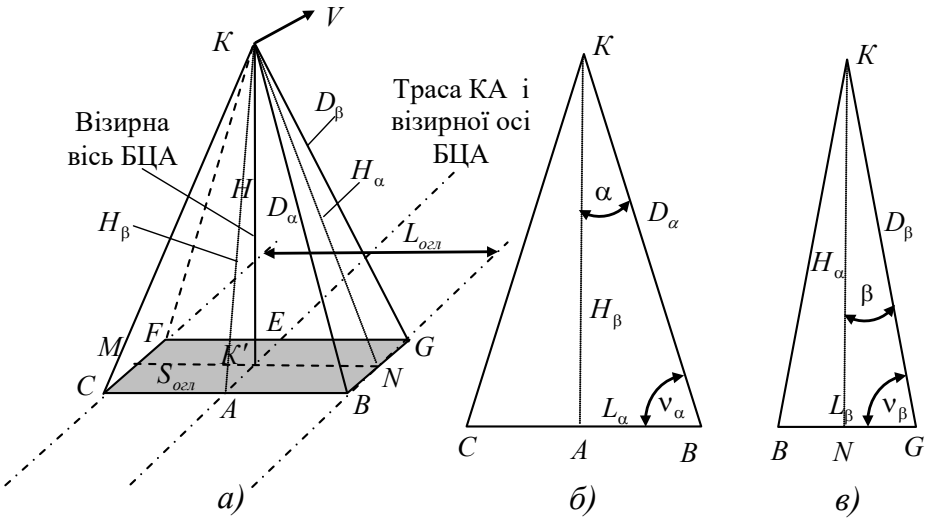


Рис. 5. До ситуації спостережень у надир плоскої Землі пірамідальною зоною огляду КА

У цьому разі площа ПЗО $S^{*}_{огл}$ становить собою площу прямокутника $CFGB$ (рис. 5а), яку можна обчислити як добуток його сторін [12, 14]

$$S^{\perp}_{огл} = CB \cdot BG = 2L_\alpha \cdot 2L_\beta; \tag{29}$$

$$L_\alpha = Htg\alpha / cos\beta; \tag{30}$$

$$L_\beta = Htg\beta / cos\alpha. \tag{31}$$

Підставивши (30) та (31) у вираз (29), отримаємо миттєву площу знімання

$$S^{\perp}_{огл} = 4H^2 tg\alpha tg\beta / cos\alpha cos\beta. \tag{32}$$

Оскільки в реальних умовах кути поля зору БЗА невеликі ($\alpha \le 10^\circ$ і $\beta \le 10^\circ$), то отримані залежності можна застосовувати і для *сферичної* моделі Землі.

Якщо за рахунок кутового маневру КА за креном його зона огляду і візирна вісь БЗА відхилені від надира на кут η (рис. 6а), то ПЗО на поверхні плоскої Землі трансформується в рівнобічну трапецію $C_1B_1G_1F_1$ (рис. 6б).

Тоді площа ПЗО є площею трапеції $C_1F_1G_1B_1$ (див. рис. 6б), яку можна обчислити через середню лінію трапеції та її висоту:

$$S^{\diamond}_{огл}(\eta) = A_1E_1 \cdot M_1N_1. \tag{33}$$

Середню лінію трапеції A_1E_1 визначаємо через півсуму її основ:

$$A_1E_1(\eta) = H\left[sec(\alpha+\eta) + sec(\alpha-\eta)\right] tg\beta. \tag{34}$$

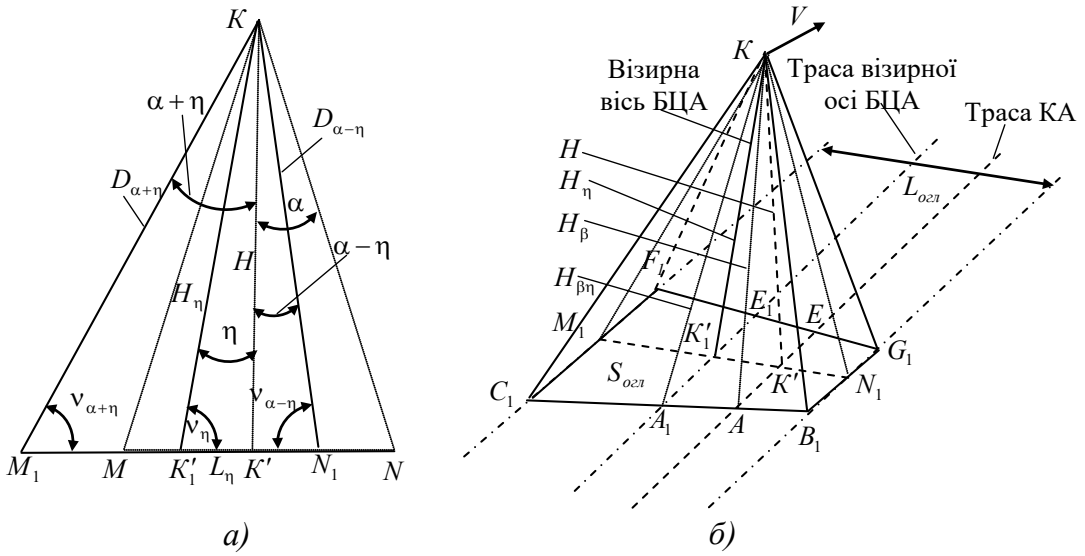


Рис. 6. До ситуації спостережень плоскої Землі пірамідальною зоною огляду КА з відхиленням візирної осі БЗА за креном

Ширину смуги огляду можна знайти через висоту трапеції M_1N_1 (див. рис. 5б) як

$$M_1N_1 = L^{\Diamond}_{огл}(\eta) = H\left[tg(\alpha+\eta)+tg(\alpha-\eta)\right]. \tag{35}$$

Підставивши вирази (34) та (35) у формулу (33), отримаємо кінцевий вираз для обчислення площі ПЗО (миттєвої площі космічного знімання) на *плоскій* Землі за *відхилень* візирної осі від надира:

$$S^{\Diamond}_{огл}(\eta) = H^2 tg\beta\left[tg(\alpha+\eta)+tg(\alpha-\eta)\right]\cdot\left[sec(\alpha+\eta)+sec(\alpha-\eta)\right]. \tag{36}$$

Для *сферичної* Землі *ширину смуги огляду* можна знайти як [12, 14]

$$\widehat{L}^{\Diamond}_{огл}(\eta) = R_з\left\{\pi - 2\alpha - arccos\left[A_H^{-1}\,sin(\alpha-\eta)\right] - arccos\left[A_H^{-1}\,sin(\alpha+\eta)\right]\right\}, \tag{37}$$

де $A_H = R_з/(R_з+H)$ – аргумент висоти орбіти КА.

Для обчислення миттєвої площі знімання на *сферичній* Землі за *відхилень* візирної осі від надира можна скористатися наближеною формулою, отриманою як добуток виразів (34) та (37):

$$\widehat{S}^{\Diamond}_{огл}(\eta) \approx \widehat{L}^{\Diamond}_{огл}(\eta)\cdot H\left[sec(\alpha+\eta)+sec(\alpha-\eta)\right]tg\beta. \tag{38}$$

Графічна інтерпретація залежностей (35)−(38) подана на рис. 7. Наведені графіки свідчать про таке:

а) миттєві площі знімання визначаються *технічними характеристиками* БЗА та *висотою* орбіти КА, але не залежать від параметрів орбітального руху;

б) у разі відхилень візирної осі БЗА від надира ці *площі суттєво зростають*, особливо за кутів крену $\eta \geq 30^{\circ}$, якщо $\eta \geq 45^{\circ}$, то може суттєво *погіршуватися детальність* отримуваних космічних знімків.

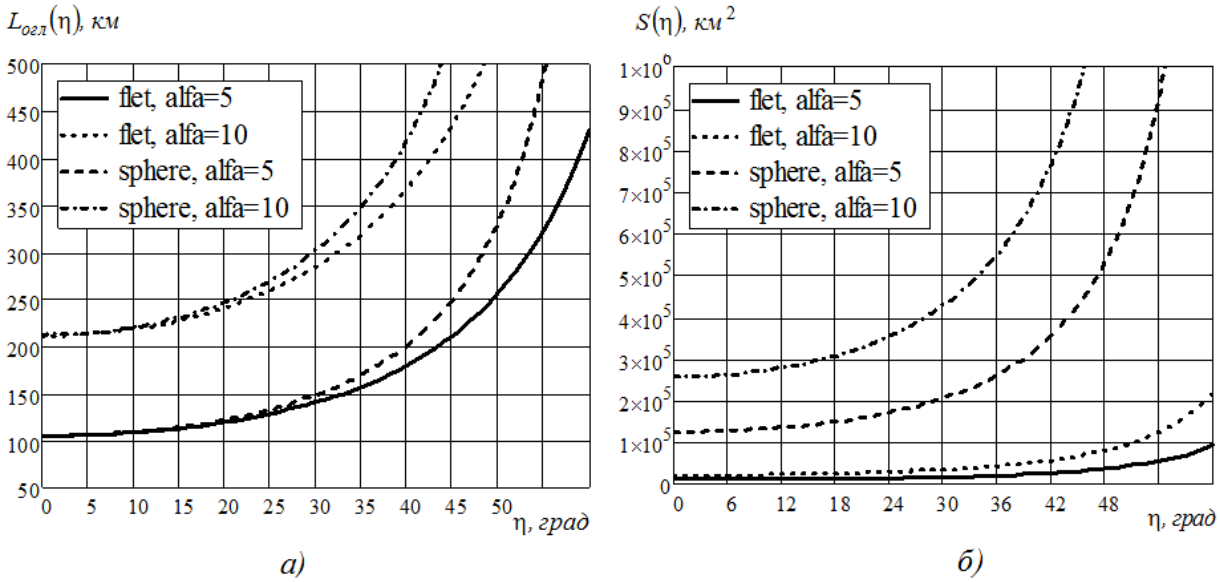


Рис. 7. Залежність ширини смуги огляду (а) та миттєвої площі знімання (б) від кута крену (flet – плоска Земля; sphere – сферична Земля; alfa – кут α в градусах)

Знята сцена $Ц_{\mu}^{\tau}(\lambda_*,\varphi_*)$ (див. рис. 2б) – це частина смуги огляду μ-го КА, обмежена її шириною $L_{огл}^{*}$ та довжиною спостережуваної ділянки $Д_{v}(t)$, яка утворюється за рахунок орбітального руху КА з лінійною швидкістю $V(t)$ за час космічного знімання τ.

Для розрахунків площі сцени, знятої μ-м КА за час τ, скористаємося такою формулою [12]:

$$Q_{\mu}^{\tau}(*) = S_{огл}^{*} + L_{огл}^{*} \int_{t_v^n}^{t_v^n+\tau} A_H \sqrt{\mu_0\left(\frac{2}{R_з + H} - \frac{1}{a}\right)}\, d\tau, \tag{39}$$

де $R_з = 6371$ км – середній радіус Землі;

$\mu_0 = 3{,}986 \cdot 10^5$ км^3/с^2 – гравітаційний параметр Землі;

$a = 0{,}5\left(H_A + H_П + 2R_з\right)$ – велика піввісь еліптичної орбіти;

H_A і $H_П$ – висота апогею і перигею еліптичної орбіти;

$H = H(t)$ – поточна висота орбіти КА.

Якщо для спостережень застосовують колові або майже колові орбіти з висотою H_o, то для розрахунків площі знятої сцени замість виразу (39) можна скористатися спрощеною формулою

$$Q_{\mu}^{\tau}(*) \approx S_{огл} + L_{огл} \frac{R_з \sqrt{\mu_0 / (R_з + H_o)}}{R_з + H_o} \tau. \tag{40}$$

Форму спостережуваної частини m-го РЗ, її розмір та положення на земній поверхні можна знайти як результат перетину фігур цього району та знятої сцени $Ц_{\mu}^{\tau}(\lambda_*,\varphi_*)$:

$$P_{m\mu}^{*}(\varphi_*,\lambda_*) = P_{m}^{*}(\varphi_*,\lambda_*) \cap Ц_{\mu}^{\tau}(\varphi_*,\lambda_*), \tag{41}$$

де символом ($*$) позначено форму фігури;

$(\varphi_*, \lambda_*) = (\varphi_*^{пн}, \varphi_*^{пд}, \lambda_*^{сх}, \lambda_*^{зх})$ – скорочене позначення географічних меж РЗ, знятої сцени та спостережуваної ділянки (північна та південна широта, східна та західна довгота відповідно).

Висновки

1. Запропоновані просторові та часові показники дозволяють оцінювати та/або прогнозувати наявність або відсутність *геометричної* видимості між μ-м КА та m-м РЗ, що становить необхідні, але ще недостатні умови для вибору доступних космічних систем, придатних для ОЕСп.

2. Для кінцевого вибору КА геометричні умови слід доповнити *фізичними*, зокрема показниками освітленості РЗ Сонцем, станом атмосфери, рівнем хмарності тощо. Ці фактори доцільно дослідити в наступних статтях.

СПИСОК ЛІТЕРАТУРИ

1. Концепція реалізації державної політики у сфері космічної діяльності на період до 2032 року, схвалена розпорядженням Кабінету Міністрів України від 30.03.2011. № 238-р. URL: http://zakon1.rada.gov.ua (дата звернення: 25.03.2019).

2. Загальнодержавна цільова науково-технічна космічна програма України на 2019–2023 роки (проект). URL: http://zakon1.rada.gov.ua (дата звернення 26.03.2019).

3. Фриз П. В. До проблеми управління процесом космічних спостережень заданих районів Землі при вирішенні оперативних завдань // Озброєння та військова техніка : наук.-техн. журнал. Київ : ЦНДІ ОВТ ЗС України, 2017. Вип. 1. С. 64–69.

4. Liu Xiaolua, Bai Baocunb, Chen Yingwua, Yao Fenga. Multi satellites scheduling algorithm based on task merging mechanism // Applied Mathematics and Computation. 2014. № 230. P. 687–700.

5. He Chuan, Liu Jin, Ma Manhao. A Dynamic Scheduling Method of Earth-Observing Satellites by Employing Rolling Horizon Strategy // The Scientific World Journal. 2013. P. 34–42

6. Towards dynamic real-time scheduling for multiple earth observation satellites / Jianjiang Wanga, Xiaomin Zhua, Laurence Yangb and other // Journal of Computer and System Sciences. 2015. № 81. P. 110–124.

7. A Distributed Cooperative Dynamic Task Planning Algorithm for Multiple Satellites Based on Multi-agent Hybrid Learning / Chong Wang, Jun Li, Ning Jing and other // Chinese Journal of Aeronautics. 2011. № 24. P. 493–505.

8. Гончаров А. К., Чернов А. А. Планирование сеансов приёма информации с космических аппаратов орбитальной группировки при ограниченном количестве приёмных комплексов // Космонавтика и ракетостроение. 2014. № 3 (74). С. 180–189.

9. Куссуль Н. М., Фриз В. П., Янчевський С. Л. Можливий підхід до раціонального планування космічної зйомки Землі на основі багатокритерійної оптимізації // Проблеми створення, випробовування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ НАУ, 2011. Вип. 4. С. 97–105.

10. Ожінський В. В., Парфенюк В. Г. Планування роботи бортових систем космічних апаратів при використанні координатних методів управління // Вісник ЖДТУ. Технічні науки. Житомир : ЖДТУ, 2011. Вип. № 1 (56). С. 61–71.

11. Савчук А. В. Оптимальне обслуговування заявок на отримання цільової інформації з борту космічних апаратів дистанційного зондування Землі // Вісник ЖДТУ. Технічні науки. Житомир : ЖДТУ, 2010. Вип. № 1 (52). С. 140–146.
12. Фриз П. В. Удосконалений математичний апарат для розрахунків розмірів контрольованих ділянок земної поверхні при космічних спостереженнях пірамідальною зоною огляду // Проблеми створення, випробовування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ НАУ, 2012. Вип. 6. С. 113–127.
13. Фриз П. В. Математичний апарат для оцінювання спостережуваності заданих районів Землі в задачах дистанційного зондування із космосу // Озброєння та військова техніка : наук.-техн. журнал. Київ : ЦНДІ ОВТ ЗС України, 2015. Вип. 1. С. 64–69.
14. Фриз П. В. Удосконалений математичний апарат для визначення спостережуваної площі заданого району Землі у завданнях космічного моніторингу // Вісник ЖДТУ. Технічні науки. Житомир : ЖДТУ, 2017. Вип. 2 (80). С. 126–134.
15. Кондратов О. М., Фриз П. В. Алгоритм автоматизованого вибору релевантних космічних апаратів для оптико-електронного спостереження заданих районів Землі // Вісник ЖДТУ. Технічні науки. Житомир : ЖДТУ, 2012. Вип. № 2 (61). С. 138–146.

Подано 17.04.2019

П. В. Фриз

СПОСОБ ВЫБОРА ДОСТУПНЫХ КОСМИЧЕСКИХ АППАРАТОВ ПО УСЛОВИЯМ ГЕОМЕТРИЧЕСКОЙ ВИДИМОСТИ МЕЖДУ НИМИ И ЗАДАННЫМИ РАЙОНАМИ ЗЕМЛИ

В условиях боевых действий на востоке Украины особо актуальной стала проблема обеспечения военного руководства информацией космической съемки. С учётом отсутствия отечественных средств для решения этих задач возможным практическим путем получения информации космической съемки является ее заказ и приобретение у зарубежных операторов. Следует отметить, что рынок этих услуг достаточно развит, поэтому возникает проблема корректного формирования заказов на съемку.

В статье предложен оригинальный способ выбора доступных иностранных космических аппаратов дистанционного зондирования Земли для использования их целевой информации в интересах Вооруженных Сил Украины. Он базируется на заблаговременных расчетах ожидаемых коэффициентов временного и пространственного накрытия заданных районов Земли зоной обзора определенных космических аппаратов, сравнении их с требованиями заказчиков целевой информации и выборе на этой основе наиболее подходящих вариантов.

Формализованы условия видимости заданного района Земли определенным космическим аппаратом в конкретную календарную дату. При этом использован аппарат логических функций геометрической видимости. Кроме того, предложен математический аппарат для расчета площади заданного района съемки в случае ее описания многоугольником произвольной формы с учетом эксцесса этого сферического многоугольника. Разработана математическая модель определения мгновенной площади

съемки на сферической Земле пирамидальной зоной обзора космического аппарата при отклонении визирной оси бортовой целевой аппаратуры по крену.

Предложены направления дальнейших исследований, в частности определение физических условий наблюдения заданных районов съемки.

Ключевые слова: *доступные космические аппараты; оптико-электронные наблюдения; проекция поля зрения; часовой и пространственный коэффициенты накрытия; заданный район Земли; бортовая съемочная аппаратура.*

P. V. Fryz

THE METOD OF SELECTING THE AVAILABLE SPACE VEHICLES UNDER THE TERMS OF GEOMETRICAL VISIBILITY BETWEEN THEM AND THE EARTH'S DESIGNATED AREAS

Under the warfare conditions in the east of Ukraine the problem of providing the command with space shooting information is gaining topicality. With respect to the absence of national means for solving these tasks, ordering and purchasing the space shooting information from foreign operators appears the only practical way of gaining the above information. It is noteworthy, that the market of these services is well-developed, this the problem of the reasonable formation of orders for shooting appears topical.

The paper suggests a unique method for selecting available foreign space vehicles for the Earth's remote sensing with the aim of using their target information for the benefit of the Armed Forces of Ukraine. The method is based on the advance calculations of the prognosticated coefficients of the temporal and spatial coverage of the Earth's designated areas by the inspection zone of the space vehicles selected, comparing them with the requirements of the target information ordering customers, as well as on choosing the most appropriate options on this basis.

The visibility conditions of the Earth's designated area by the determined space vehicle at a given calendar date are formalized. Along with it the instrument of logical functions of the geometric visibility is used. Besides, the author suggests the mathematical instruments for the calculating the area of the designated territory of shooting in case of its description by the polygon of arbitrary shape with respect to the excess of this spherical polygon. The author also develops the mathematical model for determining instant shooting area on the spherical Earth by the pyramid coverage zone of the space vehicle under the in roll deviation of the sight axis of the onboard target equipment.

The directions for the further research in general, and determining the physical conditions of monitoring the designated shooting areas in particular, are suggested.

Keywords: *available space vehicles; optical and the electronic observations; field of view projection; temporal and spatial coverage coefficients; Earth's designated area, onboard shooting equipment.*

ISSN 2076-1546

УДК 621.396.6 DOI: 10.46972/2076-1546.2019.16.10

С. О. Ковтун., С. В. Ковальчук, П. П. Топольницький

СТАТИСТИЧНІ ХАРАКТЕРИСТИКИ ЕНЕРГЕТИЧНО ПРИХОВАНОГО ФАЗОМАНІПУЛЬОВАНОГО СИГНАЛУ

На виході приймального тракту, реалізованого на основі автокореляційного алгоритму з квадратурною обробкою, закон розподілу вихідного ефекту відрізняється від нормального. За відсутності сигналу на вході приймача розподіл вихідного ефекту відповідає закону Релея, а за наявності – Релея – Райса.

Розглянуто розподіл щільності ймовірності на виході некогерентного автокореляційного приймача з квадратурною обробкою відносно вхідного рівня енергетично прихованого фазоманіпулюваного сигналу.

Для виявлення корисного сигналу необхідно, щоб на виході приймача відношення сигнал / шум перевищувало значення порога виявлення, обумовленого критерієм Неймана – Пірсона, відповідно до заданої ймовірності хибної тривоги. Розраховано рівень величини відношення сигнал / шум на виході некогерентного автокореляційного приймача з квадратурною обробкою. Характерною особливістю наведених графіків є лінійна залежність вихідного відношення сигнал / шум відносно вхідного. Ця особливість спостерігається в разі вхідного відношення сигнал / шум, меншого за одиницю.

Побудовано криві розподілу щільності ймовірності вхідної суміші сигналу та шуму, які відповідають узагальненому закону Релея (Релея – Райса). Спостерігається зміщення кривих за віссю абсцис відповідно до заданих імовірностей хибної тривоги і часу накопичення (спостереження). З отриманих графіків видно, що зміщення за віссю абсцис величини вхідного відношення сигнал / шум суттєво залежить від часу накопичення вхідної суміші.

На основі розподілу щільності ймовірності отримано криві виявлення енергетично прихованого фазоманіпулюваного сигналу некогерентним автокореляційним приймачем із квадратурною обробкою.

Результати розрахунків свідчать, що виявлення фазоманіпулюваного сигналу на фоні білого шуму можливе в разі вхідного відношення сигнал / шум, меншого за одиницю, тобто до -32 дБ *у реальному масштабі часу (до 0,1* с*).*

Ключові слова: *автокореляційний алгоритм; адитивна суміш; закон розподілу; квадратурна обробка; кодофазоманіпульований сигнал; статистичні характеристики; щільність імовірності.*

Постановка проблеми в загальному вигляді. Останнім часом спостерігається тенденція впровадження радіоелектронних систем (РЕС) із розширеним спектром (spread spectrum) у різних сферах радіоелектроніки, наприклад, у радіолокації, зв'язку та навігації. Сигнали з розширеним спектром у науковій літературі називаються складними, широкосмуговими, шумоподібними, богатомірними тощо. У РЕС із розширеним спектром широко застосовуються (особливо в супутникових системах радіонавігації) сигнали з кодовою фазовою маніпуляцією (КФМ).

Для вирішення завдання моніторингу сигналів із розширеним спектром (низькою спектральною щільністю потужності) необхідно знати деякі відомості про корисний сигнал і шум (заваду), а також за можливості максимально використовувати ці відомості для аналізу прийнятої суміші. Отримані апріорні дані дозволяють за сукупністю відмінностей між сигналом і шумом (завадою) встановити факт наявності або відсутності корисного сигналу в прийнятій суміші.

Синтезувати алгоритми обробки вхідних радіосигналів під час ведення моніторингу в умовах повної апріорної невизначеності параметрів вхідних сигналів можна на основі методу статистичного синтезу. При цьому однією з необхідних умов для синтезу радіоприймальних пристроїв моніторингу 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. Отже, виникає потреба більш детального дослідження параметрів таких сигналів.

Аналіз останніх досліджень і публікацій. Відомо [1, 2], що внаслідок просторової, поляризаційної, частотної, амплітудної, часової та структурної селекції на виході лінійного тракту радіоприймального пристрою присутня двокомпонентна адитивна суміш сигналу та шуму:

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

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

Як сигнальна складова розглядається КФМ коливання з рівномірно розподіленою початковою фазою, а шумова є гаусівським стаціонарним білим шумом із нульовим математичним сподіванням. У цьому разі потужність (дисперсія) сукупності сигналу σ_S^2 і шуму σ_ξ^2 дорівнює їх сумі [3, 4]:

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

На виході приймального тракту, реалізованого на основі автокореляційного алгоритму з квадратурною обробкою, закон розподілу вихідного ефекту відрізняється від нормального. За відсутності сигналу на вході приймача розподіл вихідного ефекту відповідає закону Релея, а за наявності – Релея – Райса [3, 4].

Виділення не вирішених раніше частин загальної проблеми, яким присвячується стаття. Статистичні характеристики адитивної суміші сигналу й білого шуму, наведені вище, справедливі, коли потужність сигналу перевищує потужність шуму $\left(\sigma_S^2 > \sigma_\xi^2\right)$. У випадку, що досліджується, на вході приймача моніторингу сигнальна складова значно менша за шумову $\left(\sigma_S^2 << \sigma_\xi^2\right)$, що недостатньо висвітлено в науковій літературі, а тому потребує більш глибокого вивчення. Слід також розглянути, як впливає тривалість накопичення таких сигналів на вихідний ефект приймача, що є досить актуальним.

Формулювання завдання дослідження. З урахуванням наведеного **метою та основним змістом статті** є визначення статистичних характеристик адитивної суміші нормального шуму і набагато слабшого КФМ сигналу на виході радіоприймального пристрою, реалізованого на основі автокореляційного алгоритму з квадратурною обробкою.

Виклад основного матеріалу. Для моніторингу енергетично прихованого сигналу є обґрунтованим [1, 2] використання приймача, побудованого на основі некогерентного автокореляційного алгоритму з квадратурною обробкою. Такий алгоритм є стійким до апріорної невизначеності параметрів вхідних сигналів невідомої форми з невідомою початковою фазою на фоні гаусівського стаціонарного шуму (завади).

Узагальнений закон Релея (Релея – Райса) має такий вигляд [3, 4]:

$$p(s) = s \cdot exp\left(-\frac{q^2 + s^2}{2}\right) I_0(q \cdot s), \tag{3}$$

де s – нормована напруга на виході тракту виявлення;

$I_0(\cdot)$ – модифікована функція Бесселя першого роду нульового порядку.

Графік розподілу щільності ймовірності за формулою (3) подано на рис. 1, де характерним є те, що зі збільшенням величини s функція розподілу Райса задовільно апроксимується функцією розподілу Гауса $(s \geq 3)$ [3].

