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

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

ЗБІРНИК НАУКОВИХ ПРАЦЬ

ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Виходить 4 рази на рік

Випуск № 54

КИЇВ – 2016

УДК621.43
ББК 32-26.8-68.49
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 54. – 249 с.

Голова редакційної колегії:

Лєнков С.В. доктор технічних наук, професор;

Члени редакційної колегії:

Барабаш О.В. доктор технічних наук, професор;
Білик Л.І. доктор педагогічних наук, професор;
Вишнівський В.В. доктор технічних наук, професор;
Вербицький В.В. доктор педагогічних наук, професор;
Жердєв М.К. доктор технічних наук, професор;
Замаруєва І.В. доктор технічних наук, професор;
Заславський В.А. доктор технічних наук, професор;
Лепіх Я.І. доктор фізико-математичних наук, професор;
Марушкевич А.А. доктор педагогічних наук, професор;
Мокрицький В.А. доктор технічних наук, професор;
Оксіюк О.Г. доктор технічних наук, професор;
Пономаренко Л.А. доктор технічних наук, професор;
Плахотнік О.В. доктор педагогічних наук, професор;
Сейко Н.А. доктор педагогічних наук, професор;
Слюсаренко Н.В. доктор педагогічних наук, професор;
Толубко В.Б. доктор технічних наук, професор;
Шарий В.І. доктор військових наук, професор;
Шаронова Н.В. доктор технічних наук, професор;
Шворов С.А. доктор технічних наук, професор;
Ягупов В.В. доктор педагогічних наук, професор.

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

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

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

Затверджено на засіданні вченої ради ВІКНУ від 15.12.16р., протокол № 6.

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

Відповідальність за новизну і достовірність наведених результатів, тактико-технічних та економічних показників і коректність висловлювань несуть автори. Точка зору редколегії не завжди збігається з позицією авторів. Усі матеріали надруковані в авторській редакції.

Електронні версії Збірників розміщені на сайті бібліотеки ім. В.І. Вернадського та на сайті Військового інституту.

Примірники збірників знаходяться у Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича та у бібліотеці Військового інституту.

Адреса редакції: 03689, м. Київ, вул. Ломоносова,81 тел./факс +38 (044) 521 – 33 – 82
Наклад 300 прим.

Ел.адреса редактора: lenkov_s@ukr.net

Офіційний сайт журналу: http://miljournals.knu.ua/

ТЕХНІКА

Гришин С.П., Мірошніченко О.В., Бадрук О.О. Аналіз світових програм і проектів створення зброї спрямованої енергії…… **7**
Жиров Г.Б. Методи цифрової обробки в задачах ідентифікації і придушення завад сигналів УКХ діапазону……. **16**
Коваленко І.Г., Міщенко А.О., Вавасова О.С. Аналіз електромагнітної сумісності засобів радіозв'язку……. **22**
Кошевой Н.Д., Костенко Е.М., Кошевая И.И. Сравнительный анализ методов синтеза оптимальных по стоимостным (временным) затратам планов многофакторного эксперимента……. **33**
Лисий М.І., Балицький І.І., Бабій Ю.О., Поліщук В.В. Узагальнення класифікації технічних засобів для охорони та захисту кордону……. **40**
Лоза В.Н. Анализ принципа дискретной частотной вейвлет-фильтрации сигнала и синтез оптимального алгоритма построения базы фильтров…….. **50**
Нікіфоров М.М., Жиров Г.Б., Пампуха І.В. Можливості інтегрованої системи пасивного моніторингу простору в умовах застосування високоточної зброї……. **55**
Радзівілов Г.Д., Романенко В.П., Бригадир С.П. Оцінка показників якості діагностичного забезпечення ремонту військової техніки зв'язку……. **63**
Рома О.М., Василенко С.В. Вибір параметрів алгоритму входження в синхронізм радіолінії управління безпілотним літальним апаратом з псевдовипадковим переналаштуванням робочої частоти…… **71**
Чешун В.М., Лєнков С.В., Прокопчук С.О., Охрамович М.М., Шевченко В.В. Моделі динамічних несправностей дискретних інтегральних компонентів комплементарної логіки……. **79**
Шишанов М.О., Любарець А.А., Шатров А.М., Горбачевський С.А. Визначення терміну технічної придатності засобів ураження на основі моделі надійності з аргументом, що запізнюється……. **88**
Procenko Ya.M. Model of adaptive condition based technical maintenance of radioelectronic technology objects…..... **94**