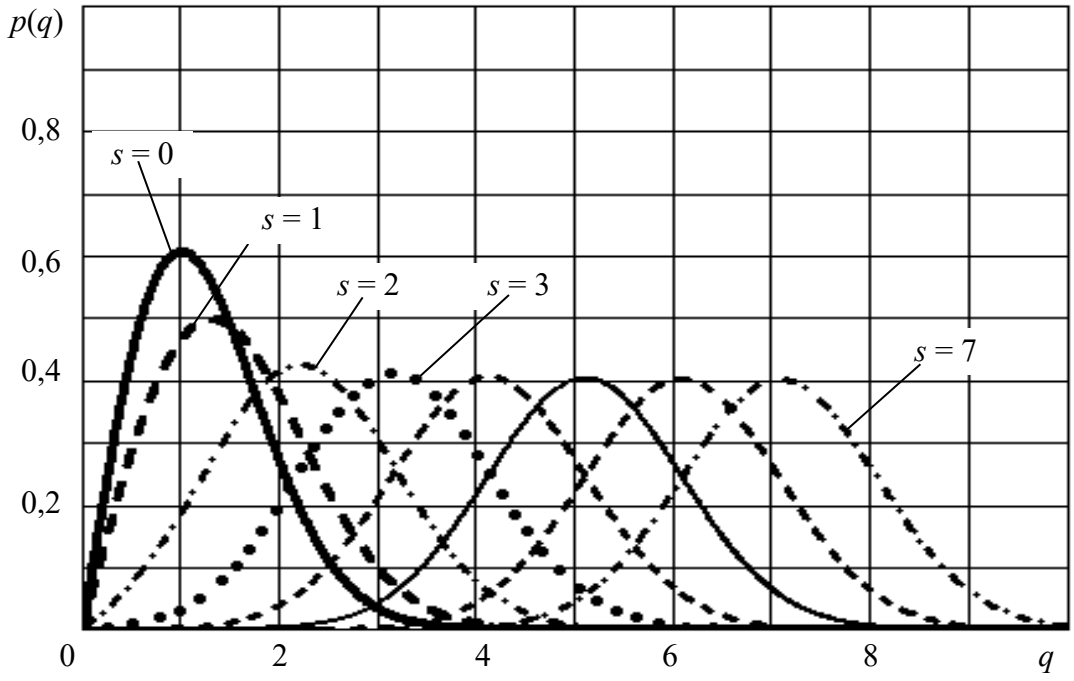


Рис. 1. Графік розподілу щільності ймовірності відповідно до узагальненого закону Релея

Для виявлення корисного сигналу необхідно, щоб на виході приймача відношення сигнал / шум перевищувало значення порога виявлення, обумовленого критерієм Неймана – Пірсона, відповідно до заданої ймовірності хибної тривоги. Вирази для розрахунку величини відношення сигнал / шум q на виході зазначеного вище приймача мають такий вигляд [5]:

$$q = \frac{\sqrt{2} g^2 \rho_s(\tau_{dl}) \sqrt{2 \Delta f T}}{\sqrt{\left(1 + \rho_\xi^2(\tau_{dl})\right) + 2g^2\left(1 + \rho_s(\tau_{dl})\rho_\xi(\tau_{dl})\right) + 2g^4\left(1 - \rho_\xi^2(\tau_{dl})\right)\frac{\Delta f}{\Delta f_S}}}, \quad (4)$$

$$g^2 = \frac{U_{\text{ms}}^2}{2\sigma_\xi^2}; \quad \sigma_\xi^2 = N_0 \Delta f; \quad \rho_\xi(\tau_{dl}) = \frac{sin(\pi \Delta f \tau_{dl})}{\pi \Delta f \tau_{dl}}; \quad \rho_s(\tau_{dl}) = \begin{cases} \left(\tau_p - |\tau_{dl}|\right); & |\tau_{dl}| \le \tau_p \\ 0, & |\tau_{dl}| > \tau_p \end{cases}, \quad (5)$$

де g^2 – відношення сигнал / шум за потужністю на вході приймача;

$\rho_s(\tau_{dl})$, $\rho_\xi(\tau_{dl})$ – коефіцієнти автокореляції обвідної вхідного сигналу й шуму відповідно;

N_0 – спектральна щільність білого шуму на вході приймача;

Δf_S – ширина спектра КФМ сигналу;

τ_p – бітовий інтервал КФМ сигналу;

τ_{dl} – часова неузгодженість, яка вноситься лінією затримки автокореляційного приймача з квадратурною обробкою.

На рис. 2 наведено результати розрахунку за співвідношенням (4) вихідного відношення сигнал / шум від вхідного. Відповідно до виразу (4) величина q суттєво залежить від ширини смуги пропускання приймача Δf і спектра сигналу Δf_S, автокореляційної функції сигналу й шуму, але найбільш важливим параметром є час накопичення (спостереження) вхідної суміші T, на який можна впливати на приймальній позиції радіомоніторингу.

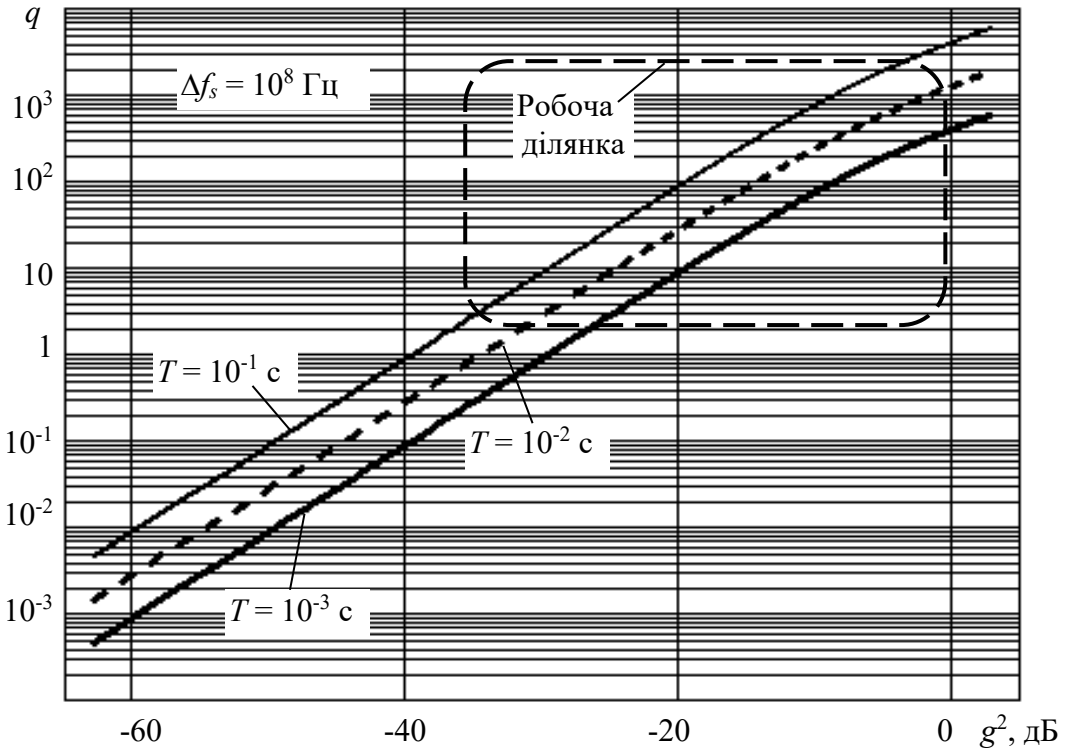


Рис. 2. Залежність вихідного відношення сигнал / шум від вхідного

Враховуючи вирази (3)–(5), побудуємо розподіл щільності ймовірності вхідної суміші сигналу і шуму (рис. 3). Математичне сподівання наведених сигналів взято відповідно до порогових значень, обумовлених критерієм Неймана – Пірсона відповідно до заданих імовірностей хибної тривоги $P_F = 10^{-3}$ і $P_F = 10^{-6}$. З графіків, наведених на рис. 3, видно, що зміщення за віссю абсцис величини вхідного відношення сигнал / шум суттєво залежить від часу накопичення вхідної суміші відповідно до співвідношення (4).

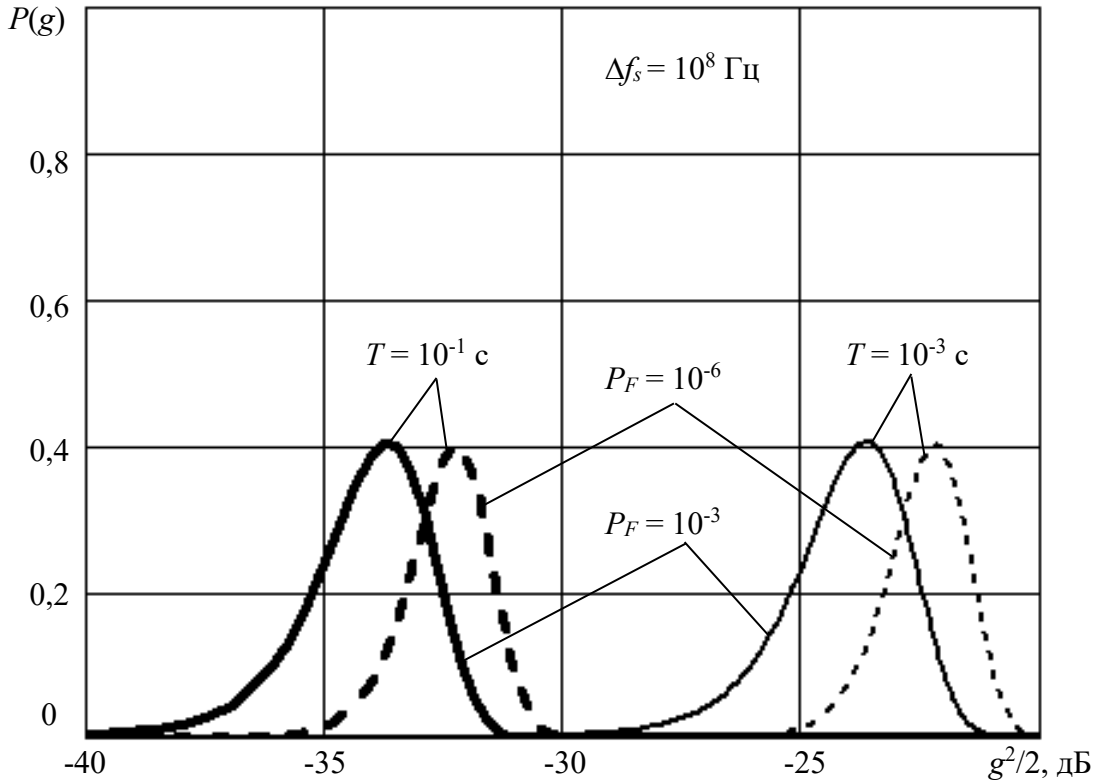


Рис. 3. Розподіл щільності ймовірності вхідної суміші сигналу та шуму

Отже, наведені криві розподілу щільності ймовірності вхідної суміші сигналу та шуму відповідають узагальненому закону Релея (Релея – Райса). Спостерігається зміщення кривих за віссю абсцис відповідно до заданих імовірностей хибної тривоги та часу накопичення (спостереження).

Отримавши криві розподілу щільності ймовірності вхідної суміші сигналу та шуму, можна розрахувати криві виявлення слабкого КФМ сигналу. Імовірність правильного виявлення визначається таким співвідношенням [3, 4]:

$$P_D = \int_{q_{trd}}^{\infty} s \cdot exp\left(-\frac{q^2 + s^2}{2}\right) I_0\left(q \cdot s\right) ds, \qquad (6)$$

де q_{trd} – умовний поріг виявлення за напругою.

Згідно зі співвідношенням (6), а також з урахуванням (4) і (5) проведено розрахунки характеристик виявлення, результати яких наведено на рис. 4. Вони свідчать, що виявлення КФМ сигналу на фоні білого шуму можливе в разі вхідного відношення сигнал / шум, меншого за одиницю. У розглянутому випадку (з урахуванням втрат за

некогерентної обробки) для забезпечення ймовірності правильного виявлення $P_D = 0{,}9$ за $\tau_{dl} = 1/\Delta f$ ($\Delta f \approx \Delta f_S$), імовірності хибної тривоги $P_F = 10^{-3}$ і $P_F = 10^{-6}$ (порогове відношення сигнал / шум $q_{trd} = 3{,}717;\ 5{,}257$) і постійної часу інтегратора $T = 10^{-3}$ с необхідно, щоб вихідне відношення сигнал / шум було не менше $q = 4{,}88;\ 6{,}45$, а вхідне відношення сигнал / шум $g^2 = -22{,}6$ дБ і $-21{,}4$ дБ відповідно (рис. 4). За $T = 10^{-1}$ с для досягнення тих самих імовірностей P_D і P_F необхідно, щоб вхідне відношення сигнал / шум було не менше $g^2 = -32{,}6$ дБ і $-31{,}4$ дБ відповідно.

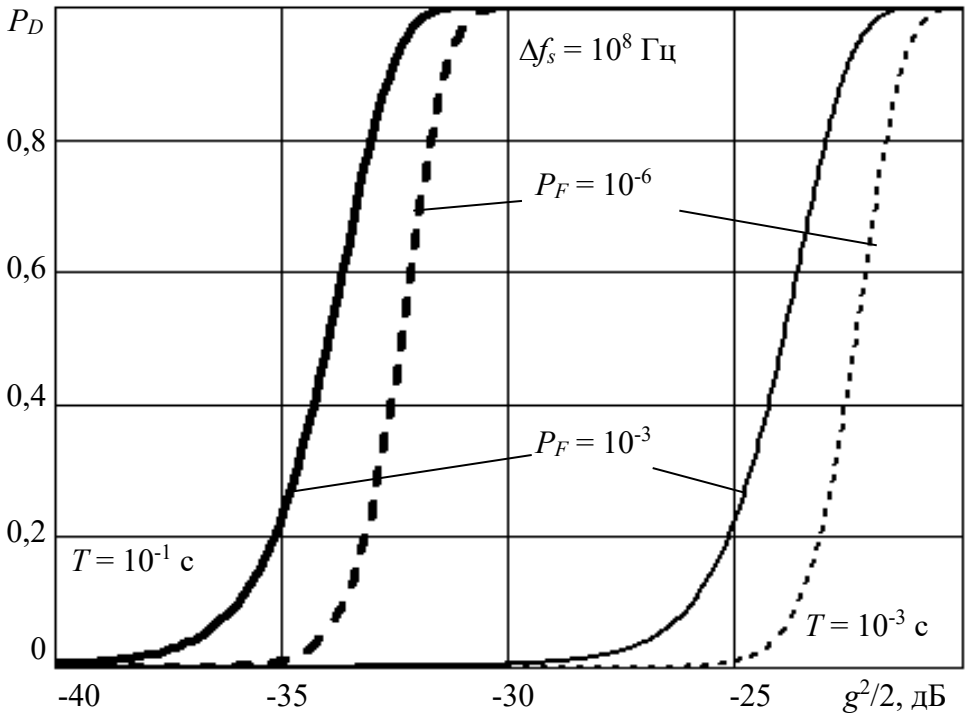


Рис. 4. Криві виявлення енергетично прихованого КФМ сигналу на фоні білого шуму

Висновки. У статті визначено статистичні характеристики адитивної суміші нормального шуму і набагато слабшого КФМ сигналу на виході радіоприймального пристрою, реалізованого на основі автокореляційного алгоритму з квадратурною обробкою.

Результати розрахунків свідчать, що виявлення КФМ сигналу на фоні білого шуму можливе в разі вхідного відношення сигнал / шум до -32 дБ у реальному масштабі часу (до 0,1 с).

Провівши дослідження статистичних характеристик енергетично прихованого КФМ сигналу доцільно в подальшому здійснити обґрунтування (синтез) приймача моніторингу.

СПИСОК ЛІТЕРАТУРИ

1. Ковтун С. О. Результати аналізу відомих алгоритмів для обробки енергетично прихованих сигналів // Зб. наук. праць НДІ ГУР МО України. 2011. № 31. С. 100–114.

2. Ковальчук С. В., Стейскал А. Б. Методичний підхід до визначення статистичних характеристик кодофазоманіпульованих сигналів // Наукові проблеми розвитку і удосконалення функціонування системи воєнної розвідки України : Зб. тез доп. наук. конф. (29 травня 2014 р.). Київ, 2014. С. 71–72.

3. Тихонов В. И. Оптимальный прием сигналов. Москва : Радио и связь, 1983. 320 с.
4. Левин Б. Р. Теоретические основы статистической радиотехники. Кн. 1. Москва : Сов. радио, 1966. 728 с.
5. Дятлов А. П., Кульбикаян Б. Х. Радиомониторинг излучений спутниковых радионавигационных систем. Москва : Радио и связь, 2006. 270 с.
6. Кобзарь А. И. Прикладная математическая статистика. Для инженеров и научных работников Москва : ФИЗМАТЛИТ, 2012. 816 с.
7. Ефимова М. Р., Петрова Е. В., Румянцев В. Н. Общая теория статистики : учебник. Москва : ИНФРА-М, 2013. 416 с.

Подано 27.05.2019

С. А. Ковтун, С. В. Ковальчук, П. П. Топольницкий

СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ЭНЕРГЕТИЧЕСКИ СКРЫТОГО ФАЗОМАНИПУЛИРОВАННОГО СИГНАЛА

На выходе приемного тракта, реализованного на основе автокорреляционного алгоритма с квадратурной обработкой, закон распределения выходного эффекта отличается от нормального. При отсутствии сигнала на входе приемника распределение выходного эффекта соответствует закону Рэлея, а при наличии – Рэлея – Райса.

Рассмотрено распределение плотности вероятности на выходе некогерентного автокорреляционного приемника с квадратурной обработкой относительно входного уровня энергетически скрытого фазоманипулированного сигнала.

Для выявления полезного сигнала необходимо, чтобы на выходе приемника отношение сигнал / шум превышало значение порога обнаружения, обусловленного критерием Неймана-Пирсона, в соответствии с заданной вероятности ложной тревоги. Рассчитан уровень величины отношения сигнал / шум на выходе некогерентного автокорреляционного приемника с квадратурной обработкой. Характерной особенностью представленных графиков является линейная зависимость выходного отношения сигнал / шум относительно входного. Эта особенность наблюдается при входном отношении сигнал / шум меньше единицы.

Построены кривые распределения плотности вероятности входной смеси сигнала и шума, которые соответствуют обобщенному закону Рэлея (Рэлея – Райса). Наблюдается смещение кривых по оси абсцисс в соответствии с заданными вероятностями ложной тревоги и времени накопления (наблюдения). Из полученных графиков видно, что смещение по оси абсцисс величины входного отношения сигнал / шум существенно зависит от времени накопления входной смеси.

На основе распределения плотности вероятности получены кривые обнаружения энергетически скрытого фазоманипулированного сигнала некогерентным автокорреляционным приемником с квадратурной обработкой.

Результаты расчетов свидетельствуют, что выявление фазоманипулированного сигнала на фоне белого шума возможно при входном отношении сигнал / шум меньше единицы, то есть до -32 дБ *в реальном масштабе времени (до 0,1* с*).*

Ключевые слова: *автокорреляционный алгоритм; аддитивная смесь; закон распределения; квадратурная обработка; кодофазоманипулированный сигнал; статистические характеристики; плотность вероятности.*

S. A. Kovtun, S. V. Kovalchuk, P. P. Topolnytsky

STATISTICAL CHARACTERISTICS OF THE ENERGY-CONCEALED PHASE-MANIPULATED SIGNAL

The law of distribution of the output effect differs from the normal one at the output of the receiving path realized on the basis of autocorrelation algorithm with quadrature processing. When there is no signal at the input of the receiver, the distribution of the output effect corresponds to Rayleigh's or Rayleigh – Rice's law in condition of its presence.

The probability density distribution at the output of an incoherent auto correlation receiver with quadrature processing is considered in relation to the input level of the energy-concealed phase-manipulated signal.

In order to detect a useful signal it is necessary that, at the output of the receiver, the signal / noise ratio exceeds the detection threshold determined by the Neumann – Pearson criterion according to the given probability of false alarm. The level of the signal-to-noise ratio at the output of an incoherent autocorrelation receiver with quadrature processing has been calculated. A characteristic feature of the presented graphs is the linear dependence of the output signal / noise ratio relative to the input signal. This feature is observed in the input signal / noise ratio which is less than one.

The curves for the distribution of the probability density of the input signal mix and noise corresponding to the generalized Rayleigh's law (Rayleigh-Rice) are constructed in the book. There is a shift of curves for the abscissa axis according to the given probabilities of false alarms and accumulation time (observation). It is evident from the given graphs that the offset of the abscissa of the input signal value / noise ratio significantly depends on the accumulation of the input mixture time.

The curves for detecting an energy-concealed phase-manipulated signal by a non-coherent autocorrelation receiver with quadrature processing on the basis of the probability density distribution are obtained.

The results of the calculations indicate that detection of a phase-manipulated signal on the background of "white" noise is possible in case of an input-to-noise ratio of less than one, that is, up to -32 dB *in real time (up to 0.1* s*).*

Keywords*: autocorrelation algorithm; additive mixture; distribution law; quadrature processing; code-phase-manipulated signal; statistical characteristics; density probability.*

УДК 681.32 DOI: 10.46972/2076-1546.2019.16.11

В. В. Стрінада, М. О. Гуменюк, В. П. Добровінський, А. О. Ткач

КРИТЕРІЙ УПРАВЛІННЯ РОБОТИЗОВАНОЮ СИСТЕМОЮ З УРАХУВАННЯМ ВПЛИВУ НЕКОНТРОЛЬОВАНИХ ФАКТОРІВ

У статті запропоновано критерій управління роботизованою системою, який на основі інформаційного підходу дозволяє враховувати вплив неконтрольованих факторів та статистичних зв'язків між ними в процесі добування інформації.

У даній науковій роботі вибір оптимальної стратегії управління роботизованою системою в процесі добування інформації забезпечує показник, який характеризує ефективність управління. Слід зауважити, що наявність неконтрольованих факторів (перешкод, погодних умов, технічних несправностей тощо), які враховані у формальній математичній моделі управління, призводить до залежності показника ефективності не лише від вибраної стратегії управління, а й від значень неконтрольованих факторів. При цьому як вибрана стратегія управління, так і показник ефективності процесу добування інформації є функціями від неконтрольованих факторів відповідно.

Використання запропонованого критерію дозволяє приймати правильні рішення в процесі управління роботизованою системою в разі впливу неконтрольованих факторів. Він може бути застосований за умов статистичної залежності неконтрольованих факторів та зміни станів досліджуваного процесу. Даний критерій не вимагає побудови моделей на основі оцінюваних комбінацій факторів, що істотно знижує часові та обчислювальні витрати для прийняття рішень у процесі управління роботизованою системою. Його використання дозволяє визначати, наскільки нове спостереження збільшить обізнаність роботизованої системи щодо стану досліджуваного процесу.

Варто зауважити, що перспективи подальших досліджень можуть полягати в модифікації чинних та розробці нових методів планування застосування роботизованої системи на основі запропонованого критерію.

Ключові слова: *критерій управління; роботизована система; вплив неконтрольованих факторів; інформаційний підхід.*

Постановка проблеми в загальному вигляді. В умовах стрімкого розвитку роботизованих систем постійно підвищуються вимоги до процесу управління ними. Це зумовлює необхідність підвищення ефективності управління роботизованими системами, одним із пріоритетних напрямків якого є розроблення сучасної методологічної бази автоматизованого процесу обробки інформації на основі всебічного комплексного аналізу даних. При цьому процес добування інформації роботизованою системою визначається як стохастичний [1, 2], а управління ним здійснюється відповідно до певного критерію для прийняття правильного рішення за результатами спостережень.

Також слід зазначити, що процес управління роботизованою системою характеризується впливом великої кількості неконтрольованих факторів (перешкод, погодних умов, технічних несправностей тощо), неврахування яких під час прийняття управлінських рішень призводить до зниження ефективності самого процесу управління.

Тому актуальною проблемою є обґрунтування критерію управління роботизованою системою з урахуванням впливу неконтрольованих факторів.

Аналіз останніх досліджень і публікацій.

Інформаційний підхід набув широкого розповсюдження в робототехніці, зокрема в управлінні роботизованими системами. Так, у [3, 4] запропоновано керувати роботами на основі кількості інформації між даними сенсорів та координатами цілі. У [5] використано схожий метод для дослідження навколишнього середовища в умовах невизначеності. У [6–8] розглянуто проблему планування маршрутів для дослідження навколишнього середовища на основі інформаційного критерію.

У [9, 10] використано інформаційний підхід для управління мережею сенсорів у процесі добування даних для визначення стану навколишнього середовища. В [11] описано використання інформаційного підходу для процесу управління дослідження стану стохастичної системи. У [12] показано переваги цього підходу для управління сенсорами з бінарними вимірюваннями порівняно з іншими критеріями.

У роботах [13, 14] запропоновано використання інформаційного підходу в ході планування застосування мобільних роботів для вирішення завдань із дослідження навколишнього середовища. Однак запропоновані в [13, 14] підходи не є адаптованими до врахування нових вимірювань у процесі виконання запланованого завдання. Це значно знижує ефективність управління в умовах зміни обстановки.

Слід зазначити, що у вказаних публікаціях не враховано вплив неконтрольованих факторів на процес управління та є припущення щодо незалежності результатів проведених роботами вимірювань, а це призводить до хибного визначення інформативності сукупності вимірювань та, як наслідок, до помилкових рішень у ході управління роботизованою системою.

Таким чином, **метою статті** є розробка критерію управління роботизованою системою на основі інформаційного підходу, який дозволить враховувати вплив неконтрольованих факторів та статистичних зв'язків між ними в процесі добування інформації.

Виклад основного матеріалу. В ідеальному випадку вибір оптимальної стратегії управління добуванням інформації роботизованою системою U забезпечує число $G = G(U)$, яке характеризує ефективність управління роботизованою системою. Водночас наявність неконтрольованих факторів x, які враховують у формальній математичній моделі управління, веде до залежності показника ефективності не лише від вибраної управлінської стратегії, а й від x, тобто $G = G(U, x)$. При цьому як вибрана стратегія управління, так і показник ефективності процесу добування інформації є функціями неконтрольованих факторів.

Розглянемо роботизовану систему Ω, яка отримує інформацію про досліджувану систему Λ. Під час добування даних система Λ може знаходитися в одному зі станів $L_i = \{L_1, L_2, ..., L_N\}$, де N – кількість можливих станів, які утворюють повну групу подій. Процес переходу системи Λ в один зі станів L_i є випадковим, опишемо його кінцевою множиною ймовірностей $\{p(L_1), p(L_2), ..., p(L_N)\}$, $\sum_{i=1}^{N} p(L_i) = 1$.

Припустимо, що в процесі добування інформації на роботизовану систему Ω може впливати неконтрольований фактор x_k, який може приймати J дискретних значень (градацій).

Ентропію рішення про стан системи Λ, за умови визначення j-ї градації k-го неконтрольованого фактора, будемо знаходити як

$$H\left(L/x_{kj}\right)=-\sum_{i=1}^{N}p\left(L_i/x_{kj}\right)log_N\,p\left(L_i/x_{kj}\right), \tag{1}$$

де $p\left(L_i/x_{kj}\right)$ – умовна ймовірність знаходження системи Λ в i-му стані за умови визначення j-ї градації k-го неконтрольованого фактора, $j=\overline{1,J}$.

Застосовуючи формулу Бейєса для визначення умовної ймовірності $p\left(L_i/x_{kj}\right)$, отримаємо

$$p\left(L_i/x_{kj}\right)=\frac{p\left(L_i\right)p\left(x_{kj},/L_i\right)}{p\left(x_{kj}\right)},$$

де $p\left(L_i\right)$ – апріорна ймовірність знаходження системи Λ у L_i-му стані;

$p\left(x_{kj}\right)=\sum_{i=1}^{N}p\left(L_i\right)p\left(x_{kj}/L_i\right)$ – імовірність отримання j-ї градації k-го неконтрольованого фактора в ході добування інформації;

$p\left(x_{kj}/L_i\right)$ – умовна ймовірність отримання j-ї градації k-го неконтрольованого фактора в разі знаходження системи Λ у L_i-му стані.

Після підстановки останнього виразу в (1) формула для розрахунку ентропії рішення про стан системи в разі отримання j-ї градації k-го неконтрольованого фактора матиме вигляд:

$$\begin{aligned}H\left(L/x_{kj}\right)&=-\frac{1}{p\left(x_{kj}\right)}\sum_{i=1}^{N}p\left(L_i\right)p\left(x_{kj}/L_i\right)log_N\frac{p\left(L_i\right)p\left(x_{kj}/L_i\right)}{\sum_{i=1}^{N}p\left(L_i\right)p\left(x_{kj}/L_i\right)}=\\&=-\frac{1}{p\left(x_{kj}\right)}\left(\begin{array}{l}\sum_{i=1}^{N}p\left(L_i\right)p\left(x_{kj}/L_i\right)log_N\,p\left(L_i\right)p\left(x_{kj}/L_i\right)-\\-\sum_{i=1}^{N}p\left(L_i\right)p\left(x_{kj}/L_i\right)log_N\sum_{i=1}^{N}p\left(L_i\right)p\left(x_{kj}/L_i\right)\end{array}\right).\end{aligned} \tag{2}$$

Для одержання ентропії рішення слід знайти суму значень величин $H\left(L/x_{kj}\right)$ за всіма градаціями з вагами, пропорційними ймовірності появи кожної з них, тобто $p\left(x_{kj}\right)$. Тоді матимемо

$$\begin{aligned}H\left(L/x_k\right)&=-\sum_{j=1}^{J}p\left(x_{kj}\right)H\left(L/x_{kj}\right)=-\sum_{j=1}^{J}\sum_{i=1}^{N}p\left(L_i,x_{kj}\right)\times\\&\times log_N\,p\left(L_i,x_{kj}\right)+\sum_{j=1}^{J}\sum_{i=1}^{N}p\left(L_i,x_{kj}\right)\sum_{i=1}^{N}log_N\,p\left(L_i,x_{kj}\right),\end{aligned} \tag{3}$$

де $p(L_i, x_{kj}) = p(L_i)p(x_{kj} / L_i)$.