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Гунченко Ю.О., Бойчук В.О., Юмашов В.С. Метод виявлення загрози поширення забороненої до розповсюдження інформації в комп'ютерних мережах……. **99**
Козак І.В., Огнєвий О.В. Метод протидії прихованим загрозам в середовищі хмарних обчислень……. **107**
Кольцов Р.Ю. Ідентифікація невідомих систем координат за допомогою додатку ArcGis - ARCMAP 10.2…….. **114**
Лєнков С.В., Джулій В.М., Романовська І.А. Метод підвищення ефективності видачі результату пошуку в інформаційному середовищі…….. **120**
Міночкін Д.А. Аналіз механізмів кешування контенту в безпроводових мережах наступного покоління……. **128**
Муляр І.В., Гусляков Г.В., Солодєєва Л.В. Розробка математичної моделі та методу її вирішення для підвищення ефективності використання обчислювальних ресурсів на основі технології віртуалізації…….. **134**
Мясіщев О.А., Лєнков Є.С., Білик О.М. Розпізнавання графічних образів з використанням нейронних мереж……. **143**
Селюков О.В., Огнєвий О.В., Осипа В.О., Бабій І.М. Розробка моделей надійності

програмного забезпечення для технології типу «клієнт-сервер»……. **149**
Хірх-Ялан В.І. Аспекти автоматизації картографічної генералізації для створення електронних карт відповідних масштабів топографічною службою Збройних Сил України……. **157**
Gostev V.V., Pampuha I.V., Savkov P.A., Savkova V.P. A typical fuzzy controller……. **166**
Kubiavka N. The control of information support of the processes of influence on the opponent…… **174**

СИСТЕМНІ ПИТАННЯ В НАУЦІ ТА ОСВІТІ

Апатова Н.В. Структура учебной деятельности при компьютерном обучении…….. **182**
Бойченко О.В., Тупота Е.С. DLP-технологии в системе экономической безопасности предприятия……. **191**
Горячева К.С. Аналіз функціонального потенціалу абревіатур в англомовній політичній сфері…….. **199**
Грибок А.О. Соціально-психологічні особливості адаптації курсантів - учасників бойових дій в районі проведення антитерористичної операції, до навчальної діяльності у вищому військовому навчальному закладі……. **205**
Гуменна О.І., Муляр І.В., Ряба Л.О. Доступний бібліотечний простір для користувачів з обмеженими можливостями……. **216**
Дячук А.О. Види та характеристика пожеж в екосистемах і їх вплив на загальний стан екологічної безпеки Хмельницької області…….. **223**
Кошевой Н.Д., Стадник А.С. Оптимальное планирование эксперимента в условиях ограниченных ресурсов…… **230**
Нікіфоров М.М., Турченко Ю.В. Захист від інформаційно-психологічного впливу як складова частина морально-психологічного забезпечення службово-бойових завдань в зоні АТО…… **235**
Дані про авторів……... **243**
Алфавітний покажчик……. **247**

TECHNICS

Grishin S.P., Miroshnichenko O.V., Badruk O.O. Analysis of global programms and projects of creation directed energy weapons ……. **7**
Zhyrov G.B. Methods of digital processing in the problem of identification and suppression noise signals VHF……. **16**
Kovalenko I.Г., Mishchenko A.A., Vavasova O.S. Analysis of electromagnetic compatibility telecommunication means……. **22**
Koshevoy N.D., Kostenko E.M., Koshevaya I.I. The comparative analysis of the methods of synthesis of multifactorial experiment's optimal plans in cost (time)…….. **33**
Lisiy N.I., Balitchi I.I., Babi Yu.A., Polishchuk V.V. Summary of the classification of technical means for the safety and protection of borders……. **40**
Loza V.N. Construction of algorithm multi-level discrete wavelet - filtration radar signal and the synthesis of optimal algorithm for constructing base filters……. **50**
Nikiforov N.N., Zhyrov G.B., Pampuha I.V. Possibilities of интегрированой of system of passive monitoring of space in the conditions of application of high-fidelity weapon…… **55**
Radzivslov G.D., Romanenko V.P., Brigader S.P. Evaluation of a diagnostic maintenance repair equipment military communications……. **63**
Roma A.N., Vasylenko S.V. Setting algorithm acquisition entry into radioline control UAV with FHSS…… **71**
Cheshun V.M., Lyenkov S.V., Prokopchuk S.O., Ohramovych M.M., V.V. Shevchenko. Discrete model of dynamic fault integral component complementary logic……. **79**
Shishanov M.O., Ljubarec A.A., Shatrov A.M., Horbachevskii S.A. The definition of the line technical feasibility means destruction, on the basis of reliability models with retarded argument……. **88**
Procenko Ya.M. Model of adaptive condition based technical maintenance of radioelectronic technology objects…..... **94**