Відповідно до [2] кількість інформації про стан системи Λ, у разі отримання k-го неконтрольованого фактора, можна знайти як

$$I_k(L) = H_0(L) - H(L / x_k), \tag{4}$$

де $H_0(L)$ – початкова ентропія рішення про стан системи Λ.

Значення початкової ентропії рішення знайдемо за виразом

$$H_0(L) = -\sum_{i=1}^{N} p(L_i) log_N\, p(L_i). \tag{5}$$

За відсутності статистичних зв'язків між неконтрольованими факторами кількість інформації про стан системи Λ за умови визначення n неконтрольованих факторів знайдемо за виразом

$$I(L) = \sum_{k=1}^{n} I_k(L), \tag{6}$$

де $k = \overline{1,n}$.

Однак оцінити кількість інформації, що добуває роботизована система, у разі впливу статистично зв'язаних неконтрольованих факторів, використовуючи шеннонівську міру, досить складно, оскільки для цього потрібно знайти багатомірні розподіли ймовірностей.

Щоб обійти складності оцінювання багатомірних розподілів імовірностей неконтрольованих факторів та водночас врахувати статистичні зв'язки між ними, використаємо спосіб, наведений у [15]. Відповідно до нього значення кількості інформації, що добуває роботизована система з урахуванням статистичних зв'язків між неконтрольованими факторами, будемо знаходити за таким виразом:

$$I(L) = \sum_{k=1}^{n} I_k(L)\left[1 - \sum_{\beta=0}^{k-1} \gamma_{k\beta} \frac{I_\beta(L)}{\left(I_\beta(L)\right)_{max}}\right], \tag{7}$$

де $I_k(L)$ та $I_\beta(L)$ – кількість інформації, що добуває роботизована система в ході визначення відповідно k-го та β-го неконтрольованого фактора;

$\left(I_\beta(L)\right)_{max}$ – максимально можлива кількість інформації, яку добуває роботизована система в разі визначення β-го неконтрольованого фактора;

$\gamma_{k\beta}$ – коефіцієнт, що характеризує статистичний зв'язок між k-м та β-м неконтрольованим фактором.

Як видно з (7), для знаходження кількості інформації, добутої роботизованою системою, необхідно оцінити статистичні зв'язки між факторами, які характеризуються коефіцієнтом $\gamma_{k\beta}$. Для цього використаємо критерії згоди, які базуються на обчисленні ступеня розходження виміряних частот сумісної появи дискретних значень факторів із гіпотетичним розподілом частот, що відповідає умові незалежності факторів.

Спочатку припустимо, що неконтрольовані фактори статистично незалежні. Гіпотетичний розподіл частот, який відповідає цій умові, потрібно статистично перевірити. Для цього використаємо критерій Пірсона.

Припустимо, що необхідно кількісно визначити статистичний зв'язок між факторами x_1 та x_2, що можуть мати в загальному випадку декілька градацій, тобто x_{1j} та $x_{2\phi}$ ($\phi = \overline{1,q}$, q – максимальна кількість градацій ϕ-го фактора).

У табл. 1 наведено розподіли виміряних частот $M_{j\phi}$ сумісної появи j-го значення x_1-го та ϕ-го значення x_2-го неконтрольованих факторів.

Таблиця 1

Частоти сумісної появи j-го значення x_1-го та ϕ-го значення x_2-го неконтрольованих факторів

Градація x_1	Градація x_2				
	x_{21}	x_{22}	…	x_{2q}	$\sum$
x_{11}	$\left[M_{11}^0\right]\ M_{11}$	$\left[M_{12}^0\right]\ M_{12}$	…	$\left[M_{1q}^0\right]\ M_{1q}$	$M_1(x_{2q})$
x_{12}	$\left[M_{21}^0\right] M_{21}$	$\left[M_{22}^0\right] M_{22}$	…	$\left[M_{2q}^0\right] M_{2q}$	$M_2(x_{2q})$
…	…	…	$\left[M_{j\phi}^0\right] M_{j\phi}$	…	…
x_{1J}	$\left[M_{J1}^0\right] M_{J1}$	$\left[M_{J2}^0\right] M_{J2}$	…	$\left[M_{Jq}^0\right] M_{Jq}$	$M_J(x_{2q})$
$\sum$	$M_1(x_{1J})$	$M_2(x_{1J})$	…	$M_q(x_{1J})$	W

У даній таблиці використано такі позначення:

$M_j(x_{2q})$ – підсумкові частоти відповідних рядків дискретних значень градацій першого неконтрольованого фактора ($M_j(x_{2q}) = \sum_{\phi=1}^{q} M_{j\phi}$, коли $j = const$);

$M_\phi(x_{1J})$ – підсумкові частоти відповідних стовпців дискретних значень другого неконтрольованого фактора ($M_\phi(x_{1J}) = \sum_{j=1}^{J} M_{j\phi}$, коли $\phi = const$);

$W = \sum_{j=1}^{J} M_j(x_{2\phi}) = \sum_{\phi=1}^{q} M_\phi(x_{1j})$ – сума всіх виміряних частот сумісної появи дискретних значень неконтрольованих факторів;

$\left[M_{j\varphi}^0\right] = \left[M_j(x_{2q})\right]\left[M_q(x_{1J})\right] / W$ – гіпотетичні частоти.

Сформуємо зважені суми квадратів величин $M_{j\phi}$ від їх гіпотетичних частот $\left[M_{j\phi}^0\right]$:

$$\nu^2 = \sum_{j=1}^{J}\sum_{\varphi=1}^{q} \frac{\left(M_{j\varphi} - \left[M_{j\varphi}^0\right]^2\right)^2}{\left[M_{j\varphi}^0\right]}. \qquad (8)$$

Подвійна сума (8) розподілена приблизно як $\chi^2_{k\beta}$ з кількістю ступенів вільності $\xi = (J-1)(q-1)$ [15]. Тому будемо вважати, що

$$\chi^2_{k\beta} = \nu^2. \tag{9}$$

Чим більша величина $\chi^2_{k\beta}$ для кожної пари факторів x_k та x_β, тим більший статистичний зв'язок між ними (для статистично незалежної пари факторів $M_{j\phi} = \left[M^0_{j\phi}\right]$ та $\chi^2_{k\beta} = 0$).

У разі використання критерію Пірсона у виразі (8) величину $\chi^2_{k\beta}$ для пар факторів потрібно нормувати, розділивши їх на $\left(\chi^2_{k\beta}\right)_{max}$ для цієї пари параметрів, тобто потрібно знайти

$$\gamma_{k\beta} = \chi^2_{k\beta} / \left(\chi^2_{k\beta}\right)_{max}, \tag{10}$$

де $\left(\chi^2_{k\beta}\right)_{max} = W$.

Статистичні зв'язки між неконтрольованими факторами у (8) враховано в усіх їх парних комбінаціях. Зв'язками більш високих порядків знехтували через їх несуттєвість для практичних розрахунків [15].

Отже, за критерій управління роботизованою системою доцільно взяти максимальну кількість інформації, що її добуває система внаслідок реалізації варіанта застосування $I^*(L) = \max\limits_{a \in A} I(L)$, де $A = \{a_1, a_2, ..., a_D\}$ – усі можливі варіанти використання роботизованої системи. Даний критерій забезпечить управління роботизованою системою з урахуванням неконтрольованих факторів, що впливають на процес добування інформації.

Висновки. Таким чином, у статті вирішено актуальне завдання розробки критерію управління роботизованою системою. Запропонований критерій на основі інформаційного підходу дозволяє оцінювати ефективність управління роботизованою системою в умовах впливу неконтрольованих факторів з урахуванням статистичних зв'язків між ними. Його застосування дозволяє прийняти рішення про те, наскільки нове спостереження підвищить обізнаність роботизованої системи щодо стану об'єкта дослідження.

Наукова новизна отриманих результатів полягає в удосконаленні критерію управління роботизованою системою за рахунок врахування впливу неконтрольованих факторів та статистичних зв'язків між ними.

Подальші дослідження слід присвятити розробленню методики планування застосування роботизованої системи на основі запропонованого критерію.

СПИСОК ЛІТЕРАТУРИ

1. Charrow B. Information-theoretic active perception for multi-robot teams, PhD thesis / Benjamin Charrow. Philadelphia: University of Pennsylvania, 2015. 175 p.

2. Humeniuk M. O., Sashchuk I. M., Zhuravskyi Yu. V. The criterion for feature informativeness estimation in multi robot teams control // Радіоелектроніка, інформатика, управління. 2018. № 4. С. 96–105. DOI 10.15588/1607-3274-2018-4-9.

3. Grocholsky B. Information-theoretic control of multiple sensor platforms, PhD thesis. Sydney : University of Sydney, 2002. 199 p.
4. Grocholsky B., Makarenko A., Durrant-Whyte H. Information theoretic control of multiple sensor platforms // In Proceedings of the IEEE International Conference on Robotics and Automation. 2003. Vol. 1. P. 1521–1526.
5. Bourgault F., Makarenko A., Williams S. Information based adaptive robotic exploration // In Proceedings of the IEEE International Conference on Intelligent Robots and Systems. 2002. P. 540–545.
6. Choi H. L., How J. P. Continuous trajectory planning of mobile sensors for informative forecasting // Automatica. 2011. P. 145–152.
7. Ny J. L., Pappas G. J. On trajectory optimization for active sensing in gaussian process models // In Proceedings of the Joint IEEE Conference on Decision and Control and Chinese Control Conference. 2009. P. 6282–6292.
8. Singh A., Krause A., Guestrin C. Efficient planning of informative paths for multiple robots // In Proceedings of the International Joint Conference on Artificial Intelligence. 2007. P. 93–105.
9. A scalable information theoretic approach to distributed robot coordination / [B. Julian, M. Angermann, M. Schwager et al.] // In IEEE/RSJ Conference on Intelligent Robots and Systems (IROS). 2011. P. 46–53.
10. Zhao F., Shin J., Reich J. Information-driven dynamic sensor collaboration // IEEE Signal Processing Magazine. 2002. P. 61–72.
11. Feng X., Loparo K., Fang Y. Optimal state estimation for stochastic systems: An information theoretic approach // IEEE Transactions on Automatic Control. 1997. Vol. 42, № 6. P. 771–785.
12. Kreucher C., Kastella K., Hero A. Information based sensor management for multitarget tracking // In Processing SPIE, Bellingham, WA. 2003. Vol. 5204. P. 480–489.
13. Efficient informative sensing using multiple robots / [A. Singh, A. Krause, C. Guestrin et al.] // J. of AI Research. 2009. № 34 (1). P. 707–755.
14. Binney J., Krause A., Sukhatme G. Optimizing waypoints for monitoring spatiotemporal phenomena // International Journal Robotics Research. 2013. № 32 (8). P. 873–888.
15. Анисимов Б. В., Курганов В. Д., Злобин В. К. Распознавание и цифровая обработка изображений : учеб. пособ. для студентов вузов. Москва : Высшая школа, 1983. 295 с.

Подано 19.06.2019

В. В. Стринада, М. А. Гуменюк, В. П. Добровинский, А. А. Ткач

КРИТЕРИЙ УПРАВЛЕНИЯ РОБОТИЗИРОВАННОЙ СИСТЕМОЙ С УЧЕТОМ ВЛИЯНИЯ НЕКОНТРОЛИРУЕМЫХ ФАКТОРОВ

В статье предложен критерий управления роботизированной системой, который на основе информационного подхода позволяет учитывать влияние неконтролируемых факторов и статистических связей между ними в процессе добывания информации.

В данной статье выбор оптимальной стратегии управления роботизированной системой в процессе добывания информации обеспечивает показатель, характеризующий эффективность управления. Вместе с тем наличие неконтролируемых факторов (помех, погодных условий, технических неисправностей и т. п.), учтённых в формальной математической модели управления, ведет к зависимости показателя эффективности не только от выбранной стратегии управления, но и от значений неконтролируемых

факторов. При этом как выбранная стратегия управления, так и показатель эффективности процесса управления являются функциями от неконтролируемых факторов.

Использование предложенного критерия позволяет принимать правильные решения в процессе управления роботизированной системой при воздействии неконтролируемых факторов. Он может быть применен в условиях статистической зависимости неконтролируемых факторов и изменения состояний изучаемого процесса. Данный критерий не требует построения моделей на основе оцениваемых комбинаций факторов, существенно снижает временные и вычислительные затраты для принятия решений в процессе управления роботизированной системой. Его использование позволяет определять, насколько новое наблюдение увеличит осведомленность роботизированной системы о состоянии исследуемого процесса.

Перспективы дальнейших исследований могут заключаться в модификации существующих и разработке новых методов планирования применения роботизированной системы на основе предложенного критерия.

Ключевые слова: *критерий управления; роботизированная система; влияние неконтролируемых факторов; информационный подход.*

V. V. Strinada, M. O. Humeniuk, V. P. Dobrovinskiy, A. O. Tkach

CRITERIA OF MANAGEMENT BY THE ROBOTIC SYSTEM WITH ACCOUNT OF THE INFLUENCE OF NON-CONTROLLED FACTORS

The article proposes a criterion for managing a robotic system, which, based on the information approach, allows to take into account the influence of uncontrolled factors and statistical connections between them in the process of obtaining information.

In this article, the choice of strategy for managing a robotic system in the process of obtaining information provides an indicator that characterizes the effectiveness of management. At the same time, the presence of uncontrolled factors (obstacles, weather conditions, technical malfunctions etc.), which are taken into account in the formal mathematical model of management, leads to the dependence of the efficiency indicator not only on the chosen management strategy, but also on the values of uncontrolled factors. At the same time, both the chosen management strategy and the indicator of the efficiency of the process of obtaining information are functions from uncontrolled factors.

Using the proposed criterion allows you to make the right decisions in the process of managing a robotic system in the event of the influence of uncontrolled factors. The developed criterion can be applied in the conditions of statistical dependence of uncontrolled factors and changes of states of the investigated process. This criterion does not require the construction of models based on evaluated combinations of factors, which significantly reduces the time and computing costs for decision-making in the process of managing a robotic system. Its use allows determining how much new observation will increase awareness of the robotic system in relation to the state of the process being studied.

Prospects for further research may consist of modifying the existing and developing new methods for planning the use of a robotic system based on the proposed criterion.

Keywords: *control criterion; robotic system; influence of uncontrolled factors; information approach.*

ISSN 2076-1546

УДК 004.056 DOI: 10.46972/2076-1546.2019.16.12

О. С. Бойченко, І. В. Гуменюк, Р. І. Гладич

МАТЕМАТИЧНА МОДЕЛЬ ОЦІНКИ РИЗИКУ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ КОРИСТУВАЧАМИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

Стаття присвячена вирішенню актуального науково-практичного завдання – розробці математичної моделі оцінки ризику несанкціонованого доступу до інформації користувачами інформаційно-телекомунікаційної системи. Наведено тлумачення таких понять: несанкціонований доступ до інформації, ризик та оцінка ризику, – які застосовують у ході досліджень внутрішніх загроз. Визначено ознаки користувача інформаційно-телекомунікаційної системи, які впливають на величину ймовірності несанкціонованого доступу до інформації. Показано, що врахування теоретичних та практичних знань користувача інформаційно-телекомунікаційної системи характеристик фізичного середовища, обчислювальної системи, оброблюваної інформації, які він може використовувати для свідомого порушення правил розмежування доступу з метою отримання несанкціонованого доступу до інформації, дозволить більш точно оцінити даний ризик.

Проведено перевірку адекватності розробленої математичної моделі оцінки ризику несанкціонованого доступу до інформації користувачами інформаційно-телекомунікаційної системи за допомогою спеціального програмного забезпечення. Встановлено, що користувачі, які мають найбільший стаж і досвід роботи з інформаційно-телекомунікаційними системами (не тільки в установі, що розглядається), найвищий рівень допуску до інформації з обмеженим доступом, займають відповідальні посади та є недисциплінованими, становлять найбільш імовірну внутрішню загрозу щодо несанкціонованого доступу до інформації. Саме використання математичної моделі оцінки ризику несанкціонованого доступу до інформації користувачами інформаційно-телекомунікаційної системи дозволить удосконалити комплексну систему захисту інформації відповідної інформаційно-телекомунікаційної системи.

Ключові слова: *внутрішні загрози; модель порушника; несанкціонований доступ; потенційні збитки; ризик.*

Постановка проблеми в загальному вигляді. Стрімкий розвиток інформаційних технологій спричинив появу інформаційно-телекомунікаційних систем (ІТС), за допомогою яких автоматизовано процеси накопичення, модифікації, обміну, зберігання інформації. Такий рівень автоматизації роботи зумовлює ризики несанкціонованого доступу (НДС) до неї. Під НДС до інформації в контексті даного дослідження слід розуміти отримання доступу до неї особою, яка має право на це, але в обсязі, що перевищує необхідний для виконання службових обов'язків.

Відповідно до [1] захист інформації від НСД в ІТС полягає в забезпеченні додержання правил розмежовування доступу шляхом створення і підтримки в дієздатному стані системи заходів із захисту інформації.

У сучасних комплексних системах захисту інформації (КСЗІ) модель порушника не враховує в необхідному обсязі можливостей внутрішньої загрози. Тому в ході розробки моделі порушника під час створення КСЗІ постає важливе науково-практичне завдання щодо оцінювання ризику НСД до інформації користувачами ІТС з метою зменшення потенційних збитків від реалізації внутрішніх загроз.

Виникнення цього важливого науково-практичного завдання обумовлено наявною об'єктивною суперечністю між вимогами до зменшення потенційних збитків від внутрішніх загроз та принциповою неможливістю їх врахування через реальну модель порушника, що й визначає своєчасність та актуальність досліджень.

Аналіз останніх досліджень та публікацій. Нормативні документи з технічного захисту інформації (НД ТЗІ) визначають вимоги до захисту інформації від НСД в автоматизованих системах [1−5]. Зокрема в цих документах окремо визначено характеристики фізичного середовища, обчислювальної системи, оброблюваної інформації та користувачів.

Так, у НД ТЗІ [3] наведено категорії користувачів за рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконують у процесі функціонування ІТС. Даний розподіл доцільно враховувати в ході розробки моделі порушника в частині, що стосується внутрішніх загроз.

У відкритих джерелах питанню оцінки ризику НСД до інформації користувачами ІТС не приділено належної уваги, а саме не було запропоновано математичні моделі, які б описували у формалізованому вигляді ймовірність виникнення внутрішніх загроз.

Формулювання завдання дослідження. Метою статті є розробка математичної моделі оцінки ризику НСД до інформації користувачами ІТС з урахуванням таких критеріїв, як: рівень освіти, стаж роботи загальний та в установі (організації), наявність допуску до державної таємниці, посада та кількість дисциплінарних стягнень за поточний рік.

Виклад основного матеріалу. Розмежування доступу користувачів до інформації здійснюється адміністратором безпеки та/або уповноваженим на це співробітником установи (організації) на основі розробленої політики безпеки. При цьому не враховується той факт, що від самого адміністратора безпеки може надходити загроза. Для запобігання цьому пропонуємо математичну модель, яка дозволяє оцінювати ризик НСД до інформації шляхом розрахунку ймовірності реалізації певної загрози від користувача ІТС з належними йому ознаками.

Під ризиком у даному науковому дослідженні слід розуміти кількісну міру безпеки, яка дорівнює добутку ймовірності НСД до інформації користувачем ІТС на ймовірність потенційних збитків унаслідок цього [6, 7]:

$$r = \sum_{i=1}^{N} p_i \cdot w_i, \qquad (1)$$

де N – кількість ознак користувача;

p_i – імовірність НСД до інформації користувачем ІТС за його i -ю ознакою;

w_i – імовірність потенційних збитків унаслідок НСД до інформації відповідним користувачем ІТС з i-ю ознакою.

Відповідно до методології оцінювання ризиків OWASP [8] для визначення втрат використовують якісну шкалу (малий/посередній/великий). Тоді ймовірність потенційних збитків унаслідок НСД до інформації відповідним користувачем ІТС з i-ю ознакою можна описати шляхом ранжування шкали від 0 до 1, отримавши значення, наведені в табл. 1.

Таблиця 1

Імовірність потенційних збитків

Величина потенційних збитків	Імовірність
Мала	$w_1 = 0,33$
Посередня	$w_2 = 0,66$
Велика	$w_3 = 0,99$

Результати аналізу сучасних підходів до формалізованого опису внутрішнього порушника (інсайдера) свідчать про те, що в моделі поведінки внутрішнього порушника не враховані його ознаки, які характеризують мотиви поведінки під час певного виду порушень політики безпеки. При цьому не розглядаються також його теоретичні та практичні знання характеристик фізичного середовища, обчислювальної системи, оброблюваної інформації, які він може використовувати для свідомого порушення правил розмежування доступу з метою отримання НСД до інформації в ІТС [9−11]. Тому в даному дослідженні характеризувати користувача ІТС пропонуємо за певними ознаками. Розглянемо їх детальніше.

1. Рівень освіти. За цією ознакою пропонуємо оцінювати теоретичні знання користувача щодо можливості отримання ним НСД до інформації. Запропоновані рівні освіти користувача ІТС та відповідні їм числові значення, які характеризують імовірність НСД до інформації, наведено в табл. 2.

Таблиця 2

Ознака “Рівень освіти”

Освіта	Значення
Середня	$Ed_1 = 0,1$
Середня спеціальна	$Ed_2 = 0,3$
Середня спеціальна (технічна)	$Ed_3 = 0,7$
Вища	$Ed_4 = 0,5$
Вища (технічна)	$Ed_5 = 0,9$

2. Стаж роботи. За цією ознакою пропонуємо оцінювати знання користувача з організації роботи в ІТС інших установ (організацій). При цьому слід враховувати його досвід роботи з ІТС. Запропоновані рівні трудового стажу та відповідні їм числові значення, які характеризують імовірність НСД до інформації, наведено в табл. 3.

Таблиця 3

Ознака “Стаж роботи”

Стаж	Значення
Відсутній	$Tw_1 = 0,1$
До 1 року (ІТС відсутня)	$Tw_2 = 0,2$
До 1 року (ІТС)	$Tw_3 = 0,5$
До 5 років (ІТС відсутня)	$Tw_4 = 0,3$
До 5 років (ІТС)	$Tw_5 = 0,7$
Більше 5 років (ІТС відсутня)	$Tw_6 = 0,4$
Більше 5 років (ІТС)	$Tw_7 = 0,9$

3. Стаж роботи в установі (організації). За цією ознакою пропонуємо оцінювати ризик НСД до інформації на основі знань користувача з організації роботи в ІТС установи (організації). При цьому потрібно враховувати його досвід праці з ІТС. Запропоновані рівні стажу роботи та відповідні їм числові значення, які характеризують імовірність НСД до інформації, наведено в табл. 4.

Таблиця 4

Ознака “Стаж роботи в установі (організації)”

Стаж	Значення
Відсутній	$Twg_1 = 0,1$
До 6 місяців (ІТС відсутня)	$Twg_2 = 0,2$
До 6 місяців (ІТС)	$Twg_3 = 0,7$
До 1 року (ІТС відсутня)	$Twg_4 = 0,4$
До 1 року (ІТС)	$Twg_5 = 0,8$
Більше 1 року (ІТС відсутня)	$Twg_6 = 0,5$
Більше 1 року (ІТС)	$Twg_7 = 0,9$

4. Допуск до державної таємниці. За цією ознакою пропонуємо оцінювати обізнаність користувача щодо можливості отримання ним НСД до інформації шляхом свідомого порушення організаційних заходів, спрямованих на забезпечення захисту інформації в ІТС. Запропоновані форми допуску до державної таємниці та відповідні їм числові значення, які характеризують імовірність НСД до інформації, наведено в табл. 5.

Таблиця 5

Ознака “Допуск до державної таємниці”

Форма допуску	Значення
Форма 1	$Ts_1 = 0,9$
Форма 2	$Ts_2 = 0,8$
Форма 3	$Ts_3 = 0,7$
Без допуску	$Ts_4 = 0,5$

5. Рівень допуску до інформації з обмеженим доступом установи (організації). За цією ознакою потрібно оцінювати обізнаність користувача щодо характеристик фізичного

середовища, обчислювальної системи, оброблюваної інформації, які він може використовувати для свідомого порушення правил розмежування доступу з метою отримання НСД до інформації в ІТС. Запропоновані рівні допуску до інформації з обмеженим доступом установи та відповідні їм числові значення наведено в табл. 6.

Таблиця 6

Ознака "Допуск до інформації з обмеженим доступом установи (організації)"

Гриф інформації	Значення
Відкрита	$Tsg_1 = 0,2$
Для службового користування	$Tsg_2 = 0,4$
Таємно	$Tsg_3 = 0,6$
Цілком таємно	$Tsg_4 = 0,8$
Особливої важливості	$Tsg_5 = 0,9$

6. Кількість дисциплінарних стягнень за останній рік. За цією ознакою оцінюють стан користувача щодо можливості отримання ним НСД до інформації з метою завдання навмисної шкоди установі (організації). Запропоновані кількість дисциплінарних стягнень за останній рік та відповідні їм числові значення наведено в табл. 7.

Таблиця 7

Ознака "Кількість дисциплінарних стягнень за останній рік"

Кількість	Значення
0	$Dis_1 = 0,1$
1	$Dis_2 = 0,4$
2	$Dis_3 = 0,7$
3 та більше	$Dis_4 = 0,9$

7. Посада користувача в установі (організації). За цією ознакою пропонуємо оцінювати можливості отримання НСД до інформації користувачем відповідно до його владних повноважень в установі (організації). Запропоновані типові посади та відповідні їм числові значення наведено в табл. 8.

Таблиця 8

Ознака "Посада користувача в установі (організації)"

Назва	Значення
Адміністратор безпеки ІТС	$Ra_1 = 0,9$
Адміністратор операційних систем, баз даних, мережевих додатків	$Ra_2 = 0,8$
Начальник структурного підрозділу	$Ra_3 = 0,7$
Технічний обслуговуючий персонал ІТС	$Ra_4 = 0,6$
Розробник програмних засобів для модифікації ІТС	$Ra_5 = 0,6$
Розробник апаратних засобів для модифікації ІТС	$Ra_6 = 0,5$
Технічний персонал (електрики, технічний персонал з обслуговування будівель, ліній зв'язку тощо)	$Ra_7 = 0,3$
Інший персонал установи (організації)	$Ra_8 = 0,1$

У роботі [11] доведено, що інтегровану оцінку можливих втрат за всіма варіантами вибору дає середній ризик. Враховуючи ці результати, середній ризик НСД до інформації користувачем ІТС розраховано за таким виразом:

$$R = \frac{\sum_{i=1}^{N} p_i \cdot w_i}{N}, \tag{2}$$

Для перевірки адекватності математичної моделі оцінки ризику НСД до інформації користувачами ІТС розроблено програмне забезпечення, екранну форму якого наведено на рис. 1.

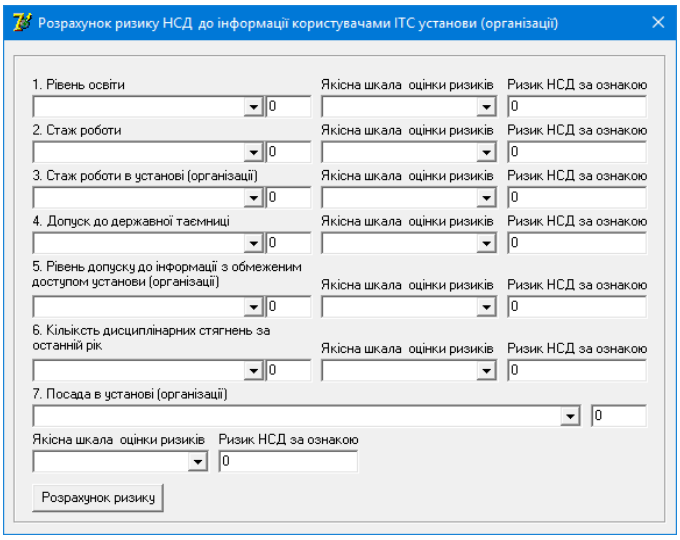


Рис. 1. Екранна форма програмного забезпечення

Перевірку працездатності математичної моделі проведено на прикладах.

Приклад 1. Оцінити ризик НСД до інформації користувачем ІТС, який має певні ознаки, та потенційні збитки:

1. Рівень освіти – “Середня”; величина потенційних збитків – “Мала”.

2. Стаж роботи – “Відсутній”; величина потенційних збитків – “Посередня”.

3. Стаж роботи в установі (організації) – “Відсутній”; величина потенційних збитків – “Посередня”.

4. Допуск до державної таємниці – “Без допуску”; величина потенційних збитків – “Посередня”.

5. Рівень допуску до інформації з обмеженим доступом установи (організації) – “Відкрита”; величина потенційних збитків – “Велика”.

6. Кількість дисциплінарних стягнень за останній рік – “0”; величина потенційних збитків – “Посередня”.

7. Посада в установі (організації) – “Технічний персонал з обслуговування ліній зв’язку”; величина потенційних збитків – “Велика”.

Відповідно до математичної моделі для користувача були обрані числові значення його ознак та розраховано ризик НСД до інформації (рис. 2).

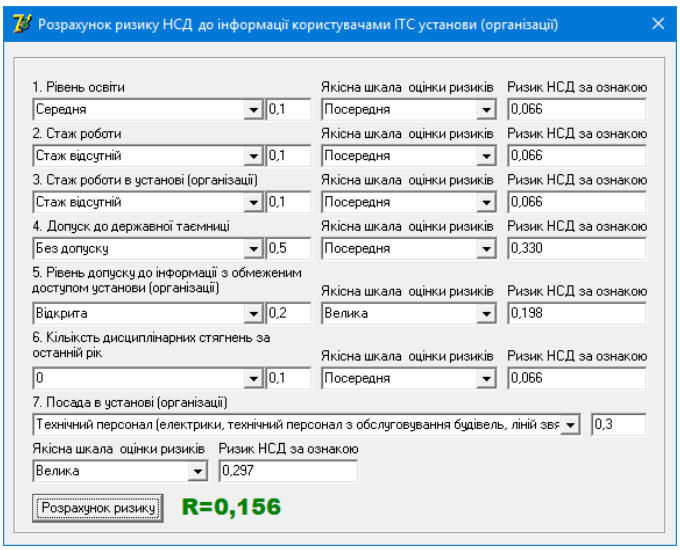


Рис. 2. Результати розрахунку для прикладу 1

Приклад 2. Оцінити ризик НСД до інформації користувачем ІТС, який має такі ознаки:

1. Рівень освіти – “Середня спеціальна технічна”; величина потенційних збитків – “Мала”.

2. Стаж роботи – “До 1 року в іншій установі, де був користувачем ІТС”; величина потенційних збитків – “Посередня”.

3. Стаж роботи в установі – “Відсутній”; величина потенційних збитків – “Посередня”.

4. Допуск до державної таємниці – “Форма 3”; величина потенційних збитків – “Посередня”.

5. Рівень допуску до інформації з обмеженим доступом установи (організації) – “Таємно”; величина потенційних збитків – “Велика”.

6. Кількість дисциплінарних стягнень за останній рік – “2”; величина потенційних збитків – “Посередня”.

7. Посада в установі (організації) – “Технічний обслуговуючий персонал ІТС”; величина потенційних збитків – “Велика”.

Відповідно до математичної моделі для користувача були обрані числові значення його ознак та розраховано ризик НСД до інформації (рис. 3).

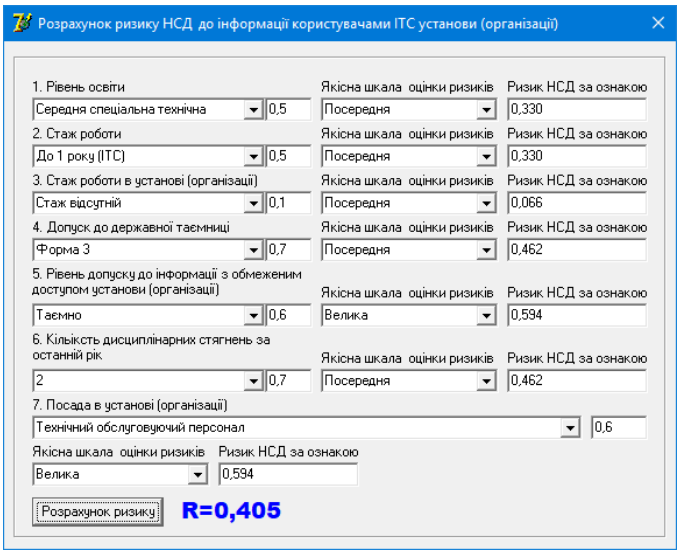


Рис. 3. Результати розрахунку для прикладу 2

Приклад 3. Оцінити ризик НСД до інформації користувачем ІТС, який має такі ознаки:

1. Рівень освіти – “Вища технічна”; величина потенційних збитків – “Посередня”.

2. Стаж роботи – “Більше 5 років в іншій установі, де був користувачем ІТС”; величина потенційних збитків – “Посередня”.

3. Стаж роботи в установі (організації) – “Більше 1 року, користувач ІТС”; величина потенційних збитків – “Посередня”.

4. Допуск до державної таємниці – “Форма 1”; величина потенційних збитків – “Посередня”.

5. Рівень допуску до інформації з обмеженим доступом установи (організації) – “Особливої важливості”; величина потенційних збитків – “Велика”.

6. Кількість дисциплінарних стягнень за останній рік – “3 та більше”; величина потенційних збитків – “Посередня”.

7. Посада в установі (організації) – “Адміністратор безпеки ІТС”; величина потенційних збитків – “Велика”.

Відповідно до математичної моделі для користувача були обрані числові значення його ознак та розраховано ризик НСД до інформації (рис. 4).

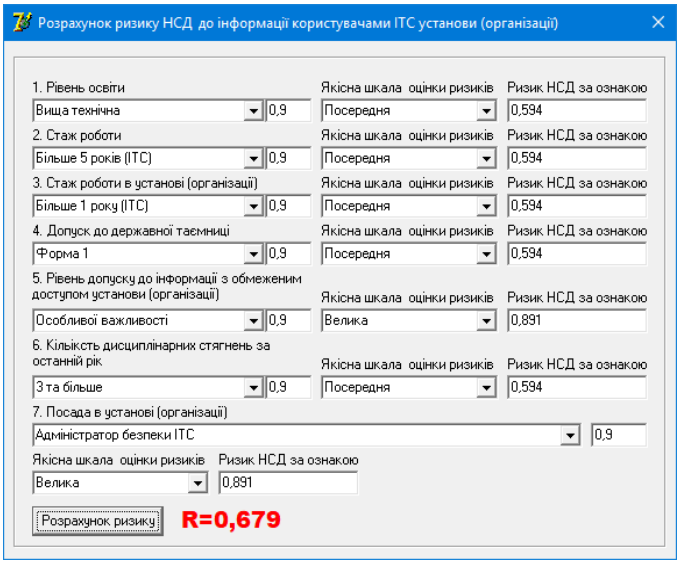


Рис. 4. Результати розрахунку для прикладу 4

Відповідно до отриманих результатів ризик НСД до інформації користувачами ІТС зростає залежно від:

рівня освіти: чим вищий рівень освіти, тим імовірніша загроза від цього користувача;

стажу роботи: чим більший стаж роботи, тим імовірніша загроза від цього користувача;

рівня допуску до державної таємниці та інформації з обмеженим доступом установи (підприємства): чим вище гриф секретності, тим імовірніша загроза;

кількості дисциплінарних стягнень за останній рік: чим їх більше, тим вища ймовірність загрози.

Імовірність виникнення загрози залежно від посади визначають за допомогою методу експертних оцінок.

Висновки. Проведена перевірка адекватності математичної моделі оцінки ризику НСД до інформації користувачами ІТС дозволяє зробити висновки про те, що ті, хто мають найбільший стаж роботи і досвід роботи з ІТС (не тільки в установі, що розглядається), мають найвищий рівень допуску до інформації з обмеженим доступом установи (організації), займають відповідальні посади та є недисциплінованими становлять найбільш імовірну внутрішню загрозу щодо НСД до інформації.

Розроблена математична модель оцінки ризику НСД до інформації користувачами ІТС доповнює модель порушника, зокрема внутрішнього. Саме врахування внутрішніх загроз дозволить вжити додаткові заходи щодо вдосконалення комплексної системи захисту інформації в ІТС.

Математична модель оцінки ризику НСД до інформації користувачами ІТС може застосовуватися як на етапі проєктування КСЗІ в ІТС, так і під час експлуатації з метою зниження рівня внутрішніх загроз.

Подальші наукові дослідження будуть спрямовані на розроблення методичних рекомендацій щодо зниження внутрішніх загроз в ІТС.

СПИСОК ЛІТЕРАТУРИ

1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22. URL: http:// dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden-1&art_id-102106&cat_id=46556&ctime=1344502446343 (дата звернення: 03.06.2019).
2. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-002-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22. URL: http:// dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340 (дата звернення: 03.06.2019).
3. Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. НД ТЗІ 2.5-008-2002 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.12.2002 № 84. URL: https://www.dsszzi.gov.ua/dsszzi/doccatalog/document/id=106343 (дата звернення: 03.06.2019).
4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407 (дата звернення: 03.06.2019).
5. Критерії захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22. URL: https://www.dsszzi.gov.ua/dsszzi/doccatalog/document/id=106342 (дата звернення: 03.06.2019).

6. Rowe W. Ananatomy of risk. New York : Iohn Wiley, 1997. 488 p.
7. Качинський А. Безпека, загрози і ризик: наукові концепції та математичні методи. Київ : Поліграфконсалтінг, 2004, 472с.
8. Managing information security risk: organization, mission, and information system view / Joint task force transformation initiative. URL: http://csrc.nist.gov/publications/detail/sp/800-39/final (last accessed: 25.06.2019).
9. Панченко В. О. Механізм протидії інсайдерам у системі кадрової безпеки // Науковий вісник Львів. держ. ун-ту внутрішніх справ. 2018. № 1. С. 219–227.
10. Рак Ю. П., Сукач Р. Ю. Математична модель оцінки ризику в проектах захисту об'єктів потенційної небезпеки // Управління проектами та розвиток виробництва. 2015. № 2 (54). С. 12–17.
11. Романюков М. Г. Критерії оцінки ймовірності витоку інформації через технічні канали // Інформатика та математичні методи в моделюванні. 2015. Т. 5, № 3. С. 240–248.

Подано 26.06.2019

О. С. Бойченко, И. В. Гуменюк, Р. И. Гладич

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ РИСКА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЯМИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ

Статья посвящена решению актуальной научно-практической задачи – разработке математической модели оценки риска несанкционированного доступа к информации пользователями информационно-телекоммуникационной системы. Приведены толкования таких понятий: несанкционированный доступ к информации, риск и оценка риска, применяемые в ходе исследований внутренних угроз. Определены признаки пользователя информационно-телекоммуникационной системы, которые влияют на величину вероятности несанкционированного доступа к информации. Показано, что учет теоретических и практических знаний пользователя информационно-телекоммуникационной системы о характеристиках физической среды, вычислительной системы, обрабатываемой информации, которые он может использовать для сознательного нарушения правил разграничения доступа с целью получения несанкционированного доступа к информации, позволит более точно оценить данный риск.

Проведена проверка адекватности разработанной математической модели оценки риска несанкционированного доступа к информации пользователями информационно-телекоммуникационной системы с помощью специального программного обеспечения. Установлено, что пользователи, которые имеют самый большой стаж и опыт работы с информационно-телекоммуникационными системами (не только в рассматриваемом учреждении), самый высокий уровень допуска к информации с ограниченным доступом, занимают ответственные должности и являются недисциплинированными, составляют наиболее вероятную внутреннюю угрозу несанкционированного доступа к информации. Именно использование математической модели оценки риска несанкционированного доступа к информации пользователями информационно-телекоммуникационной системы позволит усовершенствовать

комплексную систему защиты информации соответствующей информационно-телекоммуникационной системы.

***Ключевые слова**: внутренние угрозы; модель нарушителя; несанкционированный доступ; потенциальные убытки; риск.*

O. S. Boychenko, I. V. Gumenyuk, R. I. Hladych

MATHEMATICAL MODEL OF ASSESSMENT OF RISK UNAUTHORIZED ACCESS TO INFORMATION BY USERS OF INFORMATION AND TELECOMMUNICATION SYSTEM

The article is devoted to the solution of the actual scientific and practical task – to develop a mathematical model for assessing the risk of unauthorized access to information by users of the information and telecommunication system. Interpretations of such concepts are given: unauthorized access to information, risk and risk assessment used in the course of internal threat research. The characteristics of the user of the information and telecommunication system that affect the value of the probability of unauthorized access to information are determined. It is shown that taking into account the theoretical and practical knowledge of the user of the information and telecommunication system about the characteristics of the physical environment, the computing system, the processed information, which he can use to deliberately violate the rules of demarcation in order to gain unauthorized access to information, will provide a more accurate assessment of this risk.

A verification of the adequacy of the developed mathematical model of risk assessment of unauthorized access to information by users of information and telecommunication system with the help of special software is carried out. It is established that the users who have the most experience and experience with information and telecommunication systems (not only in the institution under consideration), the highest level of access to information with restricted access of the institution (organization), occupy responsible positions and are undisciplined are the most likely internal threat of unauthorized access to information. It is the use of a mathematical model for assessing the risk of unauthorized access to information by users of the information and telecommunication system that will improve the comprehensive information protection system of the corresponding information and telecommunication system.

***Keywords**: internal threats; user violator model; unauthorized access; potential damage; risk.*

УДК 355.421 DOI: 10.46972/2076-1546.2019.16.13

Д. А. Іщенко, В. А. Кирилюк, М. М. Проценко, І. М. Дюков

ОБҐРУНТУВАННЯ ПОКАЗНИКА ЕФЕКТИВНОСТІ РАДІОЕЛЕКТРОННОГО ЗАХИСТУ СИСТЕМИ УПРАВЛІННЯ УГРУПОВАННЯ ВІЙСЬК (СИЛ) ЗА КІЛЬКІСНИМ ПІДХОДОМ ДО ОЦІНЮВАННЯ ЇЇ СТАНУ

У статті наведено порядок оцінювання ефективності заходів радіоелектронного захисту системи управління угруповання військ (сил), що ґрунтується на використанні показника відносного зниження втрат радіоелектронних об'єктів (радіоелектронних засобів). Запропоновано оцінювати ефективність за умовою визначення достатності радіоелектронного захисту системи управління щодо деструктивних впливів противника на її елементи. Розглянуто підхід до визначення достатності радіоелектронного захисту системи управління угруповання військ (сил) в умовах впливу на її елементи засобів вогневого ураження та радіоелектронного подавлення противника. Достатність радіоелектронного захисту встановлюють за досягненням кількості збережених працездатних радіоелектронних засобів, не менше заданої, що забезпечує потрібний рівень організації управління військами (силами) та визначає стан систем управління. Порівнюють стани за кількісним показником.

Зроблено висновок про можливість оцінювання збитку системи управління як частки втрат – кількості непрацездатних радіоелектронних засобів – від загальної кількості радіоелектронних засобів, що складають систему управління. Визначення збитку формалізовано відповідно до вербальних положень нормативних документів. Його визначають за відсотком від загальної кількості радіоелектронних засобів системи управління, втрачених від вогневого ураження (кінетичного впливу), та відсотком від кількості радіоелектронних засобів системи управління, що залишилися після такого ураження, але втрачених від радіоелектронного подавлення (електромагнітного впливу).

Для коректного застосування запропонованого підходу введено обмеження та припущення, що не змінюють фізичного змісту функціонування системи управління та впливу на її елементи засобами вогневого ураження й радіоелектронного подавлення противника. Визначати стан системи управління запропоновано за кількістю працездатних радіоелектронних об'єктів (радіоелектронних засобів), що функціонують у ній за різних умов обстановки.

***Ключові слова**: вогневе ураження; радіоелектронне подавлення; система управління; радіоелектронний об'єкт; радіоелектронний засіб; радіоелектронний захист.*

Постановка проблеми в загальному вигляді. Аналіз досвіду антитерористичної операції та операції Об'єднаних сил показав значущість забезпечення стійкого управління в усіх видах діяльності військ (сил) в умовах прагнення противника до дезорганізації. Розвиток технічної складової систем управління (СУ) в оперативно-тактичній і тактичній ланках спрямовано на покращення управлінської діяльності відповідних органів як необхідну умову підвищення результативності виконання бойових завдань за призначенням військовими частинами і підрозділами. Досягнення переваги в застосуванні СУ стає невід'ємною складовою переваги над противником у всіх видах дій, одночасно її

розвиток супроводжується збільшенням кількості елементів радіоелектроніки в її складі. Сучасна СУ угруповання військ (сил) – це сукупність органів, об'єктів, засобів управління та автоматизації, технічною основою якої є система зв'язку із радіоелектронними об'єктами (РЕОб) та радіоелектронними засобами (РЕЗ), що узгоджено функціонують відповідно до загального алгоритму управління діями військ (сил). Для зменшення кількості працездатних РЕОб та РЕЗ СУ угруповань військ (сил) (далі – РЕЗ СУ) противник використовує сили та засоби вогневого ураження (ВУ) та радіоелектронного подавлення (РЕП).

Результати аналізу бойового досвіду військових частин (підрозділів) Об'єднаних сил у районі виконання завдань свідчать про наявність у противника новітніх засобів ВУ і РЕП та їх достатньо ефективне застосування на території Донецької та Луганської областей. Можливості противника з ВУ та РЕП зумовлюють потребу забезпечення ефективності СУ угруповань військ (сил) на рівні, не меншому заданого, для досягнення переваги в застосуванні СУ в усіх видах дій. Наявність нормативних та ресурсних обмежень на застосування активних засобів боротьби (ВУ та РЕП) для досягнення переваги над противником спричинює актуалізацію проблеми зменшення ступеня дезорганізації управління (ДУ) військами (силами) за рахунок підвищення результативності радіоелектронного захисту (РЕЗт) РЕЗ СУ.

Оцінювання достатності РЕЗт РЕЗ СУ для підтримання стійкого й оперативного управління в умовах ВУ та РЕП є визначальним елементом та первинним науково-практичним завданням, вирішення якого передбачає наявність відповідного науково-методичного забезпечення.

Потрібний для формування обґрунтованих вимог до РЕЗт РЕЗ СУ науково-методичний апарат оцінювання його стану та прогнозованої ефективності має зв'язок із практичними завданнями військ щодо набуття спроможності підтримки засобами радіоелектронної боротьби (РЕБ) відповідно до Єдиного переліку (каталогу) спроможностей Міністерства оборони України та Збройних Сил України [1].

Відсутність науково-методичного апарату визначення достатності РЕЗт РЕЗ СУ обмежує можливості з визначення достатніх заходів для підтримання управління військовими частинами (підрозділами) у разі змін параметрів ВУ та РЕП. Тому обґрунтування показника достатності РЕЗт СУ угруповань військ (сил) за кількісним підходом до оцінювання їх стану як складової відповідного науково-методичного апарату є важливим та актуальним науково-практичним завданням.

Аналіз останніх досліджень і публікацій показав, що елементами теорії захисту СУ, а також РЕЗ, що входять до їх складу, від ВУ та РЕП є результати багатьох наукових досліджень, у тому числі наведені у [2–10]. Крім наукових теоретичних положень у даних публікаціях описано окремі методи та методики, які також можна вважати науково-методичними результатами.

Методичний підхід до вибору та оцінювання показників живучості комплексів в умовах їх ВУ противником, що запропоновано в [2], підтверджує можливість оцінювання стану складних інформаційних систем за кількісними показниками.

Приклад формалізації СУ військового призначення сукупністю РЕЗ в інтересах планування РЕП надано в [3], але запропонований підхід не дозволяє провести оцінювання РЕЗт РЕЗ СУ.

У роботі [4] розглянуто порядок оцінювання ефективності за показниками зазнаних противником збитків з урахуванням втрат, що не дозволяє в повній мірі визначити ефективність заходів РЕЗт.

Підхід до попарного порівняння інформаційно-управляючих систем в інтересах формування вимог до рівня розвитку асиметричних до них систем РЕБ, що надано в [5, 6], враховує зменшення ефективності управління силами та засобами РЕП, але РЕЗт РЕЗ СУ не враховує.

Вимоги нормованості та безрозмірності до оцінювання ефективності, наведені в [7], потребують розроблення математичного апарату проведення перетворень для переходу до безрозмірних коефіцієнтів втрат РЕЗ. Використання положень, запропонованих у [8–10], дозволяє оцінювати ефективність заходів РЕЗт СУ за рахунок використання показника відносного зниження втрат РЕЗ.

У більшості робіт за даною тематикою розглянуто важливі, але лише окремі сторони цієї проблеми – основи побудови технічних систем захисту, що розробляються на етапі створення РЕЗ. Питанням комплексного планування та виконання заходів із метою зменшення ефективності застосування противником засобів ВУ та РЕП не приділено достатньо уваги.

Отже, проведений аналіз останніх досліджень і публікацій за тематикою обґрунтування показника ефективності РЕЗт РЕЗ СУ за кількісним підходом до оцінювання їх стану як складової відповідного науково-методичного апарату дозволяє стверджувати про наявність певних науково-практичних результатів у цій сфері. Проте відомі науково-методичні матеріали мають фрагментарний характер та не пропонують апробованого загального підходу до визначення достатності РЕЗт РЕЗ СУ, що надавав би практичні рекомендації з оцінювання захищеності РЕЗ та визначення достатніх заходів для підтримання управління військовими частинами (підрозділами) в разі змін параметрів ВУ та РЕП. Тому обґрунтування показника оцінювання ефективності РЕЗт РЕЗ СУ є завданням, що не має остаточного вирішення.

Формулювання завдання дослідження. Відповідно до не вирішених раніше частин загальної проблеми завданням дослідження є: оцінювання захищеності СУ від впливу засобів ВУ та РЕП противника; обґрунтування показника оцінювання РЕЗт РЕЗ СУ; розроблення порядку визначення достатності РЕЗт у ході планування РЕБ та її складової РЕЗт в операціях (бойових діях, боях).

Виклад основного матеріалу. СУ розглядається як сукупність органів, об’єктів, засобів управління (автоматизації), технічною основою якої є система зв’язку та формалізується сукупністю РЕЗ, що узгоджено функціонують відповідно до загального алгоритму управління діями військ (сил).

Негативний вплив противника на СУ характеризується кількістю втрачених РЕЗ, виведених з ладу на час ведення дій, за результатами ВУ та РЕП. Величина частки втрачених РЕЗ від їх загальної чисельності, потрібної в СУ для виконання відповідних завдань, визначає ступінь ДУ.

За вимогою відповідності змістовності показника ефективності системи (діяльності) її цільовій спрямованості оцінювання РЕЗт здійснюється як визначення результативності дій для зменшення кількості непрацездатних РЕЗ.

Залежно від величини та характеру збитку сукупності об'єктів, що утворює систему угруповання військ (сил), вона також може бути знищена, подавлена, дезорганізована.

З метою ДУ військами противника протиборчі сторони визначають сили та засоби (підрозділи, військові частини) ракетних військ та артилерії, авіації, РЕБ тощо, які здійснюють дії за призначенням (спеціальні дії, вогневі (ракетні, авіаційні) удари та радіоелектронні впливи), спрямовані на елементи СУ противника.

Введемо обмеження, що противник завдає ВУ та здійснює РЕП лише РЕЗ, які входять до складу СУ.

Загальним для ВУ та РЕП щодо їх впливу на СУ є внесок у загальні втрати (збиток), завдані військами (силами), або втрати РЕЗ СУ за результатами дій противника за рахунок ВУ та РЕП:

$$B = B_{ВУ} + B_{РЕП} + B_{інш}, \quad (1)$$

де B – втрати (загальний збиток), що може бути завданий СУ противником, розрахункові одиниці (од.);

$B_{ВУ}$ – втрати (загальний збиток), що може бути завданий СУ противником за рахунок ВУ (од.);

$B_{РЕП}$ – втрати (загальний збиток), що може бути завданий СУ противником за рахунок РЕП військ (сил) (од.);

$B_{інш}$ – втрати (загальний збиток), що може бути завданий противником за рахунок інших впливів на війська (сили) (од.).

За результатами аналізу відомих підходів до оцінювання втрат (збитку) угруповання (сукупності об'єктів) військ (сил) через рівні зниження їх можливостей із виконання поставлених завдань зроблено висновок про оцінювання збитку СУ як частки втрат – кількості непрацездатних РЕЗ від загальної їх кількості в системі.

Оцінювання ефективності РЕЗт здійснюється через показник відносного зниження втрат РЕЗ угруповання військ (сил) за рахунок виконання заходів РЕЗт:

$$p_{взнв} = \frac{B - B_{РЕЗт}}{B} 100\%, \quad (2)$$

де $p_{взнв}$ – показник відносного зниження втрат РЕЗ СУ за рахунок виконання заходів РЕЗт, розрахункові одиниці;

B – втрати РЕЗ СУ в операціях (бойових діях), якщо заходи РЕЗт не проводяться, розрахункові одиниці;

$B_{РЕЗт}$ – втрати РЕЗ СУ в операціях (бойових діях), якщо заходи РЕЗт проводяться, розрахункові одиниці.

Для того, щоб не використовувати в ході оперативно-тактичних розрахунків (ОТР) розрахункові одиниці, виконаємо певні перетворення та перейдемо до безрозмірних коефіцієнтів втрат РЕЗ СУ різного призначення, класу, типу та відповідної вартості $B = \eta(C)$.

Враховуючи заходи РЕЗт, отримаємо

$$B_{РЕЗт} = \eta_{РЕЗт}\left(C + C_{РЕЗт}\right), \tag{3}$$

де η, $\eta_{РЕЗт}$ – коефіцієнти втрат РЕЗ СУ в бойових діях без виконання заходів РЕЗт та з виконанням заходів РЕЗт відповідно;

C – вартість РЕЗ СУ (потенційних цілей для противника);

$C_{РЕЗт}$ – вартість виконання заходів РЕЗт.

Вважаємо, що $C >> C_{РЕЗт}$, тобто вартість РЕЗ СУ – потенційних цілей для противника – настільки більша за виконання заходів РЕЗт, що $C_{РЕЗт}$ у ході проведення ОТР можна не враховувати. У такому разі показник відносного зниження втрат можна визначити як

$$p_{взнв} = \frac{(\eta - \eta_{РЕЗт}) \cdot C}{\eta C} = 1 - \frac{\eta_{РЕЗт}}{\eta}. \tag{4}$$

Якщо виконання заходів РЕЗт не ефективне, то коефіцієнти втрат однакові $\eta = \eta_{РЕЗт}$, а $p_{взнв} = 0$. Якщо виконання заходів РЕЗт максимально ефективне, то коефіцієнт втрат $\eta_{РЕР} = 0$, а $p_{взнв} = 1$.

Коефіцієнти втрат у бойових діях без виконання заходів РЕЗт та за їх виконання – η, $\eta_{РЕЗт}$, за умови однакової важливості РЕЗ, залежать лише від кількості N збережених (втрачених) об'єктів.

З метою встановлення підходу до визначення показника РЕЗт у кількісному аспекті приймемо припущення:

призначення засобів ВУ (РЕП) противника на РЕЗ здійснюється за принципом "один на один";

у разі призначення засобу ВУ (РЕП) противника на РЕЗ, він робить його непрацездатним (впливає на роботу).

За такого припущення показник відносного зниження втрат РЕЗ СУ за рахунок виконання заходів РЕЗт можна визначити за виразом

$$p_{взнв} = 1 - \frac{N - N_{прРЕЗт}}{N - N_{пр}}, \tag{5}$$

де N – кількість РЕЗ СУ в операціях (бойових діях);

$N_{РЕЗт}$ – кількість працездатних РЕЗ СУ в операціях (бойових діях), якщо заходи РЕЗт проводяться;

$N_{пр}$ – кількість працездатних РЕЗ СУ в операціях (бойових діях), якщо заходи РЕЗт не проводяться;

$N - N_{пр}$ – прогнозований збиток СУ, який визначає, скільки працездатних РЕЗ залишається в СУ за відсутності заходів РЕЗт.

За прийнятими припущеннями, прогнозований збиток СУ, що визначає, скільки працездатних РЕЗ залишається в СУ в разі відсутності заходів РЕЗт, залежить у кількісному аспекті лише від таких параметрів:

N – кількості РЕЗ СУ в операціях (бойових діях);

R – кількості засобів ВУ (РЕП) противника, призначених для ДУ.