INFORMATION TECHNOLOGIES

Gynchenko Y.A., Boychuk V.O., Yumashov V.S. Method for detection of threats distribute illegal to spread information in computer networks…….. **99**
Kozak I.V., Ohnevyj A.V. Method of the counteracting the hidden threats in the cloud computing environment…… **107**
Koltsov R.Yu. Identify unknown coordinate systems through the application ArcGis - ARCMAP 10.2……. **114**
Lenkov S.V., Dzhuliy V.N., Romanovska I.A. Method of increasing the efficiency of the issuance of a search result in the information environment……. **120**
Minochkin D.A. Analysis of content caching mechanisms in wireless next generation networks…… **128**
Mulyar I.V, Gusliakov G.V., Solodeeva l.V. The development of mathematical models and methods of its solution to improve the utilization of computing resources based on virtualization technology…….. **134**
Myasischev O.A., Lenkov Ye.S., Bilik O.M. Recognition of graphic images using neural networks……. **143**
Selyukov A.V., Ognievyi O.V., Osupa V.A., Babiy I.M. Development of reliability models for software technology type "client-server"……. **149**
Khirkh-Ialan V.I. Aspects of automation for cartographic generalization creating

electronic maps of appropriate scale topographic service armed forces of Ukraine……. **157**
Gostev V.V., Pampuha I.V., Savkov P.A., Savkova V.P. A typical fuzzy controller…….. **166**
Kubiavka N. The control of information support of the processes of influence on the opponent…… **174**

SYSTEM ISSUES IN SCIENCE AND EDUCATION

Apatova N.V. The structure of educational activities computer training.…… **182**
Boychenko O.V., Tupota E.S. DLP technology in the system of economic security of enterprise…… **191**
Goryacheva K.S. Functional petential of abbreviation in english political sphere……. **199**
Hrybok A.A. Peculiarities of social and psychological adaptation of the cadets-participants of the anti-terrorist operation to learning activity at higher military educational institutions……. **205**
Humenna E.I., Mulyar I.V., Ryaba L.A. The library is available for users with disabilities…….. **216**
Diachuk A.A. The kind and type of fires in the ecosystem and their effects on ecological safety of khmelnytsky's region……. **223**
Koshevoy N.D., Stadnik A.S. Optimal planning experiments in conditions of limited resources……. **230**
Nikiforov M.M., Turchenko Yu.V. Information and psychological effects protection as part of the psychological and moral support of the service and combat mission in the ATO area…… **235**
Data on authors...……... **243**
Alphabetical index……. **247**

УДК 355.02

к.т.н. **Гришин С.П.** (НМЦКП МОУ)
к.т.н., с.н.с. **Мірошніченко О.В.** (ВІКНУ)
Бадрук О.О. (ВІКНУ)

АНАЛІЗ СВІТОВИХ ПРОГРАМ І ПРОЕКТІВ СТВОРЕННЯ ЗБРОЇ СПРЯМОВАНОЇ ЕНЕРГІЇ

У даний час всі роботи в області зброї спрямованої енергії йдуть в багатьох країнах світу. Основними розробниками зброї даного класу є перш за все США, Китай та РФ. Гарні результати роботи в цьому напрямку показують також Ізраїль, Німеччина та Індія. Але якщо у Китаї та РФ ці розробки є, в основному, закритими для широкого загалу, то у США навіть безперспективні проекти підлягають масовому «піару». У даній статті проведений аналіз зразків та розробок зброї спрямованої енергії, здебільше, на прикладі США та на основі матеріалів викладених у відкритих джерелах.

Наведено останні досягнення науково-технічних програм з розробки лазерних систем для тактичної оборони, перспективи розвитку лазерної зброї. Розкриті проблеми, пов'язані з потужністю, тепловою ємністю і розмірами озброєнь даного класу.

Ключові слова: зброя нелетальної дії, зброя спрямованої енергії, аналіз, вражаючі фактори, типові ситуації застосування.

Вступ. Лазери, мазери, бластери і електромагнітні гармати є частиною канонічного озброєння зі світу наукової фантастики. Проблеми, пов'язані з потужністю, тепловою ємністю і розмірами озброєнь даного класу зробили ці системи важко реалізованими у практиці, але в умовах сьогодення ці системи існують, а наукові та практичні розробки в цьому напрямку є одними з основних та перспективних у всьому світі.