У такому разі справедливим є вираз

$$N_{пр} = N - R. \tag{6}$$

Відвернутий за рахунок РЕЗт збиток СУ $N_{від}$, що визначає, на скільки більше працюючих РЕЗ залишається в СУ в разі проведення заходів РЕЗт, можна знайти за такою формулою:

$$N_{від} = N_{прРЕЗт} - N_{пр}. \tag{7}$$

З урахуванням (6) його може бути визначено як

$$N_{від} = N_{прРЕЗт} - \left(N - R\right). \tag{8}$$

Слід зауважити, що відвернутий за рахунок РЕЗт збиток СУ повинен бути не меншим за потрібний: $N_{потр} \geq N_0 - N_{кр}$, а за мінімальною вимогою дорівнювати потрібному:

$$N_{потр} = N_0 - N_{кр}, \tag{9}$$

де $N_{потр}$ – потрібна кількість РЕЗ, збережених в СУ за рахунок РЕЗт. Вона є частиною нереалізованого бойового потенціалу противника за умови, що реалізована його частина не перевищує величини критичного збитку – $N_{кр}$, за якої СУ ще здатна виконувати функціональні завдання;

$N_{кр}$ – мінімальна кількість працездатних РЕЗ, за якої СУ ще здатна виконувати функціональні завдання, – величина критичного збитку СУ;

N_0 – кількість РЕЗ, що можуть стати непрацездатними за рахунок ВУ та РЕП противником – потенційні можливості противника щодо завдання збитку СУ.

Мінімальна кількість працездатних РЕЗ, за якої СУ ще здатна виконувати функціональні завдання, – це величина критичного збитку СУ, яку можна визначати як

$$N_{кр} = \alpha_i N, \tag{10}$$

де α_i – частка (відсоток) працездатних РЕЗ від загальної кількості, припустимої відповідно до ступеня ДУ СУ (утруднення , порушення, зрив).

За прийнятими припущеннями кількість РЕЗ, що можуть стати непрацездатними за ВУ та РЕП противника, може бути визначена як $N_0 = R.$

Потрібну кількість РЕЗ, збережених у СУ за рахунок РЕЗт, (9) з урахуванням (10) можна знайти за такою формулою:

$$N_{прРЕЗт} = R - \alpha_i N. \tag{11}$$

Для визначення потрібного рівня РЕЗт РЕЗ СУ ($p_{взнв}$) через показник відносного зниження їх втрат за рахунок виконання відповідних заходів проведемо перетворення (5), з урахуванням (6), (11) отримаємо такий вираз:

$$p_{взнв} = 2 - \frac{N\left(1+\alpha_i\right)}{R}. \qquad (12)$$

У (12) необхідно розрахувати значення (α_i) частки (відсотка) працездатних РЕЗ від їх загальної кількості в СУ, що припустима відповідно до ступеня ДУ СУ (утруднення, порушення, зрив).

У теорії та практиці військового мистецтва, як правило, встановлюються чисельні показники, за якими визначають загальний рівень спроможностей військового формування – організаційно-технічної системи військового призначення, наприклад: боєздатності, бойової готовності, підготовленості до виконання завдань за призначенням. Оцінювання за такими показниками передбачає визначення певних складових, наприклад: рівня укомплектованості та підготовленості особового складу й техніки.

Відповідно до вербальних положень нормативних документів формалізовано визначення збитку РЕЗ СУ. Він характеризується відсотком від загальної кількості РЕЗ СУ, втрачених від ВУ (кінетичного впливу) та відсотком від кількості тих засобів, що залишилася після ВУ (кінетичного впливу), але втрачених від РЕП (електромагнітного впливу). Шляхом перетворень критичний збиток РЕЗ СУ, за яким визначається певний нормативний ступінь ДУ, можна знайти за таким виразом:

$$N_{кр} = N - Nd_к - \left(N - Nd_к\right) d_е = N - Nd_к - \left(Nd_е + Nd_к d_е\right) = N\left(1 + d_к d_е - d_к - d_е\right) = \alpha_i N, \qquad (13)$$

де N – склад угруповання РЕЗ у СУ (кількість РЕЗ угруповання військ (сил));

$d_к$ – частка втрат зі складу угруповання РЕЗ у СУ від ударів засобів кінетичної дії;

$d_е$ – частка втрат зі складу угруповання РЕЗ у СУ від впливів засобів електромагнітної дії.

За аналізом отриманого показника (10) ефективність РЕЗт РЕЗ залежить від:

N – абсолютної кількості РЕЗ у СУ (кількість РЕЗ може бути збільшена за рахунок резервних);

α_i – заданого ступеня дезорганізації (частини непрацюючих РЕЗ, яку можна збільшити за рахунок зменшення рівнів управління та збільшення ступеня автономності).

Позначимо співвідношення кількості РЕЗ у СУ до засобів ДУ як $K = \frac{N}{R}$ (може бути збільшено за рахунок хибних об'єктів).

Відповідно до (13) значення α_i може бути розраховане за виразом

$$\alpha_i = 1 + d_к d_е - d_к - d_е. \qquad (14)$$

За результатами аналізу (12) визначено необхідність встановлення обмежень для обчислення показника (вимог) ефективності РЕЗт за раніше прийнятими припущеннями та відповідно до чисельних значень α_i, розрахованих для кожного ступеня ДУ.

Знайдемо K для розрахунків максимального – 1 та мінімального – 0 значень показника ефективності РЕЗт РЕЗ СУ, потрібних для недопущення i-го ступеня ДУ за результатами ВУ та РЕП противника:

$$p_{івзнв} = 2 - \frac{N(1+\alpha_i)}{R} = 2 - K(1+\alpha_i). \quad (15)$$

Відповідно для K_{min} та K_{max} отримаємо

$$K_{min} = \frac{1}{(1+\alpha_i)}, \quad (16)$$

$$K_{max} = \frac{2}{(1+\alpha_i)}. \quad (17)$$

Для недопущення ДУ в результаті заходів РЕЗт сили та засоби противника також повинні бути приведені в непрацездатний стан та отримати збиток, адекватний можливому ступеню ДУ (табл. 1).

Таблиця 1

Визначення показника ефективності РЕЗт відповідно до ступенів ДУ

ДУ (відсоток (частка) непрацездатних РЕЗ)			РЕЗт СУ			
			Частка працездатних РЕЗ	Показник (вимога) ефективності РЕЗт		Умови визначення показника (вимоги)
Ступінь ДУ	ВУ РЕОб (не менше) $d_к$	РЕП РЕЗ, що залишилися (не менше) $d_е$	α_i	$p_{взнв} = 2 - \frac{N(1+\alpha_i)}{R}$	Ступінь збитку сил та засобів противника, призначених ним для ДУ	$1 \geq p_{взнв} \geq 0$
Зрив	$d_{кЗ}$	$d_{еЗ}$	$\alpha_З$	$p_{взнвЗ} = 2 - (1+\alpha_З)\frac{N}{R}$	Знищення	$\frac{1}{(1+\alpha_З)} \leq K \leq \frac{2}{(1+\alpha_З)}$
Порушення	$d_{кП}$	$d_{еП}$	$\alpha_П$	$p_{взнвП} = 2 - (1+\alpha_П)\frac{N}{R}$	Подавлення (знищення)	$\frac{1}{(1+\alpha_П)} \leq K \leq \frac{2}{(1+\alpha_П)}$
Утруднення	$d_{кУ}$	$d_{еУ}$	$\alpha_У$	$p_{взнвУ} = 2 - (1+\alpha_У)\frac{N}{R}$	Дезорганізація (подавлення, знищення)	$\frac{1}{(1+\alpha_У)} \leq K \leq \frac{2}{(1+\alpha_У)}$

Фізичний зміст залежності ефективності РЕЗт від співвідношення $K = \frac{N}{R}$ зображено на рис. 1. За відомої (прогнозованої) кількості засобів ДУ $R = const$ у противника, можна варіювати часткою працездатних РЕЗ, що залишаться після ВУ та РЕП, змінюючи загальну їх кількість N. Із рис. 1 видно, що для досягнення потрібної ефективності РЕЗт для недопущення ДУ зі ступенями “утруднення”, “порушення”, “зрив” необхідно забезпечити значення співвідношення кількості РЕЗ у СУ до засобів ДУ у визначених межах.

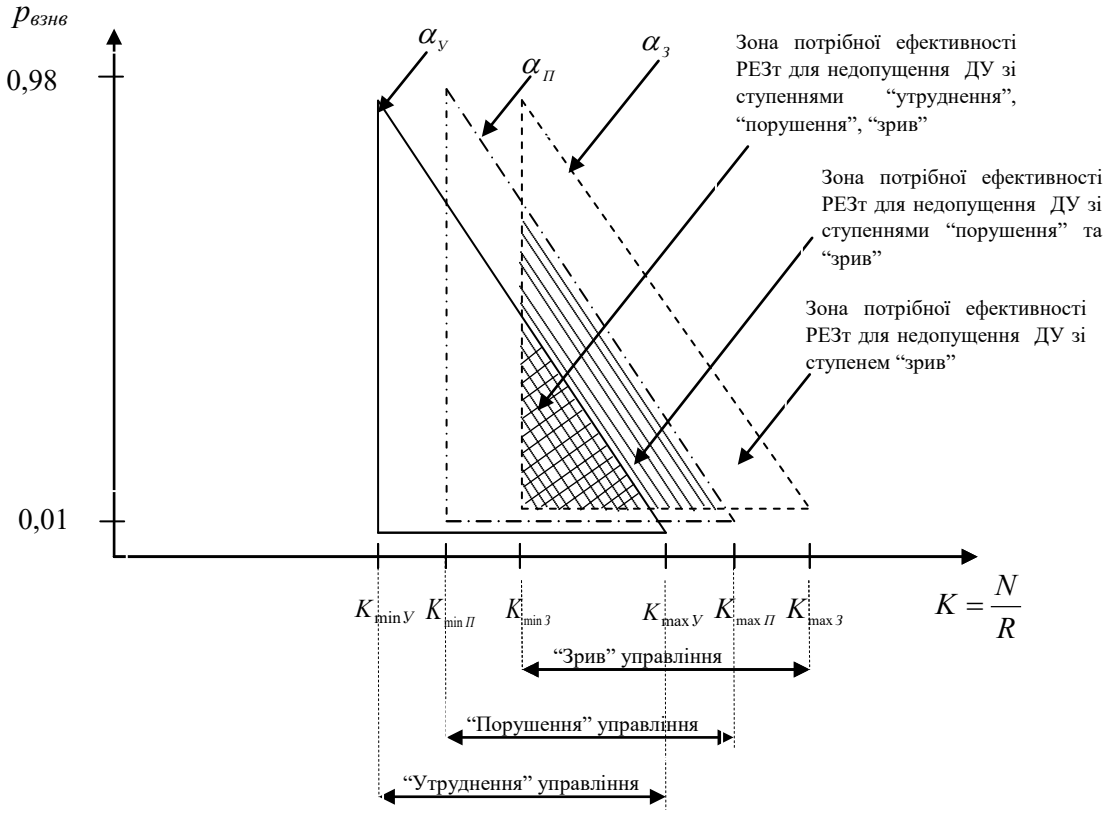


Рис. 1. Залежність показника ефективності РЕЗт від співвідношення кількості РЕЗ у СУ до ДУ

Висновки. У даній статті вирішено завдання обґрунтування показника ефективності РЕЗт СУ військ (сил) у разі впливів на неї засобами ВУ та РЕП. У результаті досліджень встановлено: для зменшення кількості працездатних РЕЗ СУ угруповань військ (сил) протиборчі сторони використовують сили та засоби ВУ та РЕП; застосування активних засобів боротьби (ВУ та РЕП) для досягнення переваги противника обумовлює виникнення проблеми зменшення ступеня ДУ військами (силами) за рахунок підвищення результативності РЕЗт РЕЗ СУ; негативний вплив противника на СУ характеризується кількістю втрачених РЕЗ, приведених у непрацездатний стан на час ведення дій, за результатами ВУ та РЕП; запропоновано оцінювати ефективність РЕЗт СУ через показник відносного зниження втрат.

Перспективним напрямом подальших досліджень є розроблення методичного апарату оцінювання ефективності РЕЗт СУ з урахуванням бойового потенціалу засобів ВУ та РЕП.

СПИСОК ЛІТЕРАТУРИ

1. Єдиний перелік (каталог) спроможностей Міністерства оборони України та Збройних Сил України. URL: www.mil.gov.uanews>20/11/17 (дата звернення: 22.08.2018).

2. Методический поход к обоснованию требований к выживаемости зенитных ракетных комплексов в условиях огневого противодействия противника / Д. Н. Ланецкий, В. В. Лукьянчук, В. В. Лисовенко [и др.] // Наука і техніка Повітряних Сил Збройних Сил України : зб. наук. праць. Харків : ХУПС, 2014. Вип. 2 (15). С. 93–97.

3. Шовкошитний І. І. Методика обґрунтування вихідних даних для оцінювання бойових

можливостей частини радіоелектронної боротьби // Системи озброєння і військова техніка : зб. наук. праць. Київ : ЦНДІ ЗС України, 2008. Вип. 1 (13). С. 136–140.
4. Крюков М. П., Барабаш О. В. Методологічні основи оцінювання ефективності застосування нового виду Збройних Сил – Повітряних Сил та їх об'єднань // Системи озброєння і військова техніка : зб. наук. праць. Київ : НАОУ, 2008. Вип. 3 (15). С. 23–28.
5. Анохин В. А., Михайлов В. В., Ходуенко Д. В. О направлениях сосредоточения усилий в развитии радиоэлектронного вооружения // Военная мысль. 2015. Вип. 12. С. 36–41.
6. Анохин В. А., Михайлов В. В., Ходуенко Д. В. Оценка эффективности функционирования полиэргатических систем управления // Вооружение. 2002. № 2. С. 22–24.
7. Радіоелектронна боротьба в операціях і бойових діях / С. О. Тищук, П. О. Міроненко, Т. Л. Куртсеітов та ін. Київ : НАОУ, 2004. 352 с.
8. Борисов Е. Г., Евдокимов В. И. Высокоточное оружие и борьба с ним : учеб. пособ. Санкт-Петербург : Изд-во "Лань", 2013. 496 с. ISBN 978-5-8114-1441-3.
9. Вайнер А. Я. Тактические расчеты. Москва : Воениздат, 1982. 176 с.
10. Методика оцінювання стійкості радіоелектронних засобів військових об'єктів до впливу зброї електромагнітного імпульсу / Д. А. Іщенко, В. А. Кирилюк, І. А. Павленко та ін. // Проблеми створення, випробовування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2016. Вип. 13. С. 51–61.

Подано 08.07.2019

Д. А. Ищенко, В. А. Кирилюк, М. М. Проценко, И. Н. Дюков

ОБОСНОВАНИЕ ПОКАЗАТЕЛЯ ЭФФЕКТИВНОСТИ РАДИОЭЛЕКТРОННОЙ ЗАЩИТЫ СИСТЕМЫ УПРАВЛЕНИЯ ГРУППИРОВКИ ВОЙСК (СИЛ) ПРИ ИСПОЛЬЗОВАНИИ КОЛИЧЕСТВЕННОГО ПОДХОДА К ОЦЕНКЕ ЕЕ СОСТОЯНИЯ

В статье приведен порядок оценивания эффективности мероприятий радиоэлектронной защиты системы управления группировки войск (сил), основанный на использовании показателя относительного снижения потерь радиоэлектронных объектов (радиоэлектронных средств). Предложено оценку эффективности осуществлять при условии определения достаточности радиоэлектронной защиты системы управления от деструктивных воздействий противника на ее элементы. Рассмотрен подход к определению достаточности радиоэлектронной защиты системы управления группировки войск (сил) в условиях влияния на ее элементы средств огневого поражения и радиоэлектронного подавления противника. Достаточность радиоэлектронной защиты устанавливается по достижению количества сохраненных работоспособных радиоэлектронных средств, не менее заданного, которое обеспечивает необходимый уровень организации управления войсками (силами) и определяет состояние систем управления. Сравнение состояний осуществляется по количественному показателю.

Сделан вывод о возможности оценки ущерба системе управления как доли потерь – количества неработоспособных радиоэлектронных средств – от общего количества радиоэлектронных средств, составляющих систему управления. Определение ущерба формализовано в соответствии с вербальными положениями нормативных документов. Ущерб радиоэлектронных средств системы управления определяется процентом от общего количества их потерь в результате огневого поражения (кинетического

воздействия) и процентом от количества тех, которые остались после такого поражения (кинетического воздействия), но были потеряны от радиоэлектронного подавления (электромагнитного воздействия).

Для корректного применения предложенного подхода введены ограничения и допущения, которые не изменяют физический смысл функционирования системы управления и влияния на ее элементы средствами огневого поражения и радиоэлектронного подавления противника. Определение состояния системы управления предложено осуществлять по количеству работоспособных радиоэлектронных объектов (радиоэлектронных средств), функционирующих в системе в различных условиях обстановки.

Ключевые слова: *огневое поражение; радиоэлектронное подавление; система управления; радиоэлектронный объект; радиоэлектронное средство; радиоэлектронная защита.*

D. A. Ishchenco, V. A. Kyryliuk, M. M. Protsenko, I. M. Diukov

JUSTIFICATION OF THE EFFICIENCY INDICATOR OF THE RADIO ELECTRONIC PROTECTION OF THE COMMAND SYSTEM OF FORCE GROUPING WHEN USING THE QUANTITATIVE APPROACH TO ASSESSING ITS CONDITION

The article describes the procedure for evaluating the effectiveness of radio-electronic protection of the command system of force grouping based on the use of the relative reduction of losses of radio-electronic objects (radio-electronic means). It is suggested to evaluate the effectiveness of the condition of determining the sufficiency of radio-electronic protection of the command system from destructive effects of the enemy on its elements. The approach to determining the sufficiency of radio-electronic protection of the command system of force grouping in the conditions of influence on its elements of fire weapons damage means and enemy radio-electronic suppression is considered. The sufficiency of radio-electronic protection is established upon reaching the number of stored able-bodied radio-electronic means not less than specified, which provides the necessary level of organization of the command system of force and determines the state of the command system. The comparison of states is carried out on a quantitative index.

The conclusion is made about the possibility of estimation of the damage of the command system as the share of losses - the number of incapable radio-electronic means from the total number of radio-electronic means constituting the command system. The determination of the damage to the radio-electronic means of the command system is formalized in accordance with the verbal provisions of the regulations. The damage to the radio-electronic means of the command system is determined by the percentage of its total amount lost from a fire damage (kinetic impact) and the percentage of the amount of radio-electronic means of the command system left after the fire damage (kinetic impact, but lost from radio-electronic suppression (electromagnetic impact).

For the correct application of the proposed approach, restrictions and assumptions have been introduced that do not change the physical meaning of the command system and its effects by means of fire damage and radio-electronic suppression of the enemy. It is suggested to determine the state of the system of management by the number of able-bodied radio-electronic objects (radio-electronic means) operating in the system in different conditions of the environment.

Keywords: *fire damage; radio-electronic suppression; command system; radio-electronic object; radio-electronic means; radio-electronic protection.*

ISSN 2076-1546

УДК 621.396.62 DOI: 10.46972/2076-1546.2019.16.14

О. А. Нагорнюк

СПОСІБ АВТОМАТИЧНОГО ВИЗНАЧЕННЯ НЕСУЧОЇ ЧАСТОТИ КОРОТКОТРИВАЛИХ СИГНАЛІВ ІЗ ЧАСТОТНОЮ МАНІПУЛЯЦІЄЮ

У статті запропоновано спосіб визначення несучої частоти короткотривалих сигналів із частотною маніпуляцією, що ґрунтується на пошуку домінантних гармонік, різниця значень частот яких близька до частоти рознесення піднесучих. У телекомунікаційних системах із пакетними видами передач закон розподілу символів модулюючої послідовності не завжди є рівномірним, що за обмеженої тривалості сигналу призводить до збільшення похибок визначення параметрів частотної маніпуляції. Зростання похибок пов'язано зі спотворенням амплітудно-частотного спектра сигналу та зниженням імовірності правильної ідентифікації гармонік піднесучих коливань. Для покращення точності визначення несучої частоти в запропонованому способі використовується апріорна інформація про значення частоти рознесення піднесучих коливань та кратності маніпуляції. Розроблений підхід полягає в отриманні амплітудно-частотного спектра сигналу, розрахунку порога пошуку домінантних гармонік, визначенні їх частот, що відповідають піднесучим коливанням, та обчисленні несучої частоти як середньоарифметичного їх значення. Для розрахунку спектра сигналу застосовано метод модифікованої періодограми Уелча з низькою дисперсією спектральних оцінок. Поріг пошуку гармонік визначається автоматично на основі статистичних характеристик амплітудно-частотного спектра. Серед гармонік з амплітудами більше порогового значення визначають такі, різниця частот між якими найближча до частоти рознесення піднесучих. Проведені моделювання в програмному середовищі MATLAB показали, що похибка визначення несучої частоти зменшилася удвічі порівняно з класичним підходом за відношення сигнал/шум від -15 дБ*, а розроблений спосіб працездатний у разі ймовірності появи символів модулюючої послідовності від 0,5 до 0,8.*

Ключові слова: *радіосигнал; частотна маніпуляція; параметр; частота; визначення; автоматизація; періодограма; амплітудно-частотний спектр; імовірність.*

Постановка проблеми в загальному вигляді. Визначення параметрів сигналів є першочерговим завданням, яке вирішується в системах радіомоніторингу. Якість його виконання безпосередньо впливає на результати подальшого розпізнавання, демодуляції та пеленгації джерел радіовипромінювання [1]. У сучасних засобах цифрового радіозв'язку часто використовують радіосигнали з частотною маніпуляцією (ЧМн), сформовані в режимі псевдовипадкового перестроювання робочої частоти (ППРЧ) [2]. Для приймання та демодуляції таких сигналів необхідно знати кратність маніпуляції, символьну швидкість, девіацію частоти та несучу частоту. Перші три параметри є однаковими для різних частотних елементів ППРЧ, а несуча частота змінюється з кожним стрибком та має постійно обчислюватися підсистемою визначення параметрів комплексу радіомоніторингу [1]. Розрахунок несучої частоти має низку ускладнень, пов'язаних із широким діапазоном перестроювання робочої частоти, малою тривалістю частотного

елемента та низьким відношенням сигнал/шум (ВСШ). Тому актуальним науково-практичним завданням є удосконалення відомих підходів до визначення несучої частоти ЧМн сигналів з урахуванням особливостей ППРЧ.

Аналіз останніх досліджень і публікацій. Відомі методи та способи визначення несучої частоти ЧМн сигналів ґрунтуються на аналізі характеристик амплітудно-частотного спектра (АЧС), гістограми миттєвої частоти та статистичних параметрів переходів через нульовий рівень. Перший підхід має порівняно низьку розрахункову складність та базується на апробованих методах спектрального аналізу [2–4], другий потребує визначення миттєвої частоти сигналу, що значно збільшує кількість обчислювальних операцій [5], точнісні характеристики третього підходу сильно залежать від ВСШ [6–7]. Загальним недоліком методів є висока похибка розрахунку несучої частоти обмежених за тривалістю сигналів із нерівномірним законом розподілу ймовірностей бітового потоку.

Формулювання завдання дослідження. Метою досліджень є підвищення точності визначення несучої частоти короткотривалих ЧМн сигналів із нерівномірним законом розподілу ймовірностей бітового потоку.

Вхідними даними для способу є комплексні відліки сигнальної суміші, отримані на виході радіоприймального пристрою (РПрП), кратність маніпуляції M та частота рознесення піднесучих f_r. Вважається, що сигнал на передавальній стороні сформовано відповідно до визначених вимог [8], він не комбінований та має один із видів багатопозиційної ЧМн.

Математичну модель сигнальної суміші на виході РПрП можна записати в такий спосіб [8]:

$$r(t) = ae^{j\left(2\pi f_c t+\theta+j\sum\limits_{k=1}^{K}2\pi f_k g(t-kT)\right)} + \xi(t), \tag{1}$$

де $f_k \in \left\{\left(2m-1-M\right)\frac{f_r}{2},\ m=1,...,M\right\},\ k=1,...,K$;

$\{f_k\}_{k=1}^{M}$ – частоти піднесучих кінцевого алфавіту ЧМн;

f_r – частота рознесення піднесучих;

$g(t)$ – імпульсна характеристика формувального фільтра;

M – кратність маніпуляції;

a – амплітуда сигналу;

f_c – частота несучого коливання;

θ – початкова фаза несучого коливання;

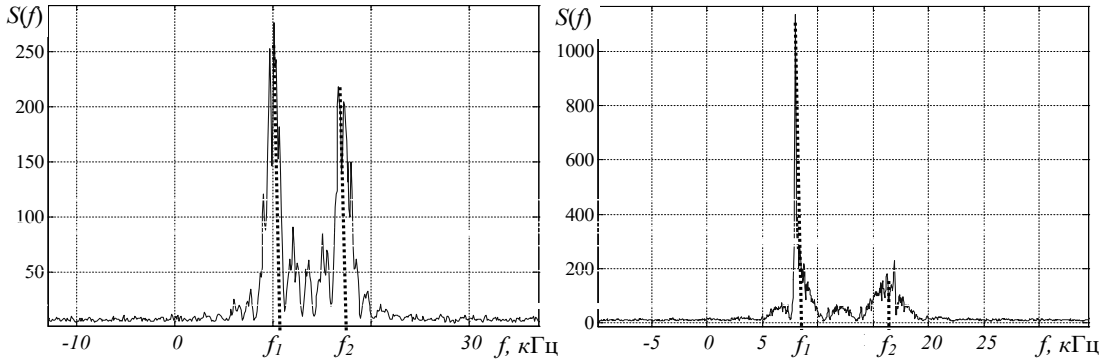
$\xi(t)$ – адитивний гаусівський шум.

Після здійснення операції аналого-цифрового перетворення з частотою дискретизації F_s отримуємо масив комплексних відліків сигналу $r[i]$. Необхідно визначити частоту несучого коливання f_c.

Виклад основного матеріалу. Відомо, що в АЧС ЧМн радіосигналів більшість потужності зосереджено навколо частот гармонік, що відповідають піднесучим коливанням [4, 8]. Дану особливість використано в класичному способі розрахунку

несучої частоти ЧМн сигналів, який полягає у визначенні частот гармонік із максимальною амплітудою та обчисленні несучої частоти як середнього їх значення [9]. Даний підхід працездатний для аналізу ЧМн сигналів, символьна послідовність яких розподілена за рівномірним законом. Однак у короткотривалих ЧМн сигналах (зокрема в каналах, що використовують розширення спектра методом ППРЧ) закон розподілу символів модулюючої послідовності не завжди рівномірний, що призводить до зміни форми АЧС і, як наслідок, збільшення похибки визначення несучої частоти.

На рис. 1 зображено АЧС двопозиційних ЧМн сигналів (ЧМн-2) для випадку рівноймовірного розподілу бітів модулюючої послідовності, а також коли ймовірність появи одного з бітів (“0” або “1”) дорівнює 0,7. Видно, що на рис. 1а АЧС має два близькі за величиною максимуми на частотах f_1 та f_2, а на рис. 1б амплітуда гармоніки АЧС на частоті f_2 у шість разів менша за амплітуду гармоніки на частоті f_1, що знижує ймовірність її правильного виявлення та збільшує похибку визначення несучої частоти.



а) *б)*

Рис. 1. АЧС ЧМн-2 сигналу: а) біти модулюючої послідовності розподілені за рівномірним законом; б) імовірність появи бітів у модулюючій послідовності дорівнює 0,7

Для підвищення ймовірності правильного виявлення домінантних гармонік на частотах f_1 та f_2 пропонуємо використати апріорно відоме значення частоти рознесення піднесучих коливань f_r.

Розроблений спосіб визначення несучої частоти ЧМн сигналів складається із такої послідовності операцій:

обчислення АЧС сигналу;

розрахунок порога пошуку домінантних гармонік;

визначення частот гармонік, що перевищують встановлений поріг;

пошук гармонік, різниця частот яких є найближчою до частоти рознесення піднесучих коливань;

розрахунок несучої частоти.

Схема способу для визначення несучої частоти ЧМн-2 сигналу зображена на рис. 2.

АЧС сигналу $S(f)$ обчислюють методом модифікованої періодограми Уелча (WL), який має низьку дисперсію спектральних оцінок [10] (блок 2). Даний метод ґрунтується на алгоритмі швидкого перетворення Фур’є, що забезпечує легку практичну реалізацію та високу швидкодію. Масив відліків АЧС $S(n)$ формується із дискретністю $F = F_s/N_s$, де N_s – його розмірність.