Зброя спрямованої енергії (англ. *Directed-energy weapon, DEW*) - зброя, що випромінює енергію у заданому напрямі без використання дротів, дротиків і інших провідників, для досягнення летального або нелетального ефекту. Цей вид озброєння існує, але перебуває на стадії НДДКР і тестування. Деякі види такої зброї існують тільки у фантастичних книгах, відеоіграх, фільмах і мультфільмах, нефункціональних іграшках, а деякі - перебувають на стадії розробки і тестування. Таке визначення дає сьогодні Вікіпедія при здійсненні пошуку в Google. Але насправді нові технології надають все більше можливостей для розробки перспективних систем зброї, метою створення яких є тимчасове позбавлення боєздатності живої сили; функціональне ураження озброєння і військової техніки протиборчої сторони; виключення необгрунтованої загибелі мирного населення, зниження втрат сил і засобів своїх військ, підвищення ефективності дій військ; скорочення часу на виконання бойових завдань; заборона руйнування культурних цінностей, збереження соціально-економічної та промислової інфраструктури в районі бойових дій; запобігання екологічних катастроф; збереження навколишнього середовища та забезпечення морально-психологічної переваги над противником.

Зброя спрямованої енергії (далі – ЗСЕ) відноситься до зброї нелетальної дії (далі – ЗНД) під якою ми пропонуємо розуміти засоби нелетального ураження противника у збройній боротьбі, застосування яких забезпечує тимчасову втрату боєздатності живої сили, озброєння, військової техніки та збереження навколишнього середовища.

При всьому різноманітті бойових властивостей видів ЗНД, вплив на об'єкти обумовлено переважно трьома основними формами енергії, яка є спільною кількісною мірою різних форм руху матерії – фізичної, хімічної і біологічної [1].

Принцип використання енергії фізичних полів променевої (хвильової) природи, руйнівна дія якої здійснюється випромінюваною енергією, сконцентрованою у вузькому пучку, дає підставу об'єднати їх при класифікації в один вид зброї спрямованої енергії.

До зброї спрямованої енергії відноситься лазерна і прискорювальна (пучкова) зброя, надвисокочастотна, мікрохвильова і акустична зброя [2 - 5]. Матеріальною основою ЗСЕ можуть бути комплекси спеціального озброєння (КСО) спрямованої енергії, що можуть створюватися на базі існуючих основних зразків бронетанкової техніки. Нелетальне ураження КСО здійснюють опроміненням.

Основна частина. В даний час всі роботи в області ЗСЕ йдуть в багатьох країнах світу. Основними розробниками зброї даного класу є перш за все США, Кітай та РФ. Гарні результати роботи в цьому напрямку показують також Ізраїль, Німеччина та Індія. Але якщо у Китаї та РФ ці розробки є, в основному, закритими для широкого загалу, то у США навіть безперспективні проекти підлягають масовому «піару». Тож, у даній статті проведений аналіз зразків та розробок ЗСЕ, здебільше, на прикладі США та на основі матеріалів викладених у відкритих джерелах.

Робота в галузі розробок ЗСЕ здійснюється в декількох напрямках. Найбільш масовим, хоча і не дуже успішним, є лазерна зброя. Всього у світі налічується кілька десятків програм і проектів, з яких до реального впровадження у війська дійшли лічені одиниці. Приблизно таким же чином йде справа і з мікрохвильовими випромінювачами, проте у випадку з останніми до практичного використання до теперішнього часу дійшла тільки одна система.

Єдиним на даний момент прикладом практично впровадженої у війська зброї, яка базується на передачі мікрохвильового випромінювання, є американський комплекс ADS (Active Denial System - «Система активного стримування»). Комплекс складається з апаратурного блоку і антени (рис. 1).

ADS, яку іноді називають тепловим променем або променем болю, була створена компанією Raytheon, світовим лідером в розробці і дослідженні мікрохвильового випромінювання. Вона є однією з перших, нелетальних, спрямованих, протипіхотних систем, розгорнутих в американській армії.

ADS посилає сфокусований пучок надзвичайно високої частоти 95 ГГц в сторону окремої людини або групи людей, викликаючи сильний біль. Ця енергія викликає підйом температури поверхні людської шкіри, що через кілька секунд стає настільки некомфортним, що люди змушені покинути контрольовану зону.

При цьому залишаються сумніви щодо наслідків для здоров'я в довгостроковій перспективі або того, що станеться, якщо людина піддавалася тривалому впливу. Також критику викликають «пробивні» здібності променя. Неодноразово висловлювалися припущення про можливість екранування випромінювання навіть за допомогою щільної тканини. Однак офіційних даних про можливості запобігання ураження, з цілком зрозумілих причин, поки опубліковано не було і, швидше за все, не буде взагалі.



Рис. 1. Комплекс ADS (Active Denial System) американських ЗС

Найбільш відомим представником іншого класу ЗСЕ, а саме – лазерної зброї, є колишній проект ABL (AirBorne Laser - «Лазер повітряного базування») і літак-прототип Boeing YAL-1 на базі лайнера Боїнг-747 (рис. 2). Літак несе два твердотільних лазера для підсвітки цілі і наведення, а також один хімічний лазер. Твердотільні лазери у цій системі використовуються для вимірювання дальності до цілі і визначення можливих спотворень променя при проходженні через атмосферу. Після підтвердження захоплення цілі вмикається хімічний лазер HEL мегаватного класу, який і знищує ціль. Проект ABL з самого початку призначався для роботи в системі ПРО.



Рис. 2. Проект ABL (AirBorne Laser) і літак-прототип Boeing YAL-1

За наявними даними, запасу реагентів на борту літака вистачало для проведення 18-20 лазерних «залпів» тривалістю до десяти секунд кожен. Дальність дії системи секретна, але її можна оцінити в 150-200 кілометрів.

Але незабаром виявилися два непереборних технологічних бар'єри. По-перше, на кожен ват електроенергії виробляється 4 вата теплової енергії, яку всю неможливо відвести. Вона йде на нагрів самого обладнання і літака-носія. При потужності в 6 МВт перегрів літака набуває катастрофічних розмірів. Тим більше що на борту знаходяться ще і ємності з рідким киснем. Другий бар'єр - плавлення лінз з розфокусуванням променя лазеру. Температура випромінювання така, що ніяке кварцове скло не витримує.

В кінці 2011 року проект ABL був закритий через відсутність очікуваних результатів і проект в тому вигляді був визнаний безперспективним. Розробка і випробування вже тоді коштували більше 5 млрд. дол. Кожен такий літак в майбутньому обходився б казні в 1,5 млрд. одноразово і близько ста мільйонів в рік на його утримання. Оскільки Boeing YAL-1 сам є легкою мішенню, бойовий сценарій передбачає його прикриття ланкою винищувачів і супровід літаком радіоелектронної боротьби. За оцінками Пентагону, така ланка зможе виконувати тактичні завдання тільки при збільшенні дальності ефективного ураження лазером в кілька разів. Це означає необхідність підвищення потужності лазера вже в десятки разів або відповідне зниження розбіжності пучка. Обидва завдання на сучасному рівні технологій є нездійсненними.

Існуючі стратегічні (Aegis) і тактичні (Iron Dome) системи ПРО використовують кінетичний принцип ураження цілей. На сьогодні вони справляються з перехопленням ракет успішніше, ніж експериментальні лазери.

Після кількох припинень і перебоїв з фінансуванням, програма YAL була остаточно закрита в грудні 2011 року. Подібна доля була і в іншої, менш претензійною програми – ATL (Advanced Tactical Laser - «Перспективний тактичний лазер»), яка є своєрідним відгалуженням від програми ABL (рис. 3).

ATL розроблялася з 1996 року. Під час обкатки системи в 46-й ескадрильї випробувального центру семитонний прототип розміщувався на транспортних літаках серії C-130H Hercules. До 2008 року вдалося знизити його масу до 5,5 тонн - тоді ж повідомлялося про успішне ураженні наземної цілі на базі ВПС Киртленд (Нью-Мексико). Влітку 2009 року було проведено випробування з імітацією бойового завдання. Лазер на літаку Lockheed NC-130H успішно вразив малогабаритну наземну ціль.

В майбутньому лазерна система ATL повинна була встановлюватися на важкоозброєні літаки підтримки сухопутних військ Lockheed AC-130. Однак проект в існуючому вигляді був також визнаний безперспективним з вищезазначених причин.



Рис. 3. ATL (Advanced Tactical Laser)

На найближчі 20-50 років потужні бойові лазери, здатні збивати ракети, будуть виключно темою творів фантастів і піарників корпорацій на кшталт «Боїнга». А лазерні амбіції світу з мегаватного рівня охололи до кіловатного.

Зараз основні ставки робляться на проект HELADS (High Energy Liquid Laser Area Defense System) і конкретні варіанти його застосування (рис. 4).

Ступінь готовності американської системи HELLADS на сьогодні достатня для впевненого ураження ракет класу «земля-повітря» і реактивних снарядів різного типу. Теоретично HELLADS здатна знищувати велику частину повітряних і деяких наземних цілей. Але міжконтинентальні балістичні ракети їй не по зубах. В основі системи лежить лазер з рідким активним середовищем. Циркуляція рідини дозволяє відводити більше тепла. В результаті можна збільшити потужність променя. На сьогоднішній день лазер HELLADS досягає потужності 150 кВт. Ще у 2014 році Пентагон мав намір оснастити нею перші винищувачі і бомбардувальники ВПС США, однак і на сьогоднішній день HELLADS є проектом, який готуються до проходження випробувань. Кардинальні доопрацювання проект отримав за останні кілька років. Перш за все, була істотно знижена маса лазерного обладнання (до 2000 кг), що дозволяє встановлювати його практично на всі типи літаків.