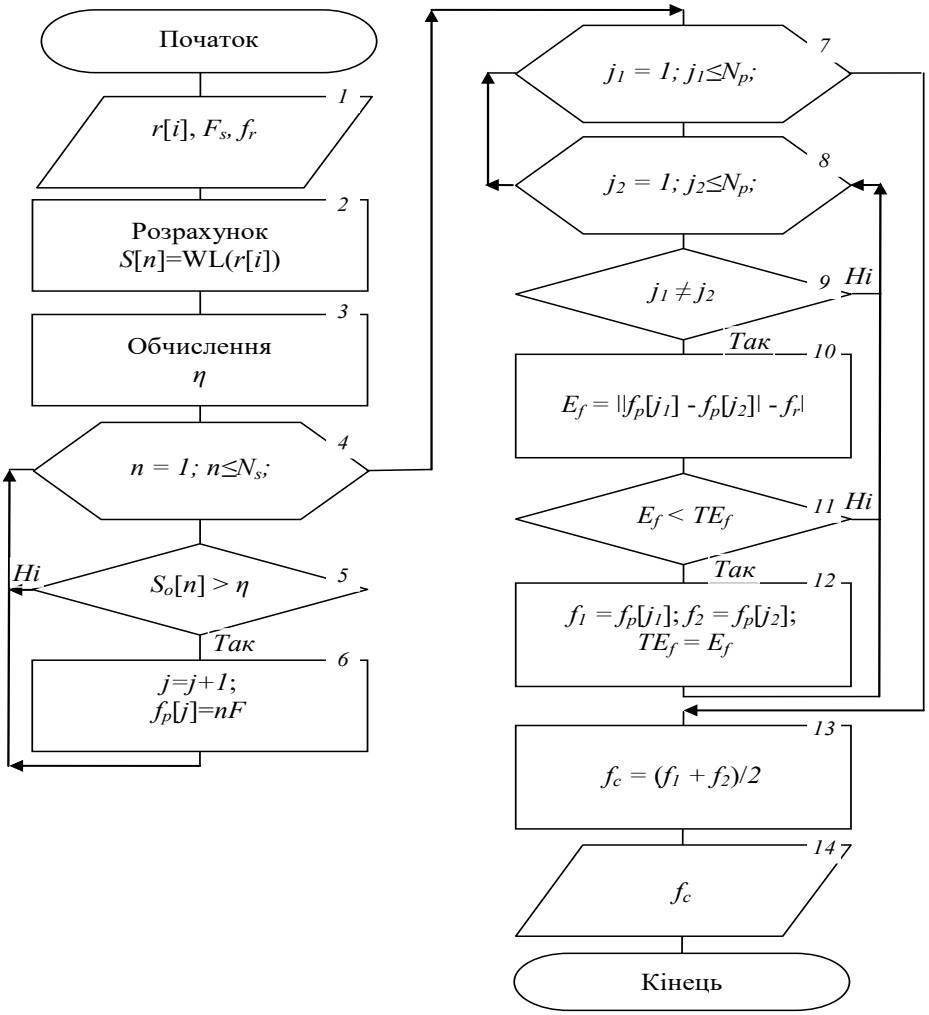


Рис. 2. Схема способу визначення несучої частоти ЧМн-2 радіосигналів

Поріг пошуку домінантних гармонік в АЧС η (блок 3) розраховують за таким виразом:

$$\eta = E\left(S_o(f)\right) + k_s STD\left(S_o(f)\right), \tag{2}$$

де $E()$ – операція обчислення арифметичного середнього;

$STD()$ – операція розрахунку середньоквадратичного відхилення;

$k_s = 1...3,5$;

$S_o(f)$ – АЧС сигналу в діапазоні частот від f_s до f_e:

$$f_s = f_{max} - 2f_r; \;\; f_e = f_{max} + 2f_r, \tag{3}$$

де f_{max} – частота гармоніки з максимальною амплітудою в АЧС $S(f)$.

Пошук гармонік, що перевищують встановлений поріг η (блок 4–6), здійснюємо за критерієм

$$if \; S_o(f_i) > \eta \; then \; f_p[j] = f_i, \; j = 1...N_p, \tag{4}$$

де $f_p[j]$ – масив значень частот домінантних гармонік;

N_p – кількість гармонік.

У масиві $f_p[j]$ присутні частоти, що відповідають піднесучим коливанням ЧМн сигналу. Їх визначають мінімізацією величини E_f (блок 7–12):

$$E_f = \left| \left| f_p[j_1] - f_p[j_2] \right| - f_r \right|;\ j_1 \neq j_2;\ j_1 = 1...N_p;\ j_2 = 1...N_p. \quad (5)$$

Частоти, для яких значення E_f мінімальне, відповідають піднесучим коливанням f_1, f_2 (блок 12), а несучу частоту f_c розраховують як їх арифметичне середнє (блок 13):

$$f_1 \underset{E_f \to min}{=} f[j_1];\ f_2 \underset{E_f \to min}{=} f[j_2];\ f_c = \frac{f_1 + f_2}{2}. \quad (6)$$

Отримані вище математичні вирази наведені для двопозиційної ЧМн. Для М-позиційної ЧМн порядок обчислення несучої частоти ідентичний, змінюються лише вирази (5) та (6):

$$E_f = \sum_{m=1}^{M-1} \left| \left| f_p[j_m] - f_p[j_{m+1}] \right| - f_r \right|;\ j_m \neq j_{m+1};\ j_m = 1...N_p; \quad (7)$$

$$f_c = \frac{\sum_{m}^{M} f_m}{M}, \quad (8)$$

де f_m – частоти піднесучих коливань, які відповідають мінімальному значенню E_f (7).

Дослідження розробленого способу проводили в програмному середовищі MATLAB. На вхід ЧМн-2 модулятора подавали випадкову послідовність з імовірністю появи бітів від 0,5 до 0,8. Вихідний сигнал переносився на задану несучу частоту, до нього додався білий адитивний гаусівський шум. На кожному кроці параметри модулятора та несуча частота змінювалися за випадковим законом. Несучу частоту сформованого сигналу визначали розробленим та класичним способами. Для кожного значення ВСШ здійснювалося 1000 кроків моделювання, а отримані результати усереднювалися.

Дослідження показали, що похибка визначення несучої частоти запропонованим способом залежить від коефіцієнта k_s, який використовується в розрахунку порога пошуку домінантних гармонік. Значення абсолютної похибки визначення несучої частоти ЧМн-2 сигналу Δε від ВСШ для k_s=1…3, 4 та ймовірності появи бітів модулюючої послідовності 0,5 і 0,7 зображено на рис. 3.

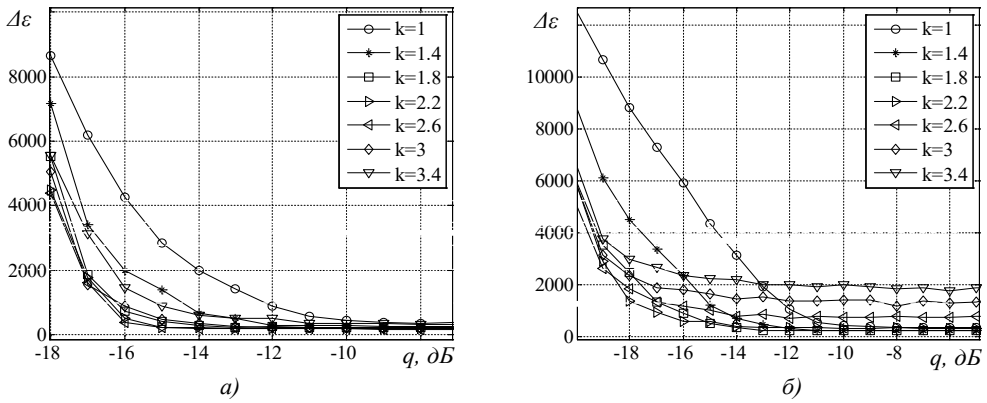


Рис. 3. Залежності абсолютної похибки визначення несучої частоти ЧМн-2 сигналу від ВСШ для значень k_s=1; 1,4; 1,8; 2,2; 2,6; 3; 3,4 та ймовірності появи бітів: а) 0,5; б) 0,6

Із рис. 3 видно, що мінімальні похибки визначення несучої частоти є в разі використання у виразі (2) значення параметра k_s від 1,8 до 2,4. Тому в подальшому було застосовано середнє значення із даного діапазону $k_s = 2{,}2$.

Дослідження ефективності розробленого способу здійснено шляхом його порівняння з класичним способом визначення несучої частоти, який ґрунтується на аналізі АЧС сигналу. Залежності абсолютної похибки визначення несучої частоти двома способами наведено на рис. 4.

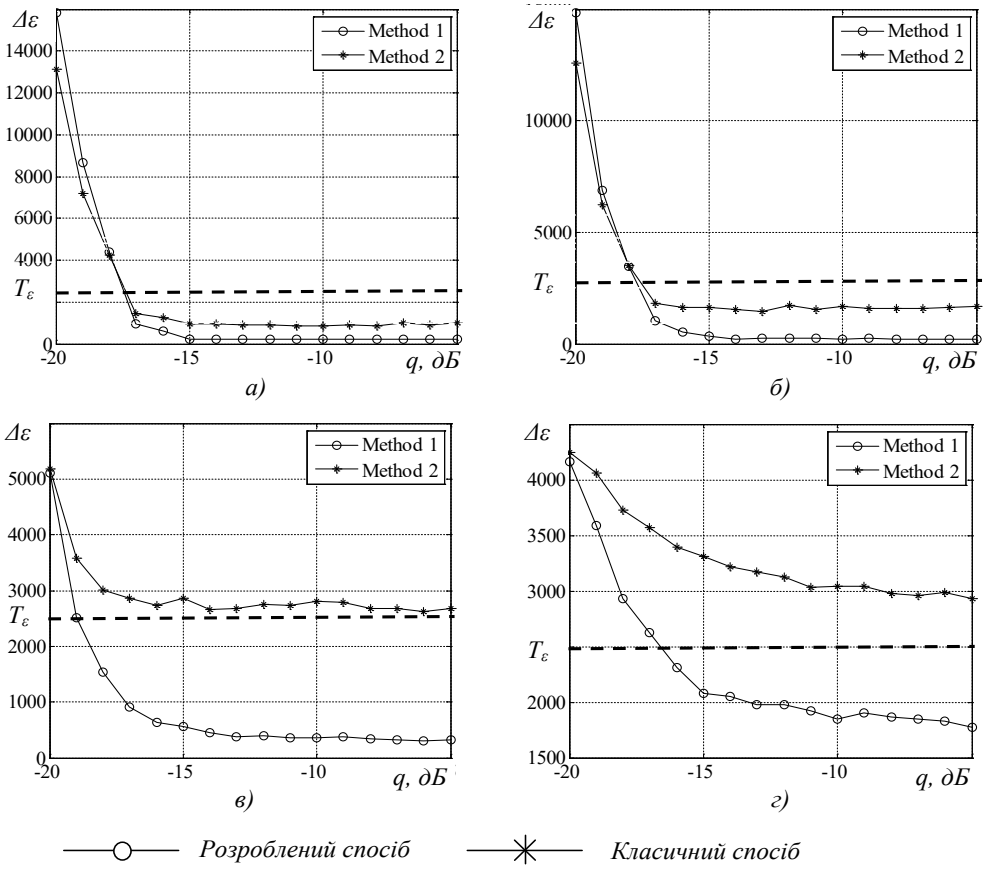


Рис. 4. Абсолютні похибки визначення несучої частоти розробленим та класичним способами для ймовірності появи бітів: а) 0,5; б) 0,6; в) 0,7; г) 0,8

З рис. 4 випливає, що абсолютна похибка визначення несучої частоти класичним способом зростає зі збільшенням імовірності появи бітів у модулюючій послідовності, а за значення ймовірності більше 0,6 класичний спосіб є непрацездатним, оскільки похибка перевищує встановлений поріг T_ε. Абсолютна похибка визначення несучої частоти розробленим способом менше принаймні удвічі від похибки класичного способу за ВСШ від -15 дБ. Вона не перевищує порога T_ε за ВСШ від -16 дБ та ймовірності появи бітів від 0,5 до 0,8.

Обчислювальна складність запропонованого підходу залежить від ВСШ сигнальної суміші, оскільки зі зменшенням ВСШ зростає кількість домінантних гармонік, які перевищують поріг η. У такому разі кількість операцій, розрахованих за формулою (5), дорівнює N_p^2-1. Моделювання показують, що середня кількість домінантних гармонік за ВСШ більше -16 дБ не перевищує $N_p = 8$. Тоді розрахунків за виразом (5) буде 63, що значно менше, ніж кількість операцій, реалізованих на попередніх етапах, зокрема для

обчислення АЧС сигналу. Так, алгоритм швидкого перетворення Фур'є розмірністю 4096 вимагає виконання 49152 операцій. Отже, порівняно з класичним способом обчислювальна складність підвищується несуттєво (не більше 0,2%).

Висновки. Підвищення ймовірності появи символів модулюючої послідовності ЧМн радіосигналу призводить до зміни його АЧС та зростання похибки визначення несучої частоти. Для зменшення похибки запропоновано спосіб, що ґрунтується на пошуку домінантних гармонік в АЧС, різниця частот яких близька до значення частоти рознесення піднесучих коливань. Спосіб потребує апріорної інформації про кратність маніпуляції та частоту рознесення піднесучих, а його обчислювальна складність зростає не більше ніж на 0,2% порівняно із класичним. Похибка визначення несучої частоти розробленим способом у разі ВСШ від -16 дБ не перевищує порогового рівня за ймовірності появи символів модулюючої послідовності від 0,5 до 0,8 та є меншою принаймні удвічі порівняно із класичним підходом.

Подальші дослідження в даному напрямку доцільно спрямувати на удосконалення способу з метою забезпечення його роботи в умовах апріорної параметричної невизначеності.

СПИСОК ЛІТЕРАТУРИ

1. Rembovsky A. M., Ashikhmin A. V., Kozmin V. A., Smolskiy S. M. Radio monitoring: automated systems and their components. Springer international publishing AG. London, 2018. 457 p.

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

3. Technical identification of digital signals. Recommendation ITU-R SM.1600-3. Spectrum management. Geneva, 2017. 32 p.

4. Нагорнюк О. А., Павлюк В. В. Методика автоматизованого розрахунку параметрів частотної маніпуляції в умовах апріорної невизначеності // Сучасні інформаційні технології у сфері безпеки та оборони. Київ, 2016. Вип. 2 (26). С. 74–80.

5. Qin Y., Lv M. A new method of parameter estimation of frequency-hopping signal // 2nd International Conference on Information, Electronics and Computer. Wuhan, 2014. P. 138–141.

6. Xiong H. Zeng D., Xiong H., He X. Parameter estimation approach of FSK/PSK Radar Signal // Journal of electronic science and technology. China, 2010. P. 341–345.

7. De Vito L., Dobre O. A. Joint classification and parameter estimation of compressive sampled FSK signals // 20th IMEKO TC4 international symposium and 18th international workshop on ADC modelling and testing. Benevento, 2014. P. 473–479.

8. Skliar B. Digital communication fundamentals and application. 2nd ed. New-York, 2001. 1072 p.

9. Benvenuto N., Cherubini G. Algorithms for communications systems and their applications. Chichester, 2003. 1285 p.

10. Ifeachor E., Jervis B. Digital signal processing: a practical approach. 2nd ed. Harlow, 2002. 933 p.

Подано 29.07.2019

А. А. Нагорнюк

СПОСОБ АВТОМАТИЧЕСКОГО ОПРЕДЕЛЕНИЯ НЕСУЩЕЙ ЧАСТОТЫ КРАТКОВРЕМЕННЫХ СИГНАЛОВ С ЧАСТОТНОЙ МАНИПУЛЯЦИЕЙ

В статье предложен способ определения несущей частоты кратковременных сигналов с частотной манипуляцией, основанный на поиске доминантных гармоник, разность значений частот которых близка к частоте разнесения поднесущих. В телекоммуникационных системах с пакетными видами передач закон распределения символов модулирующей последовательности не всегда равномерный, что при ограниченной длительности сигнала приводит к увеличению погрешностей определения параметров частотной манипуляции. Рост погрешностей связан с искажением амплитудно-частотного спектра сигнала и снижением вероятности правильной идентификации гармоник поднесущих колебаний. Для улучшения точности определения несущей частоты в предложенном способе используется априорная информация о значении частоты разнесения поднесущих колебаний и кратности манипуляции. Разработанный подход заключается в получении амплитудно-частотного спектра сигнала, расчете порога поиска доминантных гармоник, определении их частот, соответствующих поднесущим колебаниям, и вычислении несущей частоты как их среднеарифметического значения. Для расчета спектра сигнала применен метод модифицированной периодограммы Уэлча с низкой дисперсией спектральных оценок. Порог поиска гармоник определяется автоматически на основе статистических характеристик амплитудно-частотного спектра. Среди гармоник с амплитудами больше порогового значения определяют такие, разность частот между которыми наиболее близка к частоте разнесения поднесущих. Проведенные моделирования в программной среде MATLAB показали, что погрешность определения несущей частоты уменьшилась вдвое по сравнению с классическим подходом при отношении сигнал/шум от -15 дБ*, а предложенный способ работоспособен для вероятности появления символов модулирующей последовательности от 0,5 до 0,8.*

Ключевые слова: *радиосигнал; частотная манипуляция; параметр; частота; определение; автоматизация; периодограмма; амплитудно-частотный спектр; вероятность.*

O. A. Nahorniuk

METHOD OF AUTOMATIC DETERMINATION OF THE CARRIER FREQUENCY OF SHORT-TIME FREQUENCY-SHIFT KEYING SIGNALS

Method for determination of the carrier frequency of short-time frequency-shift keying signals based on searching for dominant harmonics whose frequency difference is close to the subcarrier spacing frequency is proposed in the article. In telecommunication systems with burst transmissions, the symbol distribution law of the modulating sequence is not always uniform, which under a limited signal duration leads to an increase in the errors in determining the frequency-shift keying parameters. The increase in errors is due to distortion of the amplitude-frequency spectrum of the signal and a decrease in the probability of the correct identification of

the subcarrier oscillations harmonics. To improve the accuracy of determining the carrier frequency proposed method uses a priori information about the value of the spacing frequency of the subcarrier oscillations and the multiplicity of frequency-shift keying. The developed approach consists in obtaining the amplitude-frequency spectrum of the signal, calculating the search threshold of dominant harmonics, determining their frequencies which correspond to subcarrier oscillations, and calculating the carrier frequency as their arithmetic mean value. To calculate the signal spectrum was used the modified Welch periodogram method with has a low dispersion of spectral estimates. The harmonic search threshold is determined automatically based on the statistical characteristics of the amplitude-frequency spectrum. Among harmonics with amplitudes greater than the threshold value, those are determined that the frequency difference between which is closest to the subcarrier spacing frequency. The simulations performed in the MATLAB software environment showed that the error in determining the carrier frequency was halved compared to the classical approach under signal-to-noise ratio from -15 dB, and the developed method was efficient if the symbol appearance probability were from 0,5 to 0,8.

Keywords*: radio signal; frequency-shift keying; parameter; frequency; determination; automation; periodogram; amplitude-frequency spectrum; probability.*

УДК 519.21:358 DOI: 10.46972/2076-1546.2019.16.15

Д. А. Іщенко, В. А. Кирилюк, О. М. Наумчак, А. М. Стариков

ПРОГНОЗУВАННЯ ЕФЕКТИВНОСТІ ВОГНЕВОГО УРАЖЕННЯ ПІД ЧАС ОЦІНЮВАННЯ МОЖЛИВОСТЕЙ ПРОТИВНИКА З ДЕЗОРГАНІЗАЦІЇ УПРАВЛІННЯ ВІЙСЬКАМИ

У роботі з урахуванням досвіду проведення антитерористичної операції та операції Об'єднаних сил для забезпечення національної безпеки й оборони, відсічі та стримування збройної агресії Російської Федерації в Донецькій та Луганській областях запропоновано математичний апарат прогнозування ефективності вогневого ураження під час визначення можливостей противника з дезорганізації управління військами. Досліджено питання оцінювання прогнозованого ступеня дезорганізації управління військами (силами) за збитком системі управління, що завдає противник її елементам шляхом застосування засобів радіоелектронного подавлення та вогневого ураження. Оцінювання збитку здійснюється за відносною часткою втрачених (подавлених) об'єктів від їх загальної чисельності в системі управління. Залежно від величини та характеру збитку сукупності радіоелектронних об'єктів і засобів стан системи може бути охарактеризований відповідним ступенем дезорганізації управління: порушення, ускладнення або зрив управління. Для оцінювання збитку сукупності радіоелектронних об'єктів і засобів запропоновано ймовірнісний підхід.

Ступінь дезорганізації за рахунок вогневого ураження визначають з використанням моделі ураження об'єктів системи управління військами, створеної за таких допущень: складний груповий об'єкт подається набором елементарних об'єктів; ураження групового об'єкта визначається відповідно до ступеня ушкодження його складових або критичного елемента; елементарні об'єкти є однорідними за винятком критичних; розподіл координат точки падіння засобу ураження може бути описаний відповідним законом.

На основі аналізу структури об'єктів та можливих ушкоджень запропоновано математичний апарат оцінювання придатності елементарних об'єктів до виконання своїх завдань в умовах вогневого ураження за показниками: знищення, подавлення і дезорганізація. Розроблено модель ураження одиночного (елементарного) та групового військового об'єкта. Вона враховує: склад групового об'єкта, його розміри, розміри елементарних об'єктів; закон розподілу точки падіння засобу ураження за площею; наявність критичних елементарних об'єктів; характеристики засобів вогневого ураження.

Ключові слова: *вогневе ураження; елементарний об'єкт; груповий об'єкт; дезорганізація системи управління; ефективність вогневого ураження.*

Постановка проблеми в загальному вигляді. Аналіз досвіду проведення антитерористичної операції та операції Об'єднаних сил для забезпечення національної безпеки й оборони, відсічі та стримування збройної агресії Російської Федерації в Донецькій та Луганській областях показує, що противник у ході бойових дій зосереджує основні зусилля вогневого ураження (ВУ) та радіоелектронного подавлення

(РЕП) на системі управління військами частин (підрозділів) оперативного угруповання військ з метою забезпечення дезорганізації управління нашими військами (силами). У керівних документах з радіоелектронної боротьби подано ефективність дезорганізації управління військами (силами) противника за принципом визначення частки уражених вогневими засобами та частки РЕП радіоелектронних засобів, що залишилися Планування радіоелектронної боротьби в цілому та радіоелектронного захисту зокрема вимагає чітких та достовірних оцінок стану системи управління своїх військ в умовах РЕП та ВУ. Отримання таких оцінок в умовах певної невизначеності щодо застосування противником засобів ВУ є складним завданням.

Отже, достовірне оцінювання можливостей противника з дезорганізації управління військами потребує вирішення завдання прогнозування ефективності ВУ, що у свою чергу вимагає розроблення математичного апарату, який формалізуватиме способи застосування засобів ВУ та дозволятиме отримати оцінки їх ефективності за умов невизначеності.

Аналіз останніх досліджень і публікацій. У переважній більшості робіт завдання оцінювання ефективності РЕП [1–7] та ВУ [8–12] вирішуються окремо.

Крім того, якщо математичний апарат оцінювання ефективності РЕП в умовах невизначеності опрацьований достатньо повно [1–3], то оцінювання ефективності ВУ в більшості робіт [9–11] здійснено за умов невизначеності окремих характеристик об’єктів ураження, хоча з огляду на захист систем управління інтерес становить питання оцінювання ефективності за умов невизначеності застосування засобів ВУ.

У роботі [9] розглянуто методичний підхід до оцінювання ефективності ураження об’єктів високоточними засобами ураження (ЗУ) з комбінованою дією. Об’єкти і зони ураження подано прямокутниками з відомими лінійними розмірами. Ефективність ураження об’єкта характеризується відносною часткою площі перекриття зон з урахуванням прямого влучення ЗУ в ціль. У [10, 11] запропоновано алгоритми імітаційного моделювання, що дозволяють оцінювати збитки внаслідок різних способів ВУ одиночних і групових об’єктів, у тому числі з урахуванням накопичення збитків, та наведено приклад розрахунку. Алгоритми побудовано на використанні індикаторів попадання елементарних об’єктів у дискретні зони ураження певних типів, що призводить до наявності похибок за рахунок дискретизації зон. У роботі [12] викладено методики оцінювання ефективності ВУ в разі наявності даних про характеристики ЗУ та умови їх застосування, що не завжди відомі під час оцінювання захищеності об’єктів.

Роботи [8, 13] містять детальні методики оцінювання захищеності об’єктів, але їх використання доцільне на етапі їх проєктування. Крім цього, зазначені методики не в повній мірі враховують особливості взаємного розташування елементів групового об’єкта.

Формулювання завдання дослідження. Отже, не вирішеною раніше частиною загальної проблеми оцінювання ефективності ВУ радіоелектронних об’єктів є врахування взаємного розташування елементарних об’єктів у складі групового, їх розподілу за площею, а також оцінювання ефективності за умов невизначеності точки прицілювання.

Отже, потребують вирішення такі завдання:

узгодження якісних і відповідних їм кількісних характеристик ВУ військових об’єктів (одиночних та групових);

визначення ступеня ураження одиночного (елементарного) військового об'єкта;

визначення ступеня ураження групового військового об'єкта.

Відповідно, завданням дослідження є розроблення моделі ураження одиночного (елементарного) та групового військового об'єкта, яка буде враховувати його склад, розміри, розміри елементарних об'єктів, що входять до складу групового; наявність критичних елементарних об'єктів; розташування елементарних об'єктів у складі групового, їх розподіл по площі; характеристики засобів ВУ.

Виклад основного матеріалу. Для оцінювання ефективності ВУ об'єктів використовують підхід, який полягає у визначенні збитку, завданого їм унаслідок вогневого впливу [14]. З погляду радіоелектронного захисту об'єктів збиток полягає у зменшенні боєздатності систем управління військами та зброєю. Зменшення боєздатності (здатності об'єкта виконувати бойові завдання або забезпечувати їх виконання в конкретних умовах бойової обстановки) запропоновано оцінювати ступенем дезорганізації системи управління.

Найчастіше застосовують підхід до визначення ступеня ураження об'єктів (цілей), що передбачає їх однорідність. При цьому збиток асоціюється з кількістю уражених елементарних цілей у складі групового об'єкта або з величиною ураженої частини його площі.

Прийнято вважати, що 50–60% втрат – знищення групового об'єкта, 25–30% втрат – подавлення (обмеження (заборона) діяльності особового складу на об'єкті).

Для військового об'єкта на основі аналізу структури ушкоджень (переліку та складу виведених з ладу агрегатів, вузлів, апаратурних блоків і захисних елементів конструкції) необхідно оцінити придатність елементарних об'єктів до виконання своїх завдань в умовах бойової обстановки. Втрата боєздатності визначається для одиночних об'єктів двома чинниками: знищення і порушення функціонування, а для групових – трьома чинниками: знищення, подавлення і дезорганізація.

Щодо групових об'єктів оперативно-тактичний зміст понять виражається в такий спосіб: знищення – завдання збитку, за якого досягається повна втрата боєздатності; метою подавлення є часткова (тимчасова) втрата боєздатності; у результаті дезорганізації порушується робота органів управління, сил і засобів забезпечення, втрачається мобільність або здатність виконувати бойове завдання в повному складі.

Збиток груповим неоднорідним об'єктам оцінюють за сукупністю даних про втрати елементарних складових. Він характеризується, з одного боку, ступенем тяжкості ушкоджень, а з іншого – переліком (абсолютним або відносним) уражених елементарних об'єктів. Звідси випливає, що метрична шкала вимірювання збитку для групових об'єктів неприйнятна. У зв'язку з цим необхідна порядкова шкала, що визначає міри втрати об'єктами боєздатності: знищення, подавлення, дезорганізація.

Як основні приймаються такі допущення:

кожен складний груповий об'єкт подається набором елементарних цілей;

ураження групового об'єкта визначають відповідно до ступеня ушкодження його складових відповідно до табл. 1;

за наявності у складі групового об'єкта критичної елементарної цілі, її ураження встановлюють відповідно до табл. 2, а визначений тип ураження характерний для всього групового об'єкта;

для кожної елементарної цілі, що входить до групового об'єкта, відомі координати її місця розташування і геометричні розміри.