Рис. 4. HELADS (High Energy Liquid Laser Area Defense System)

Компанія Northrop Grumman, якій належать більшість наведених вище розробок, також є лідером і в області лазерних систем для флоту. Так, наприклад, архітектура LaWS (Laser Weapon System) - перспективна бойова лазерна система для ВМС США (рис. 5). Перший варіант установки отримав назву MLD (Maritime Laser Demonstrator). В даний час завершуються активні роботи по проекту MLD (Maritime Laser Demonstration - «Демонстрація морського лазера»). Як і деякі інші бойові лазери, комплекс MLD повинен забезпечувати протиповітряну оборону кораблів військово-морських сил. Крім того, до задач цієї системи може бути введена задача захисту бойових кораблів від катерів та інших малих плавзасобів противника. Основою комплексу MLD є твердотільний лазер JHPSSL і система його наведення.



Рис. 5. Боевой лазер ВМС США (LaWS)

На даний момент, вся система LaWS, представлена серією з трьох дослідних концептуальних проектів, які значною мірою різняться між собою. У лінійку даного виду зброї входять наступні дослідні зразки:

1. MLD - два варіанти (від Northrop і Raytheon) випробувані в березні-червні 2009 року.
2. LaWS на базі ЗАК Mk 15 Phalanx CIWS - випробуваний в травні 2010 року.
3. LaWS Prototype - випробуваний влітку і восени 2012 року на есмінці USS Dewey (DDG-105).

Щодо наземних проектів, то армія США протягом майже місяця проводила випробування нового наземного бойового лазера HEL MD (High Energy Laser Mobile Demonstrator, мобільний демонстратор високоенергетичного лазера) (рис. 6). Випробування проводилися з 18 листопада по 10 грудня 2013 року на ракетному полігоні «Уайт-Сендз». За цей час система вразила понад 90 мінометних пострілів і кілька безпілотних літальних апаратів.



Рис. 6. Наземний бойовий лазер HEL MD (High Energy Laser Mobile)

До складу випробувальної системи входила радіолокаційна станція EMMR, яка виявляла повітряні цілі і передавала їх параметри бойовій системі управління вогнем, що контролює лазер. Потужність випробуваного лазера склала десять кіловат. У перспективі на мобільне шасі системи планується встановити лазер потужністю 50 кіловат, який потім буде модернізований до ста кіловат. Одночасно будуть покращені системи енергозабезпечення.

HEL MD розробляється спеціально для захисту важливих військових об'єктів від мінометних пострілів, крилатих ракет, артилерійських снарядів і безпілотників.

Поки інші лазерні комплекси проходять випробування, відразу два американських проекти вже дали практичні результати. З березня 2003 року в Афганістані і Іраку застосовувалася бойова машина ZEUS-HLONS (HMMWV Laser Ordnance Neutralisation System - «Система лазерної нейтралізації боєприпасів на базі автомобіля HMMWV») (Рис.7), створена компанією Sparta Inc. На стандартному американському армійському джипі встановлюється комплекс обладнання з твердотілим лазером потужністю близько 10 кіловат. Такої потужності випромінювання достатньо для того, щоб направити промінь на вибуховий пристрій або на снаряд, що не розірвався, і тим самим здійснити його детонацію. Ефективна дальність дії комплексу ZEUS-HLONS наближається до 300 метрів. Живучість робочого тіла лазера дозволяє здійснювати до двох тисяч «залпів» за добу. Результативність операцій за участю цього лазерного комплексу наближається до 100 відсотків.



Рис. 7. Система лазерної нейтралізації боєприпасів на базі автомобіля HMMWV

Другим застосовуваним на практиці лазерним комплексом є система GLEF (Green Light Escalation of Force - «Ескалація сили за допомогою зеленого променя») (Рис.8). Твердотільний випромінювач кріпиться на стандартній дистанційно керованій турелі CROWS і може бути встановлений практично на будь-який вид техніки військ НАТО. GLEF має набагато меншу потужність порівняно з іншими бойовими лазерами і призначений для короткочасного осліплення противника або протидії прицілюванню. Головною особливістю цього комплексу є створення досить широкого по азимуту засвічення, яке гарантовано «накриває» потенційного противника. Примітно, що з використанням напрацювань по темі GLEF був створений портативний комплекс GLARE, розміри якого дозволяють переносити і застосовувати його всього однією людиною. Призначення GLARE точно таке ж саме - короткочасне осліплення противника.



Рис. 8. Система GLEF (Green Light Escalation of Force)

Наземні системи ППО на основі лазерів розроблені і випробувані і в інших країнах. Так, наприклад, цікава концепція німецької фірми Rheinmetall Waffe Munition, яка поряд зі створенням окремих твердотільних лазерів (до 50 кВт) на рухомих стаціонарних та рухомих засобах, розробила і системи, які одночасно фокусують випромінювання декількох окремо розташованих лазерів на одній цілі. Подібна інтегрована система дозволяє не тільки уникати проблем, що виникають при розробці єдиного потужного лазера, а й використовувати її для протидії як найменшим так і значним цілям (наприклад, крилатим ракетам).

В Ізраїлі фірмою Rafael розроблена система «Iron Beam» (Залізний промінь) (Рис.6), призначена для ураження повітряних об'єктів на відстані до 2 км. Це високоенергетична лазерна система (HEL), призначена для ураження ракет, мінометних снарядів і безпілотних літальних апаратів (БПЛА) на коротких дистанціях.

Система наземного базування використовує два мульти-кіловатних твердотільних лазера (SSL). Мобільна установка складається з РЛС огляду повітряного простору, блоків управління і контролю, а також з двох лазерних установок.



Рис. 9. Система «Iron Beam» ЗС Ізраїлю

У Російській Федерації вперше зразки радіоелектронного зброї на нових фізичних принципах були продемонстровані у вересні 2016 року у закритому показі для Міноборони Росії на полях військово-технічного форуму "Армія 2016". Російська радіоелектронна зброя на нових фізичних принципах здатна вражати техніку противника, в тому числі високоточну зброю, без застосування снарядів, так заявив офіційний представник підприємства-розробника даних комплексів - "Об'єднаної приладобудівної корпорації". Однак все це поки що заявляється на вербальному рівні, нових зразків широкому загалу збройними силами РФ представлено не було.

Варто зауважити, що розробка ЗСЕ у РФ почалася ще у радянські часи. Так, однією з організацій, що займалася розробкою бойових лазерних комплексів, було НВО «Астрофізика», де вже в 1982 році був розроблений лазерний комплекс СЛК 1К11 «Стилет» (рис. 10). Завданням лазерного комплексу було забезпечення протидії оптико-електронним

системам спостереження і управління зброєю в жорстких кліматичних і експлуатаційних умовах, що висуваються до бронетехніки.

На «Уралтрансмаш» було виготовлено дві кілька відмінних між собою машини. Відмінності були пов'язані з тим, що в порядку напрацювання досвіду і експериментів лазерні системи різнилися. Бойові характеристики комплексу були на ті часи дуже вражаючими, вони і в даний час відповідають вимогам ведення оборонно-тактичних операцій. Комплекс «Стилет» був прийнятий на озброєння, але з певних причин серійно не випускався. Дві експериментальні машини так і залишилися в єдиних екземплярах. Формально цей комплекс знаходиться на озброєнні ЗС РФ і донині. Однак про долю цих машин довгий час нічого не було відомо. По завершенню випробувань вони виявилися фактично нікому не потрібними. Розвал СРСР розкидав їх по пострадянському простору і довів до стану металобрухту.



Рис. 10. Лазерний комплекс СЛК 1К11 «Стилет» ЗС СРСР

Висновки. Звичайно, корпорації, що займаються розробкою та конструюванням зразків ЗСЕ всіляко перебільшують свої успіхи, щоб домогтися більшого фінансування. Всіляко піарять досягнення, знімають рекламні ролики, видаючи їх за документальні. На фотографіях домальовує яскраві промені. Однак всі військові лазери працюють в діапазоні невидимих хвиль.

Незважаючи на згортання проектів лазерної зброї великої потужності (як планувалося в рамках СОІ) останнім часом тривають науково-технічні програми з розробки лазерних систем для тактичної оборони. Такі програми проводяться не тільки в США (де лідерами є компанії Boeing і Northrop Grumman), а й в Індії, Китаї та РФ. Поряд з розробкою потужних лазерів для військових цілей, в даний час проводиться розробка потужних лазерів для термоядерного синтезу і дослідження процесів при високих потужностях випромінювання (США, Японія, Німеччина, Великобританія, Росія та ін.).