Таблиця 1

Характеристики ураження групового об’єкта

Тип ураження	Ступінь ушкоджень	Потенційні можливості відновлення
A	Знищення не менше 50% складових	Відновлення не менш ніж за 7 діб
B	Виведення з ладу не менше 50% елементів	Відновлення не менш ніж за 1 добу
C	Середні пошкодження не менше 50% складових	Відновлення не менш ніж за 2-3 години
D	Легкі пошкодження не менше 30% елементів	Відновлення не менш ніж за 1 годину
E	Слабкі пошкодження окремих складових	Відновлення протягом 1 години

Таблиця 2

Характеристики ураження одиночного об’єкта

Тип ураження	Ступінь ушкоджень	Потенційні можливості відновлення
A	Дуже сильні	Відновленню не підлягає (незворотні втрати)
B	Тяжкі	Капітальний ремонт (у стаціонарних ремонтних органах)
C	Середні	Середній ремонт (у військових ремонтних органах)
D	Легкі	Поточний ремонт (силами та засобами частин, підрозділів)
E	Слабкі	Дрібний ремонт (силами екіпажу, розрахунку)

Визначення ступеня ураження одиночного (елементарного) військового об’єкта Імовірність ураження об’єкта за умови прицілювання в його центр, за відсутності систематичних похибок та кругового середньоквадратичного відхилення, визначають за таким виразом [10]:

$$P_{ур\,i} = \left(1 - e^{-\frac{\left(R_{ур} + r_{об\,i}\right)^2}{2\sigma_б^2}}\right), \qquad (1)$$

де $R_{ур}$ – радіус ураження ЗУ;

$r_{об\,i}$ – радіус об’єкта;

$\sigma_б$ – середньоквадратичне відхилення ЗУ.

Імовірність ураження об’єкта за певним типом у разі накриття його круговою зоною ураження з радіусом $R_{ур}$ визначають у такий спосіб [10]:

$$P_{ур\,i(A,B,C,D,E)} = G_{(A,B,C,D,E)}\left(1 - e^{-\frac{\left(R_{ур} + r_{об\,i}\right)^2}{2\sigma_б^2}}\right), \qquad (2)$$

де $G_{(A,B,C,D,E)}$ – умовна ймовірність ураження об'єкта за певним типом.

Визначення ступеня ураження групового військового об'єкта

Групову ціль можна подати у вигляді *N* елементарних цілей, які є функціональними підсистемами (вузлами, агрегатами) вихідного об'єкта. Положення кожного елемента щодо геометричного центра групової цілі $(0,0)$ задається полярними координатами (r_i, φ_i) (рис. 1).

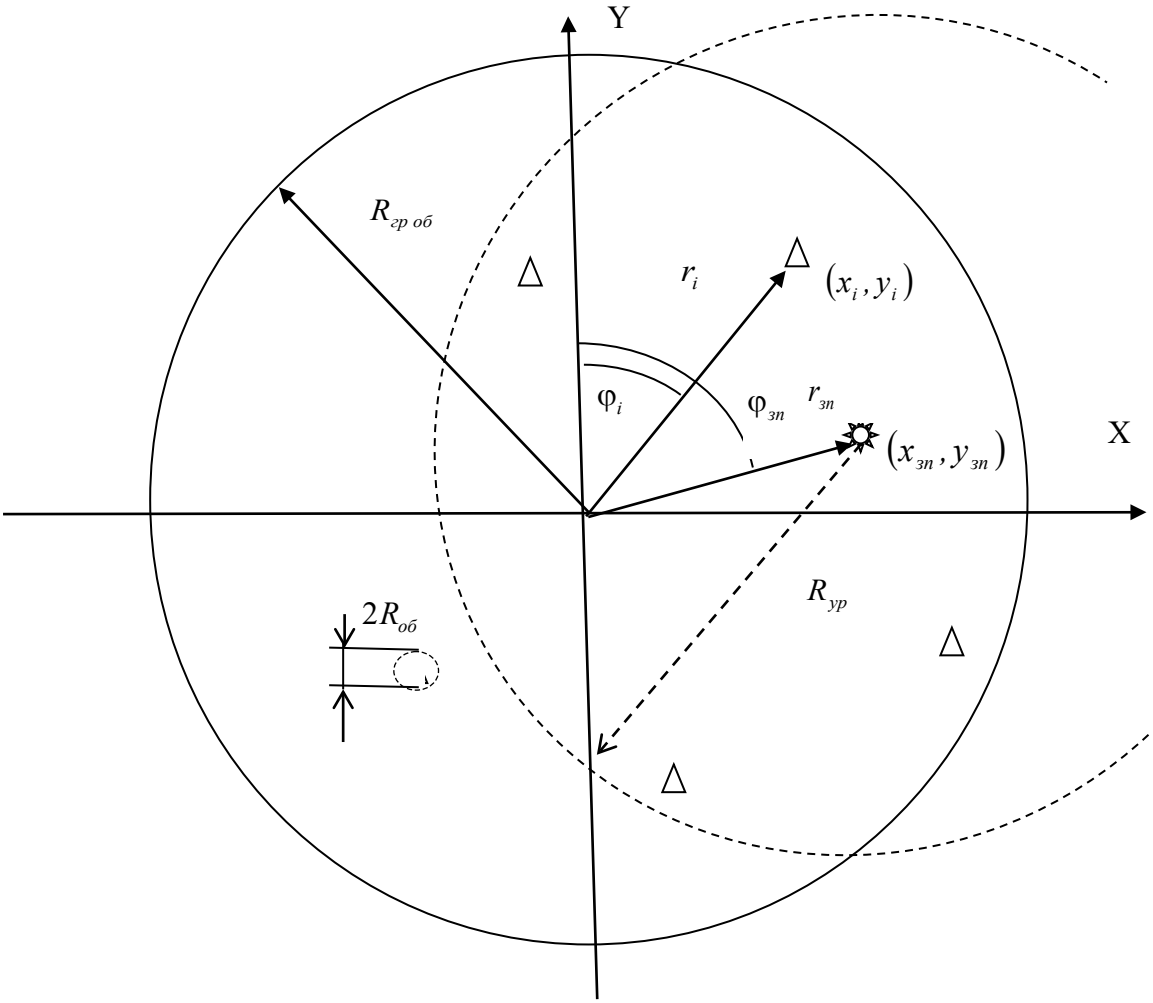


Рис. 1. Схема розташування групового об'єкта

Положення центра кругової зони ураження ЗП задається полярними координатами $(r_{зп}, \varphi_{зп})$. Імовірність ураження цілі в точці (x_i, y_i) у разі падіння ЗП у точку $(x_{зп}, y_{зп})$ приблизно можна оцінити функцією збитку [15]:

$$P^*_{ур\,i}(x_{зп} - x_i, y_{зп} - y_i) = P_{ур\,i} e^{-P_{ур\,i}\left(\left(\frac{x_{зп}-x_i}{R_x}\right)^2 + \left(\frac{y_{зп}-y_i}{R_y}\right)^2\right)}, \quad (3)$$

де R_x, R_y – значення півосей еліпса ураження.

За умови, що $R_x = R_y = R_{ур}$, вираз (3) у полярних координатах матиме такий вигляд:

$$P^*_{ур\,i}(r_{зп}, r_i, \varphi_{зп} - \varphi_i) = P_{ур\,i} e^{-P_{ур\,i}\frac{r_{зп}^2 + r_i^2 - 2r_i r_{зп}\cos(\varphi_{зп} - \varphi_i)}{R_{ур}^2}}. \quad (4)$$

Якщо прицілювання здійснюється в центр групового об'єкта, то ймовірність ураження його елементарної складової визначатимуть за виразом

$$P^{*}_{ур\,i}\left(r_i\right) = P_{ур\,i} e^{-P_{ур\,i}\frac{r_i^2}{R_{ур}^2}}. \tag{5}$$

У випадку, коли точка прицілювання невідома, раціональним є припущення, що координати точки падіння ЗП є випадковою величиною, розподіленою за законом $P_{пр}\left(r,\varphi\right)$. Тоді середня ймовірність ураження елементарного об'єкта, що входить до складу групового, визначатиметься в такий спосіб:

$$P^{*}_{ур\,i}\left(r_i,\ \varphi_i\right) = \int_0^{2\pi}\int_0^{R_{гр\,об}} P_{пр}\left(r,\varphi\right) P_{ур\,i} e^{-P_{ур\,i}\frac{r^2+r_i^2-2r_i r\ cos\left(\varphi\ -\varphi_i\right)}{R_{ур}^2}} dr d\varphi. \tag{6}$$

Для групового об'єкта, що складається з *N* елементарних, отримаємо поле *n*-мірного вектора $\vec{P}^{*}_{ур}$. За максимальним значенням цього вектора в межах площини групового об'єкта оцінюють тип його ураження.

Для рівномірного закону розподілу точки прицілювання за площею групового об'єкта середня ймовірність ураження елементарного об'єкта, що входить до його складу, визначатиметься за таким виразом:

$$P^{*}_{ур\,сер\,i}\left(r_i\right) = \frac{1}{\pi R_{гр\,об}^2}\int_0^{R_{гр\,об}} P_{ур\,i} e^{-P_{ур\,i}\frac{r^2+r_i^2}{R_{ур}^2}} dr. \tag{7}$$

Прирівнявши (2) та (6), отримаємо критерій прийняття рішення *X* про ступінь ураження елементарного об'єкта:

$$\left\{ X = \left\{A,B,C,D,E\right\} \left| \int_0^{2\pi}\int_0^{R_{гр\,об}} P_{пр}\left(r,\varphi\right) e^{-P_{ур\,i}\frac{r^2+r_i^2-2r_i r\ cos\left(\varphi\ -\varphi_i\right)}{R_{ур}^2}} dr d\varphi \in G_{(A,B,C,D,E)} \right. \right\}, \tag{8}$$

а для рівномірного закону розподілу – точки прицілювання за площею групового об'єкта:

$$\left\{ X = \left\{A,B,C,D,E\right\} \left| \frac{1}{\pi R_{гр\,об}^2}\int_0^{R_{гр\,об}} e^{-P_{ур\,i}\frac{r^2+r_i^2}{R_{ур}^2}} dr \in G_{(A,B,C,D,E)} \right. \right\}. \tag{9}$$

За оціненим значенням умовної ймовірності ураження об'єкта за певним типом (8) належить відповідному закону розподілу

$$G_{(A,B,C,D,E)}. \tag{10}$$

Оцінивши тип ураження для всіх *N* елементарних об'єктів відповідно до таблиці 2, приймають рішення про ступінь ураження групового об'єкта.

Приклад розрахунку. Розглянемо груповий об'єкт розміром $2R_{ур}$, який складається з п'яти однорідних елементарних об'єктів розміром $0{,}1R_{ур}$, розміщених на відстані від центру групового об'єкта на відстанях $0{,}1R_{ур}$; $0{,}3R_{ур}$; $0{,}5R_{ур}$; $R_{ур}$ $1{,}5R_{ур}$. Вважатимемо, що середньоквадратичне відхилення ЗУ становить $\sigma_б = 0{,}3R_{ур}$. Імовірність ураження елементарного об'єкта в разі прицілювання в його центр, розрахована за виразом (1), – 0,999. Значення ймовірності ураження елементарних об'єктів у разі прицілювання в центр групового, розраховане за (5), наведено в табл. 3.

Таблиця 3

Значення ймовірності ураження елементарних об'єктів у разі прицілювання в центр групового

Відстань	$0{,}1R_{ур}$	$0{,}3R_{ур}$	$0{,}5R_{ур}$	$R_{ур}$	$1{,}5R_{ур}$
Імовірність ураження	0,989	0,913	0,778	0,368	0,106

За умови, що функція розподілу умовної ймовірності ураження об'єкта за певним типом має вигляд, наведений у табл. 4, приймають рішення, що два елементарні об'єкти будуть уражені за типом А, один – за типом С, решта – не уражені. Отже, за наведених умов груповий об'єкт відповідно до табл. 1, 2 прогнозовано буде уражений за типом В.

Таблиця 4

Функція розподілу умовної ймовірності ураження об'єкта за певним типом

Тип ураження	A	B	C	D	E
Імовірність ураження	1–0,9	0,89–0,8	0,79–0,7	0,69–0,6	0,59–0,5

Висновки. У роботі запропоновано математичний апарат оцінювання ефективності ВУ радіоелектронних засобів, які описані моделями одиночного та групового об'єктів. Отримано аналітичні вирази для оцінювання ймовірностей ураження об'єктів для параметрів, що визначають просторове положення елементарних об'єктів, закон розподілу точки падіння ЗУ, його характеристики. Розроблено модель ураження одиночного (елементарного) та групового військових об'єктів. Модель враховує: склад групового об'єкта, його розміри, розміри елементарних об'єктів; закон розподілу точки падіння ЗУ за площею; наявність критичних елементарних об'єктів; характеристики засобів ВУ.

Наукова новизна наведених результатів полягає у врахуванні взаємного розташування елементарних об'єктів у складі групового, їх розподілу по площі, а також оцінюванні ефективності за умов невизначеності точки прицілювання.

Напрямком подальших досліджень буде оптимізація розміщення елементарних об'єктів за критерієм мінімізації ефективності їх ВУ противником.

СПИСОК ЛІТЕРАТУРИ

1. Журавський Ю. В. Оцінювання ефективності радіоподавлення в умовах невизначеності координат приймачів // Системи обробки інформації : зб. наук. праць. Харків : ХУПС, 2009. № 76 (2). С. 45–47.

2. Журавський Ю. В. Оцінювання ефективності радіоподавлення в умовах похибок визначення координат передавача сигналу // Військово-технічний збірник Академії

сухопутних військ ім. гетьмана Петра Сагайдачного : зб. наук. праць. Львів : АСВ, 2012. № 7 (2). С. 63–68.

3. Журавський Ю. В., Даник Ю. Г. Оцінювання ефективності радіоелектронного подавлення в умовах похибок визначення координат передавача та приймача сигналу // Зб. наук. праць ВІТІ НТУУ КПІ. Київ : ВІТІ НТУУ КПІ, 2012. № 2. С. 44–49.

4. Іщенко Д. А. Методика оцінювання стійкості радіоелектронних засобів військових об’єктів до впливу зброї електромагнітного імпульсу // Проблеми створення, випробовування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2016. Вип. 13. С. 51–61.

5. ВСТ 01.104.002. Боротьба радіоелектронна. Радіоелектронний захист. Захист радіоелектронних засобів від ураження електромагнітною зброєю противника. Захист радіоелектронних засобів та радіоелектронних пристроїв військових об’єктів від впливу зброї електромагнітного імпульсу. Основні організаційні та технічні вимоги. Житомир : ЖВІ, 2015. 21 с.

6. Кирилюк В. А., Іщенко Д. А., Стариков А. М. Науково-методичний апарат оцінювання захищеності радіоелектронних засобів військового призначення від впливу електромагнітної зброї // Проблеми створення, випробовування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2016. Вип. 15. С. 143–155.

7. Журавський Ю. В., Кирилюк В. А., Іщенко Д. А. Програмно-алгоритмічне забезпечення з оцінювання захищеності радіоелектронних засобів від впливу електромагнітної зброї // Труди Університету. Київ : НУО України, 2018. № 150. С. 67–74.

8. Сурин Д. В. Аналитические методы оценки защищенности и живучести объектов и комплексов. Москва : МО РФ, 1997 . 144 с.

9. Буравлев А. И. Методика оценки вероятности поражения размерных объектов высокоточными средствами поражения // Вооружение и экономика : электрон. науч. журн. 2012. № 2 (18). С. 10–14.

10. Буравлев А. И., Брезгин В. С. Методика оценки ущерба при имитационном моделировании огневого поражения объектов // Вооружение и экономика : электрон. науч. журн. 2012. № 5 (21). С. 13–21.

11. Буравлев А. И., Брезгин В. С. Об оценке эффективности поражения высокоточным оружием объектов военно-экономического потенциала // Вооружение и экономика : электрон. науч. журн. 2013. № 1 (22). С. 16–20.

12. Оценка эффективности огневого поражения ударами ракет и огнем артиллерии. Военно-теоретический труд / Под ред. А. А. Бобрикова. Санкт-Петербург : Академия военных наук, 2006. 421 с.

13. Методика обоснования требуемого уровня стойкости оборудования сетей связи в условиях внешних деструктивных воздействий / С. С. Семенов, А. С. Белов, В. С. Воловиков, А. В. Скубьев // Системы управления, связи и безопасности. 2019. № 1. С. 33–53.

14. Исламов В. К., Самсонов А. М. О теории огневого поражения // Военная мисль. 1992. № 3. С. 18–23.

15. Бондаренко Д. Л. Площадная модель воздействия на информационно-вычислительный комплекс АСУ // Математическая морфология : электрон. математ. и медико-биолог. журн. 2011. Т. 10. Вып.4. С. 4–8.

Подано 31.07.2019

Д. А. Ищенко, В. А. Кирилюк., Е. М. Наумчак, А. М. Стариков

ПРОГНОЗИРОВАНИЕ ЭФФЕКТИВНОСТИ ОГНЕВОГО ПОРАЖЕНИЯ ПРИ ОЦЕНКЕ ВОЗМОЖНОСТИ ПРОТИВНИКА ПО ДЕЗОРГАНИЗАЦИИ УПРАВЛЕНИЯ ВОЙСКАМИ

В работе с учетом опыта проведения антитеррористической операции и операции Объединенных сил для обеспечения национальной безопасности и обороны, сдерживания вооруженной агрессии Российской Федерации в Донецкой и Луганской областях предложен математический аппарат прогнозирования эффективности огневого поражения при оценке возможностей противника по дезорганизации управления войсками. Исследован вопрос оценки прогнозируемой степени дезорганизации управления войсками по ущербу системе управления, который наносит противник ее элементам путем применения средств радиоэлектронного подавления и огневого поражения. Определение ущерба осуществляется по относительной доле утраченных (подавленных) объектов от их общей численности в системе управления. В зависимости от величины и характера состояние системы может быть охарактеризовано соответствующей степенью дезорганизации управления: нарушения, затруднения или срыва управления. Для оценки ущерба совокупности радиоэлектронных объектов и средств предложен вероятностный подход.

Степень дезорганизации за счет огневого поражения определяют с использованием модели поражения объектов системы управления войсками, созданной при таких допущениях: сложный групповой объект подается набором элементарных объектов; поражения группового объекта определяется в соответствии со степенью повреждения составляющих или критического элемента; элементарные объекты являются однородными за исключением критических; распределение координат точки падения средства поражения может быть описано соответствующим законом.

На основе анализа структуры объектов и возможных повреждений предложен математический аппарат оценки пригодности элементарных объектов к выполнению своих задач в условиях огневого поражения по показателям: уничтожение, подавление и дезорганизация. Разработана модель поражения одиночного и группового военного объекта. Она учитывает состав группового объекта, его размеры, размеры элементарных объектов; закон распределения точки падения средства поражения по площади; наличие критических элементарных объектов; характеристики средств огневого поражения.

Ключевые слова: *огневое поражение; элементарный объект; групповой объект; дезорганизация системы управления; эффективность огневого поражения.*

D. A. Ishchenko, V. A. Kyrylyuk, O. M. Naumchak., A. M. Starykov

FORECASTING THE EFFICIENCY OF THE FIRE DAMAGE IN ASSESSING THE ENEMY'S ABILITY TO DISRUPT THE MANAGEMENT OF TROOPS

In the work the mathematical apparatus for forecasting the effectiveness of fire damage was proposed in assessing the enemy's ability to disarm the troop management with taking into account the experience of the antiterrorist operation and the Joint Forces Operation in order to provide national security and defense, repression and deterrence of armed aggression of the Russian Federation in the Donetsk and Luhansk oblasts. The question of estimating the predicted degree of disorganization of the

troops management by the damage for management system, that the enemy causes to its elements using the means of radio-electronic suppression and fire damage, is researched. The assessment of the loss is based on the relative proportion of the lost (suppressed) objects from their total number in the management system. Depending on the size and nature of the damage to the totality of radio-electronic objects and means, the state of the system can be estimated by the appropriate degree of disorganization: disturbance, difficulty or disruption of management. A probabilistic approach is proposed for evaluating the loss of a set of radio-electronic objects and means.

The degree of disorganization due to fire damage is estimated using the model of defeat of the objects of the troops management system. The model of fire damage is created with the following assumptions: a group object is given by a set of elementary objects; the defeat of the group object is determined according to the degree of damage to the elements or the damage to the critical element; elementary objects are homogeneous with the exception of critical elements; the distribution of the point of the fall of the lesion may be described by the relevant law.

On the basis of the analysis of the structure of objects and possible damage, a mathematical apparatus for evaluating the suitability of elementary objects for performing their tasks in conditions of fire damage was proposed based on indicators: destruction, suppression and disruption. A model of defeat of a single (elementary) and a group military object was developed. The model takes into account: the composition of the group object, its size, the size of elementary objects; the law of the distribution of the point of falling of the means of defeat by the area; the presence of critical elementary objects; characteristics of fire damage.

Keywords: *fire damage; elementary object; group object; disorganization of management system; efficiency of fire damage.*

УДК 32.019.5:351.86 DOI: 10.46972/2076-1546.2019.16.16

Ю. І. Міхєєв, О. В. Критенко

АВТОМАТИЗАЦІЯ ПРОЦЕСУ СТВОРЕННЯ МАТЕРІАЛІВ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

У статті розглянуто процес створення матеріалів інформаційно-психологічного впливу. Наведено характеристики, які необхідно враховувати під час розроблення таких матеріалів. Запропоновано також алгоритм аналізу цільової аудиторії, що є основним об'єктом для реалізації підтримувальної цілі психологічної операції (акції). Даний алгоритм передбачає послідовне виконання таких етапів: визначення та уточнення характеристик цільової аудиторії; розрахунок її ефективності; виявлення причин та наслідків її наявної поведінки; опис вразливостей; визначення сприйнятливості; розроблення аргументів та рекомендацій для психологічної операції (акції); уточнення первинних критеріїв оцінювання цільової аудиторії тощо.

Наведено структурну схему алгоритму автоматизації процесу створення матеріалів інформаційно-психологічного впливу. Згідно з ним розроблено спеціалізоване програмне забезпечення, що передбачає покрокове заповнення відповідних пунктів програми з урахуванням методології, яку використовують у підрозділах психологічних операцій (акцій) Збройних сил НАТО. Слід зауважити, що результатом роботи спеціалізованого програмного забезпечення є концепт створення друкованого продукту інформаційно-психологічного впливу.

Крім того, на етапі оформлення дизайну друкованої продукції інформаційно-психологічного впливу використовується база даних, у якій знаходяться як приклади вже готові матеріали та довідкова інформація. Наповнення бази даних відбувається за *двома групами критеріїв: перша характеризує психологічну (маніпулятивну) складову матеріалу інформаційно-психологічного впливу, друга – правила його оформлення з погляду сприйняття (привернення уваги) цільової аудиторії.*

Ключові слова: *інформаційно-психологічний вплив; цільова аудиторія; психологічна операція (акція); алгоритм; інформаційна загроза.*

Постановка проблеми в загальному вигляді. В умовах ведення гібридної війни важливу роль відіграє організація заходів із протидії негативним інформаційно-психологічнним впливам (ІПсВ). Одним із дієвих заходів протидії є виготовлення та поширення власних матеріалів ІПсВ, завдяки яким досягається бажана поведінка цільової аудиторії (ЦА), на яку вони спрямовані. Особливістю розроблення матеріалів ІПсВ є необхідність глибокого та всебічного вивчення обраного об'єкта, урахування його психологічних та соціально-психологічних характеристик, групової належності, національної та релігійної специфіки, морально-психологічного стану, соціально-політичної ситуації в державі, а також інших факторів [1–3], що потребує залучення значних часових ресурсів.

Усе це стосується й наочної продукції, яка призначена для впливу на поведінку ЦА за допомогою візуальних (текстових або графічних) матеріалів і залишається одним із основних визначальних чинників, особливо в умовах зруйнованої інфраструктури в зоні проведення бойових дій.

Аналіз досвіду виконання завдань із розроблення друкованої продукції ІПсВ спеціальними підрозділами Збройних Сил (ЗС) України під час виконання бойових завдань у зоні проведення антитерористичної операції та операції Об'єднаних сил свідчить про те, що оперативність підготовки таких матеріалів належної якості значно знижується.

Аналіз останніх досліджень і публікацій за даною тематикою свідчить про те, що більшість авторів приділяють увагу питанню створення матеріалів рекламного характеру та реалізації в них технологій привернення уваги споживачів. Так, у [4] вирішують завдання з вибору та реалізації методів і механізмів маніпуляції суспільною думкою в рекламі. У [5] розглянуто технології створення друкованої реклами, у [6] – окремі технічні аспекти розроблення контенту, при цьому особливості його ІПсВ на ЦА враховано не в повному обсязі. Результати аналізу джерел свідчать про те, що на сьогодні відсутній комплексний підхід з автоматизації розроблення спеціального контенту, який би враховував особливості планування та проведення заходів протидії негативним ІПсВ.

Досвід провідних країн НАТО з підготовки та проведення психологічних операцій (психологічних акцій) (ПсО (ПсАк)) показав, що найкращим підходом до виготовлення продукції є розподіл завдань між військовими та цивільними фахівцями. Військові під час підготовки до спеціальних дій за встановленою методикою розробляють концепт матеріалу ІПсВ, після чого цивільні – безпосередньо сам матеріал [3]. В умовах виконання бойових завдань у зоні проведення операції Об'єднаних сил увесь цикл розроблення спеціального контенту спеціальними підрозділами ЗС України покладається на військових фахівців. Тому **метою даної роботи** є підвищення якості розроблення друкованих матеріалів ІПсВ за рахунок визначення основних етапів цього процесу та їх автоматизації.

Виклад основного матеріалу. Автоматизація процесу створення друкованої продукції ІПсВ передбачає формування концепту продукту за наявними вихідними даними. Організована сукупність вихідних даних, яка містить мету ПсО, підтримувальну ціль, відомості з аналізу ЦА та інші характеристики, становить концепт такої друкованої продукції. За ним фахівець ПсО розробляє шаблон (макет) друкованого продукту ІПсВ.

Суть аналізу ЦА полягає у визначенні груп та окремих осіб, яких необхідно залучити до реалізації конкретної підтримувальної цілі ПсО (ПсАк) [3]. Алгоритм аналізу ЦА передбачає послідовне виконання взаємопов'язаних завдань з: *визначення та уточнення характеристик ЦА; розрахунку її ефективності; виявлення причин та наслідків її наявної поведінки; опису вразливостей; визначення сприйнятливості; розроблення аргументів та рекомендацій для ПсО (ПсАк); уточнення первинних критеріїв оцінювання ЦА.*

На початку аналізу з'ясовують *перелік потенційних ЦА.* Як правило, це пов'язано з тим, що їх відбір для подальшого аналізу відбувається на основі загальної категорії груп та типів ЦА (організації; демографічні групи; лідери; окремі індивіди серед лідерів (ключові комунікатори)).

Отриманий у результаті такого відбору перелік може охоплювати масштаби цілої країни або регіону, що ускладнює процес аналізу ЦА.

Межі її відбору для подальшого аналізу визначаються тільки ціллю та підтримувальною ціллю ПсО (ПсАк). Кожна окрема ЦА повинна відповідати конкретній

підтримувальній цілі ПсО (ПсАк), яка окреслює її специфічну поведінку. Формування переліку ЦА для аналізу передбачає розподіл їх на основні та вторинні суб'єкти. Основними можуть бути окремі групи або особи, які беруть безпосередню участь або можуть брати участь у заходах відповідно до підцілі ПсО (ПсАк). Вторинні суб'єкти, на відміну від основних, можуть прямо або опосередковано впливати на поведінку основних суб'єктів.

На наступному етапі розраховують *ефективність ЦА*, що передбачає аналіз її можливостей змінити поведінку, яка відповідає підцілі ПсО (ПсАк). За отриманими даними встановлюють пріоритетність вивчення ЦА, що зменшує час на проведення ПсО (ПсАк) загалом.

Перед початком визначення ефективності необхідно описати поведінку ЦА, яка прийнятна для неї. Така поведінка повинна відображати її дії, за яких досягається підціль ПсО (ПсАк). Для опису дій слід використовувати кількісні показники. Визначення ефективності ЦА відбувається за такими етапами:

встановлюють ступінь контролю, який має ЦА стосовно дій, що дозволяють їй досягати підцілі ПсО (ПсАк). Вона здатна обирати рішення (контролювати ситуацію) або бути позбавлена цих прав;

окреслюють рівень обмежень, що заважають ЦА досягати підцілі ПсО (ПсАк) своїми діями. Значення рівня обмежень доцільно встановлювати за такими показниками: фізичними, географічними, політичними, економічними, правовими, соціальними, психологічними.

За отриманим інтегральним показником визначають рейтинг ЦА щодо дій, які дозволяють їй досягати підцілі ПсО (ПсАк). Для подальшого аналізу обирають ЦА з високим рейтингом.

Надалі слід виявити причини та наслідки наявної поведінки ЦА. Причини визначають умови, які впливають на її певну поведінку. Вони можуть бути викликані *внутрішніми* або *зовнішніми* факторами, що мотивують ЦА поводитися певним чином. Серед зовнішніх виділяють такі:

ситуація – дійсний фактор або сукупність факторів навколишнього середовища, які впливають на поведінку ЦА;

події – будь-яка подія, яка спричинює поведінку ЦА.

Внутрішні фактори:

цінності – концепції життя, що є добро та зло, патріотизм, честь;

переконання (вірування) – це те, що є істинним або хибним для ЦА на основі отриманого досвіду, громадської думки, підтверджувальних доказів, позицій органів влади та їх віри;

позиція – схильність ЦА реагувати певним чином на особу або ситуацію.

Наслідки розглядаються як результат дій ЦА. Вони можуть бути позитивними, негативними або вторинними. Позитивні та негативні наслідки характеризують поведінку ЦА, яка прийнятна або неприйнятна для неї відповідно. Варто зазначити, що ЦА здебільшого не усвідомлює негативних наслідків або ігнорує їх.

Вторинні наслідки характеризують опосередкований вплив, якого зазнають інші об'єкти в результаті досліджуваної поведінки ЦА. Аналіз вторинних наслідків дозволяє отримати більш повне уявлення про поведінку ЦА щодо інших об'єктів.

Вивчення причин та наслідків сприяє визначенню факторів, які перешкоджають або обмежують ЦА в діях, зазначених у підцілі ПсО (ПсАк). За отриманими результатами формується модель поведінки ЦА, яка являє собою концептуальну основу для розуміння дій об'єктів у соціальному середовищі. Для детального аналізу ЦА вся зібрана інформація повинна бути збережена у відповідній базі даних (БД), яку необхідно своєчасно оновлювати [7]. Зміна поведінки ЦА досягається за рахунок маніпуляції причинами та наслідками або введення нових наслідків.

На наступному кроці описують вразливості ЦА, що дозволяє обрати способи зміни її поведінки. Аналіз вразливостей ЦА відбувається шляхом послідовного вивчення таких характеристик ЦА: мотиви поведінки; психологічні та соціально-демографічні характеристики; впізнавані символи; культура.

Вивчення мотивів поведінки ЦА пов'язане з визначенням факторів, які відображають її прагнення задовольнити свої потреби та бажання. Американський психолог Абрахам Маслоу запропонував ієрархічну модель людських потреб, так звану "піраміду потреб", яка знайшла широке застосування в теорії менеджменту.

Метою аналізу мотивів поведінки є встановлення того, що є первинними та вторинними потребами для ЦА. Мотиви поведінки розглядають з погляду терміновості бажання ЦА їх задовольнити: критичні, короткострокові та довгострокові.

Психологічні характеристики відображають емоційну складову ЦА, яка може бути використана для підсилення аргументу ПсО (ПсАк) під час її переконання. Їх аналіз відбувається за такими показниками: страх (фактори, які примушують її боятися); ненависть (речі, які неприйнятні для неї); гнів (те, що викликає обурення в ЦА); любов (щось, що приваблює її); сором (речі, які вона вважає непристойними); незадоволеність (чим вона не задоволена або що вона не може отримати); цінності (що найдорожче для неї); культурні норми (еталонна поведінка на думку ЦА).

Аналіз соціально-демографічних характеристик дозволяє отримати відомості про те, що саме впливає на емоції та поведінку ЦА. У такий спосіб отримуємо додаткове уявлення про способи її мотивації. Питання аналізу соціально-демографічних характеристик ЦА вивчає теорія маркетології для аналізу її спроможностей у придбанні товарів [5]. При цьому здійснення покупки можна сприймати як певну мотивовану поведінку ЦА. Тому її соціально-демографічні характеристики доцільно розглядати за такими показниками: стать; вік; релігійна належність; етнічна належність; політичні переваги; освіта; місце проживання; географічна доступність; рівень доходу; сімейний статус; професія; місце роботи; вид діяльності.

Завдання з аналізу зазначених вище характеристик полягає в тому, щоб визначити, які з них вагомо впливають на емоції або поведінку ЦА і за яких обставин. Наприклад, етнічна належність окремих членів ЦА може істотно впливати на їх вибір під час політичного голосування, але майже не впливає на їх бажання служити у збройних силах.

Символи можуть бути подані візуальним, аудіо- або аудіовізуальним об'єктом, який має культурне або контекстуальне значення для ЦА. Вони призначені для передачі складних ідей за допомогою використання простих зрозумілих зображень або звуків. Символ здатний викликати емоцію у неї або навести її на певну думку, доповнюючи будь-яку подану інформацію. Він є дуже сильним засобом переконання ЦА та може значно підвищити переконливість аргументу ПсО (ПсАк) [3, 8]. Усі символи можна подати за

такими категоріями: національні (державні); релігійні; символи організацій; знаки; ай-стоппери.

Під час використання символів у друкованій продукції ІПсВ слід враховувати особливості культури ЦА. Символи, які мають велике значення для однієї, можуть бути неоднозначними, відразливими або навіть образливими для іншої. Люди інтерпретують символи суб'єктивно, виходячи з особистого та культурного сприймання. Під час їх використання слід дотримуватися таких правил: символи повинні бути впізнаваними; у ході розроблення нових символів доцільно використовувати звичні для ЦА; символ повинен мати конкретне значення для ЦА; символ має підсилювати вплив аргументу ПсО (ПсАк).

ЦА може виступати суб'єктом міжкультурних комунікацій, які характеризують особливості вербального та невербального спілкування осіб, що належать до різних національних та мовно-культурних спільнот. Тому характеристики культури можна розглядати як однин з елементів уразливостей ЦА. Для аналізу з погляду ІПсВ доцільно обрати такі характеристики: тип культури; тип культурної структури.

Визначення сприйнятливості полягає в оцінюванні можливості ЦА сприймати ІПсВ, що дозволяє правильно виставити пріоритети серед типів продуктів ІПсВ, які розробляються для серії ПсО (ПсАк) [3]. Визначення сприйнятливості полягає в оцінюванні ступеня сприймання ЦА, складанні рейтингу та розробленні відповідних рекомендацій. Рейтинг сприйнятливості ЦА оцінюють за п'ятибальною шкалою з використанням якісних показників.

За результатами визначення рейтингу сприйнятливості ЦА оформлюють характеристики, які враховують на етапі розроблення аргументів та рекомендацій для ПсО (ПсАк) [3]. Низький рівень сприйнятливості ЦА характеризує низьку ймовірність впливу продукції ІПсВ на неї.

Розроблення аргументів та рекомендацій для ПсО (ПсАк). Аргументи визначають загальну структуру матеріалів ІПсВ, яка спонукатиме ЦА до певних дій. Їх розроблення відбувається в такій послідовності визначення: головний аргумент; підтримувальні аргументи; спосіб апеляції (звернення), який буде доцільним для подання головного аргументу; найефективніші методи (технології) переконання для подання підтримувальних аргументів.

Головний аргумент розробляють для переконання ЦА в конкретних діях. Тому він є підґрунтям, на якому створюють матеріали ІПсВ. Головний аргумент повинен визначати причини зміни поведінки ЦА, яка відповідає підтримувальній цілі ПсО (ПсАк). Для його опису використовують одне (два) речення, у яких обґрунтовано шляхи зміни поведінки ЦА, що відповідає підтримувальній цілі ПсО (ПсАк).

Зміст головного аргументу повинен відображати взаємозв'язок поведінки ЦА з однією або декількома її вразливостями. Подавати його бажано в такому форматі: "залучення ЦА в X (бажана поведінка) призведе до Y (наслідки, які прийнятні для ЦА)". Наприклад, "зростання культури в регіоні приведе до стабільного майбутнього ЦА".

Для подання головного аргументу використовують такі способи апеляції (звернення): *легітимність (авторитет)*, *неминучість (зобов'язання і послідовність)*, *з групою – проти групи (прихильність), мода (стереотипне мислення)*, *ностальгія, користь (взаємний обмін)*, *дефіцит* [10–11].

Підтримувальні аргументи використовують для підвищення мотивації ЦА щодо сприймання головного аргументу. Ефективність їх використання можна підвищити шляхом наведення фактів, конкретних прикладів, статистики. Для розроблення підтримувальних аргументів використовують відомості, отримані на етапі аналізу причин та наслідків наявної поведінки ЦА та її вразливостей. Під час подання підтримувальних аргументів у друкованій продукції ІПсВ використовують методи, способи та технології здійснення ІПсВ на ЦА, які ґрунтуються на особливостях механізмів мотивації, засвоєння інформації та прийняття рішень людиною [9, 11].

На останньому етапі аналізу ЦА *уточнюють первинні критерії оцінювання*. Їх визначають на початку планування ПсО (ПсАк) та надають разом з ціллю, підтримувальною ціллю та потенційною ЦА [3]. Процес уточнення критеріїв оцінювання ЦА передбачає отримання індикаторів (показників), за якими можна визначити зміну її поведінки. Показники класифікуються за такими ознаками: специфічні; ті, які можна виміряти; ті, що можна помітити.

Під час формування уточнених критеріїв оцінювання зазвичай використовують такі елементи: географічна місцевість (область, місто, район, село); період повторення дії (день, тиждень, місяць); інтенсивність повторюваності дії (кількість випадків за період); специфічне місце (вулиця, будинок, квартира тощо); час.

Отже, аналіз ЦА передбачає ретельне, всебічне вивчення характеристик осіб, окремих соціальних груп та є основою алгоритму автоматизації процесу створення друкованих матеріалів.

Структурна схема алгоритму автоматизації процесу створення друкованих матеріалів ІПсВ зображена на рис. 1. Покрокове заповнення відповідних пунктів програми з урахуванням методології НАТО приведе до автоматичного формування концепту опису друкованого продукту ІПсВ.

Крім того, у виконавця, який безпосередньо аналізує обрану ЦА, виникає ідея продукту, яку він втілює в концепт. Далі на етапі оформлення дизайну друкованої продукції ІПсВ він може користуватися БД, у якій знаходяться як приклади вже готові матеріали і довідкова інформація.

Наповнення БД повинне відбуватися за двома групами критеріїв: перша має характеризувати психологічну (маніпулятивну) складову продукту ІПсВ, друга – правила його оформлення з погляду сприйняття (привернення уваги) ЦА (композиція, кольорова гама, стиль шрифту).

Розроблення продукції та дизайн. На основі інформації, отриманої під час аналізу ЦА, формується концепт опису продукції ІПсВ. Основна інформація у ньому – це обрані вразливості ЦА та методи, способи ПсВ. Ефективність кінцевого друкованого продукту ІПсВ визначається не лише закладеним у нього змістом, а й умінням якісно та творчо оформити задуману концепцію. Тому розробники повинні враховувати теоретичні основи дизайну та відомі маркетингові технології створення продукції ІПсВ.

Отже, розробник не лише зменшує час на виконання завдання, а й постійно вдосконалює свої знання та навички з методики створення матеріалів ІПсВ.

Відповідно до поданого алгоритму було запропоновано програмне забезпечення автоматизації процесу розробки матеріалів ІПсВ, кінцевим результатом роботи якого є концепт створення друкованого продукту ІПсВ.

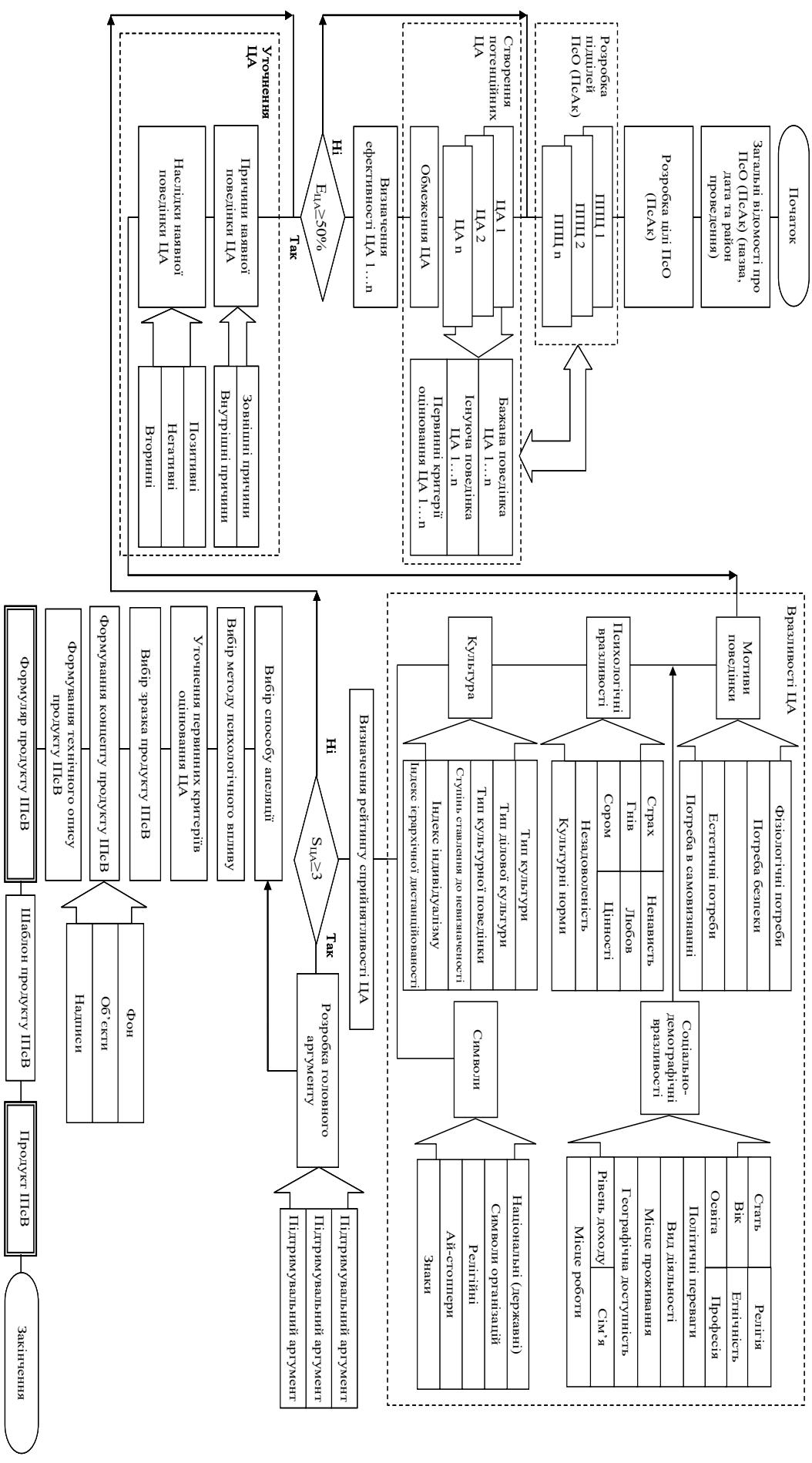


Рис. 1. Структурна схема алгоритму автоматизації процесу створення друкованих матеріалів ІПсВ

Висновки. Незважаючи на те, що сьогодні забезпеченню інформаційної безпеки держави приділяється достатня увага, основними проблемними питаннями при цьому на даному етапі залишаються: своєчасне виявлення інформаційних загроз, аналіз ситуації та планування відповідних контрзаходів, розроблення та поширення спеціального контенту, оцінювання ефективності вжитих заходів.

В умовах обмеження часового ресурсу єдиним можливим шляхом забезпечення інформаційної безпеки держави є автоматизація та інтелектуалізація завдань на всіх управлінських ланках, а особливо під час виконання заходів з інформаційно-психологічної протидії підрозділами інформаційно-психологічних операцій ЗС України. Частково підвищити ефективність виконання таких заходів можна за рахунок забезпечення якості та своєчасності розроблення відповідного контенту, спрямованого на визначену ЦА.

Подальші наукові дослідження доцільно спрямувати на автоматизацію розроблення інтелектуальної бази даних графічних елементів для матеріалів ІПсВ.

СПИСОК ЛІТЕРАТУРИ

1. Інформаційна безпека держави: підручник / В. М. Петрик та ін.; за заг. ред. В. В. Остроухова. Київ : ДНУ “Книжкова палата України”, 2016. Т. 1. 264 с.
2. Про затвердження Тимчасової настанови з психологічних операцій : наказ Генерального штабу Збройних Сил України від 13.12.2016 № 012. 49 с. Інв. 1682 т.
3. FM 3-05.301 Psychological Operations Process Tactics, Techniques and Procedures. URL: https://info.publicintelligence.net/USArmy-PsyOpsTactics.pdf. Харків, 2016. 368 с. (дата звернення: 08.02.2019).
4. Психологические основы воздействия рекламы. URL: http://center-yf.ru/data/Marketologu/Psihologicheskie-osnovy-vozdeistviya-reklamy.php (дата звернення: 08.04.2019).
5. Безлатный Д. В. Психология в рекламе: искусство манипуляции общественным сознанием. Москва : ООО “Ваш полиграфический партнер”, 2011. 236 с.
6. Фролов С. С. Социология организаций. Москва : Гардарики, 2001. 384 с.
7. Дж. Купер, Т. Герон, У. Х’юард. Прикладной анализ поведения. Москва : Практика, 2016. 864 с.
8. Базовые принципы работы с целевой аудиторией. URL: http://powerbranding.ru/potrebitel/celevaya-auditoriya (дата звернення: 29.04.2019).
9. Доценко Е. Психология манипуляции: феномены, механизмы и защита. Москва : ЧеРо, изд-во МГУ, 1997. 344 с.
10. Кара-Мурза С. Г. Манипуляция сознанием. Москва : Изд-во “Эксмо”, 2005. 832 с.
11. Роберт Б. Чалдині. Психологія впливу / Пер. з англ. М. Скоробогатова. Харків : Книжковий Клуб «Клуб Сімейного Дозвілля», 2016. 368 с.

Подано 13.08.2019

Ю. И. Михеев, О. В. Критенко

АВТОМАТИЗАЦИЯ ПРОЦЕССА СОЗДАНИЯ МАТЕРИАЛОВ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВЛИЯНИЯ

В статье рассматривается процесс создания материалов информационно-психологического влияния. Приведены характеристики, которые необходимо учитывать при разработке таких материалов. Предложен алгоритм анализа целевой аудитории, который выступает основным объектом для реализации поддерживающей цели психологической операции (акции). Алгоритм предполагает последовательное выполнение таких этапов:

определение и уточнение характеристик целевой аудитории; расчет ее эффективности; выявление причин и последствий ее существующего поведения; описание уязвимостей; определение восприимчивости; разработка аргументов и рекомендаций для психологической операции (акции); уточнение первичных критериев оценивания целевой аудитории.

Приведена структурная схема алгоритма автоматизации процесса создания материалов информационно-психологического воздействия, согласно которому разработано специализированное программное обеспечение, предполагающее пошаговое заполнение соответствующих пунктов программы с учетом методологии, которая используется в подразделениях психологических операций Вооруженных сил НАТО. Результатом работы специализированного программного обеспечения является концепт создания печатного продукта информационно-психологического воздействия.

Кроме того, на этапе оформления дизайна печатной продукции информационно-психологического влияния используется база данных, в которой находятся в качестве примеров уже готовые материалы и справочная информация. Наполнение базы данных происходит по двум группам критериев: первая характеризует психологическую (манипулятивную) составляющую материала информационно-психологического влияния, вторая – правила его оформления с точки зрения восприятия (привлечение внимания) целевой аудитории.

Ключевые слова: *информационно-психологическое влияние; целевая аудитория; психологическая операция; алгоритм; информационная угроза.*

Y. I. Mikhieiev, O. V. Krytenko

AUTOMATION OF THE PROCESS OF CREATING PSYCHOLOGICAL INFLUENCE PRODUCTS

The article discusses the process of creating psychological influence products. The characteristics for the creation of these materials are given. An analysis algorithm of target audience is proposed, which acts as the main object for the implementation of the supporting goal of a psychological operation (action). The algorithm presupposes the sequential execution of the following steps: definition and refinement of the specifications of the target audience; calculation of the target audience effectiveness; identifying the causes and consequences of existing behavior of the target audience; description of vulnerabilities of the target audience; determination of the target audiences' susceptibility; development of arguments and recommendations for a psychological operation (action); clarification of the primary criteria for evaluation of the target audience.

The block diagram of the automation process algorithm of creating psychological influence products is provided in the article. According to the presented algorithm, specialized software has been developed and involves step-by-step filling of the relevant points of the program, taking into account the methodology which is used in the units of psychological operations of the NATO armed forces. The result of the specialized software's work is the concept of creation of the printed psychological influence product.

In addition, at the stage of designing of the printed psychological influence products, there is a database which contains ready-made materials and reference information which serve as the examples. There are two groups of criteria that are used while extending the database: the first group characterizes the psychological (manipulative) component of the psychological influence products, the second – the rules for its design in terms of perception (attention) of the target audience.

Keywords: *psychological influence; target audience; psychological operation; algorithm; information threat.*

Андреєв Фелікс Михайлович – доктор технічних наук, професор, професор кафедри Харківського національного університету імені В. Н. Каразіна.
Наукові інтереси:
– розробка принципів і методів отримання та оброблення інформації в багатоканальних радіолокаційних станціях дальнього виявлення під час локації складних цілей.

Безкоровайний Володимир Валентинович – доктор технічних наук, професор, професор кафедри Харківського національного університету радіоелектроніки.
Наукові інтереси:
– системна оптимізація територіально розподілених систем.

Беспалко Ірина Анатоліївна – кандидат технічних наук, науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– дослідження функціонування та застосування космічних систем;
– методи ідентифікації та класифікації космічних систем.

Бойченко Олег Сергійович – кандидат технічних наук, начальник науково-дослідної лабораторії наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– моделювання інформаційних систем;
– системи передачі даних;
– криптографічний захист інформації.

Вдовенко Сергій Григорович – доцент кафедри Інституту інформаційних технологій Національного університету оборони України імені Івана Черняховського.
Наукові інтереси:
– криптографічний і технічний захист інформації, протидія технічним розвідкам;
– кібербезпека та кібероборона.

Випорханюк Дмитро Миколайович – науковий співробітник науково-дослідної лабораторії науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– розробка, модернізація та дослідження складних інформаційних систем;
– дослідження застосування космічних систем у військовій сфері.

Гладич Роман Іванович – науковий співробітник науково-дослідної лабораторії наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– моделювання інформаційних систем;
– технічний захист інформації.

Горбенко Іван Дмитрович – доктор технічних наук, професор, академік Академії наук прикладної радіоелектроніки, професор кафедри Харківського національного університету імені В. Н. Каразіна, професор кафедри Харківського національного університету радіоелектроніки, Голова наглядової ради – головний конструктор Приватного акціонерного товариства «Інститут інформаційних технологій».

Наукові інтереси:
– криптографічний і технічний захист інформації .

Гордієнко Юрій Олексійович – кандидат технічних наук, провідний науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– обробка геофізичної інформації.

Гордійчук Валерій Валентинович – 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.

Гуменюк Ігор Володимирович – кандидат технічних наук, старший викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– комп'ютерні мережі та компоненти;
– технічний захист інформації.

Гуменюк Максим Олексійович – кандидат технічних наук, доцент, доцент кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– управління роботизованими системами;
– алгоритми обробки інформації.

Данильчук Олександр Григорович – аспірант кафедри Одеської національної академії зв'язку імені О. С. Попова.
Наукові інтереси:
– телекомунікаційні системи;
– системи передачі даних.

Добровінський Вадим Петрович – старший викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– алгоритми обробки інформації.

Дюков Ігор Миколайович – ад'юнкт науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– перешкодозахищеність цифрових систем зв'язку, шумоподібні сигнали.

Єсіна Марина Віталіївна – кандидат технічних наук, старший викладач кафедри Харківського національного університету імені В. Н. Каразіна.
Наукові інтереси:
– криптографічний захист інформації, електронний підпис, методи багатофакторної автентифікації;
– аналіз та дослідження постквантових криптографічних перетворень.

Захарченко Микола Васильович – доктор технічних наук, професор, завідувач кафедри Одеської національної академії зв'язку імені О. С. Попова.
Наукові інтереси:
– телекомунікаційні системи;
– системи передачі даних.

Іщенко Дем'ян Андрійович – кандидат технічних наук, доцент, старший науковий співробітник науково-дослідної лабораторії науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– дослідження складних інформаційних систем;
– моделювання операцій.

Кирилюк Володимир Анатолійович – кандидат технічних наук, старший науковий співробітник, начальник науково-дослідної лабораторії науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– системи моніторингу, захисту та впливу.

Ковальчук Сергій Валерійович – науковий співробітник військової частини А1906.
Наукові інтереси:
– статистична радіотехніка.

Ковбасюк Сергій Валентинович – доктор технічних наук, старший науковий співробітник, провідний науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– розробка та вдосконалення складних інформаційно-розвідувальних систем.

Ковтун Сергій Олександрович – кандидат технічних наук, старший науковий співробітник, провідний інженер Товариства з обмеженою відповідальністю «Науково-впроваджувальна фірма "КРИПТОН"».
Наукові інтереси:
– статистична радіотехніка, системні дослідження.

Кошель Анатолій Васильович – кандидат технічних наук, доцент, завідувач автономного сейсмічного пункту Головного центру спеціального контролю Державного космічного агентства України.
Наукові інтереси:
– обробка геофізичної інформації.

Критенко Оксана Володимирівна – молодший науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– системи моніторингу, захисту та впливу.

Кулагін Костянтин Костянтинович – кандидат технічних наук, доцент, старший науковий співробітник, начальник науково-дослідного відділу Наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба.

Наукові інтереси:
– полігонні системи та комплекси;
– обробка геофізичної інформації.

Марищук Людмила Мічеславівна – молодший науковий співробітник науково-організаційного відділення Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційно-психологічна безпека.

Міхєєв Юрій Іванович – кандидат технічних наук, начальник науково-дослідної лабораторії наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
- інформаційні технології, інтернет-розвідка.

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.

Наумчак Олена Михайлівна – молодший науковий співробітник науково-дослідної лабораторії наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційно-психологічна безпека;
– інформаційно-психологічні впливи;
– психологічна стійкість до впливів.

Носова Ганна Дмитрівна – науковий співробітник науково-дослідної лабораторії наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційні системи спеціального призначення.

Орищук Ігор Олександрович – старший викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– інформаційні та психологічні операції.

Перегуда Олександр Михайлович – кандидат технічних наук, старший науковий співробітник, заступник начальника науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– проєктування, розробка та експлуатація автоматизованих систем військового призначення.

Пількевич Ігор Анатолійович – доктор технічних наук, професор, професор кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– системна інженерія;

– проєктування складних інформаційних систем.

Проценко Михайло Михайлович – кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник науково-дослідної лабораторії науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– цифрова обробка сигналів з використанням вейвлет-перетворень;
– моделювання операцій.

Романчук Микола Петрович – науковий співробітник науково-дослідного відділу наукового центру Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– обробка даних дистанційного зондування Землі;
– застосування інформаційних технологій у військовому дешифруванні;
– обробка видової інформації методами нейронних мереж.

Сидорчук Ольга Леонідівна – кандидат технічних наук, старший науковий співробітник науково-організаційного відділення 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 геофізичної інформації.

Стариков Андрій Миколайович – заступник начальника відділу Центрального управління радіоелектронної боротьби.
Наукові інтереси:
– теорія та практика здійснення заходів радіоелектронного захисту.

Стрінада Віктор Васильович – начальник кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– управління роботизованими системами;
– алгоритми обробки інформації.

Ткач Андрій Олександрович – старший викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– алгоритми обробки інформації.

Топольницький Павло Петрович – кандидат технічних наук, доцент, старший викладач кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– моделювання вимірів у радіотехнічних системах;
– обробка інформації в складних технічних системах.

Фриз Петро Васильович – заслужений працівник освіти України, кандидат технічних наук, доцент, доцент кафедри Житомирського військового інституту імені С. П. Корольова.
Наукові інтереси:
– моделювання й ефективність космічних систем;
– планування космічних спостережень.

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, розробка інформаційних систем.

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 16

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 30.09.2019. Формат 60 × 84 / 8.
Ум. друк. арк. 20,92. Тираж 100 прим. Зам. 539 офс.

Безкоштовно
Друкарня ЖВІ

10004, м. Житомир, пр-т Миру, 22