У перспективі лазерна зброя може знайти застосування і в контртерористичної діяльності. Наприклад, з розширенням доступності квадрокоптера цілком можна очікувати спроб здійснення терактів з їх допомогою (доставка вибухового пристрою в натовп або робочий кабінет посадовця, розпорошення отруйних речовин і т.п.). Застосування лазерних систем дозволяє знищити такі об'єкти безшумно, що не створить паніки.

Але, в цілому, майбутнє лазерної зброї, як і майбутнє будь-якого озброєння, в подальшому залежить від розвитку теорії та практики бойових дій.

ЛІТЕРАТУРА:

1. Салливен Джон П. Оружие мира. Террористическое и нетрадиционное оружие. Справочник. – М.: Моркнига, 2009. – 57 с.

2. Лященко В.П. Торговля оружием: Оружие направленной энергии, разработка, создание, производство, применение. – М.: Экономика, 2013. – 350 с.

3. Лященко В.П. Торговля оружием: Оружие нелетального действия, создание, производство, применение, операции. – М.: Экономика, 2011. – 302 с.

4. Лесков А. Разработка за рубежом боевых лазерных систем для борьбы с низколетящими целями. – Зарубежное военное обозрение, 2014. – №4. – с. 51–52

5. Каку Мітіо. Физика невозможного. – М.: Альпіна паблішер, 2015. – 456 с.

6. Електронний ресурс: http://oko–planet.su/politik/politikarm/269293–oruzhie–napravlennoy–energii–segodnya–problemy–moschnosti–tepla–razmerov–i–tendencii–primeneniya.html

REFERENCES:

1. Sallyven Dzhon P. (2009). Oruzhye myra. Terrorystycheskoe y netradycyonnoe oruzhye. Spravochnyk. – M.: Morknyga – 2009. – 57 p. (In Russian).

2. Ljashhenko V.P. (2013). Torgovlja oruzhyem: Oruzhye napravlennoj эnergyy, razrabotka, sozdanye, proyzvodstvo, prymenenye. – M.: Эkonomyka – 2013. – 350 p. (In Russian).

3. Ljashhenko V.P. (2011). Torgovlja oruzhyem: Oruzhye neletal'nogo dejstvyja, sozdanye, proyzvodstvo, prymenenye, operacyy. – M.: Эkonomyka – 2011. – 302 p. (In Russian).

4. Leskov A. (2014). Razrabotka za rubezhom boevыh lazernыh system dlja bor'bы s nyzkoletjashhymy celjamy. – Zarubezhnoe voennoe obozrenye. – 2014. – №4. – p. 51–52. (In Russian).

5. Kaku Mitio. (2015). Fyzyka nevozmozhnogo. – M.: Al'pina pablisher –2015. – 456 p. (In Russian).

6. Elektronnyj resurs: http://oko–planet.su/politik/politikarm/269293–oruzhie–napravlennoy–energii–segodnya–problemy–moschnosti–tepla–razmerov–i–tendencii–primeneniya.html

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

к.т.н. Гришин С.П., к.т.н., с.н.с. Мирошниченко О.В., Бадрук О.О.

АНАЛИЗ МИРОВЫХ ПРОГРАММ И ПРОЕКТОВ СОЗДАНИЯ ОРУЖИЯ НАПРАВЛЕННОЙ ЭНЕРГИИ

В настоящее время все работы в области оружия направленной энергии идут во многих странах мира. Основными разработчиками оружия данного класса является прежде всего США, Китай и РФ. Хорошие результаты работы в этом направлении показывают также Израиль, Германия и Индия. Но если в Китае и РФ эти разработки являются, в основном, закрытыми для широкой общественности, то в США даже бесперспективные проекты подлежат массовому «пиару». В данной статье проведен анализ образцов и разработок оружия направленной энергии, по большей части, на примере США и на основе материалов, изложенных в открытых источниках.

Приведены последние достижения научно-технических программ по разработке лазерных систем для тактической обороны, перспективы развития лазерного оружия. Раскрыты проблемы, связанные с мощностью, тепловой емкостью и размерами вооружений данного класса.

Ключевые слова: оружие нелетального действия, оружие направленной энергии, анализ, поражающие факторы, типичные ситуации применения.

Ph.D. Grishin S.P., Ph.D. Miroshnichenko O.V., Badruk O.O.

ANALYSIS OF GLOBAL PROGRAMMS AND PROJECTS OF CREATION DIRECTED ENERGY WEAPONS

At present, all work in the DEW are in many countries. The main developers of this class of weapons is primarily the US, China, and Russia. Good results in this direction also show Israel, Germany and India. But if China and Russia, these developments are mostly closed to the public, in the United States even viable projects to be massive "PR". This article analyzed the samples and development DEW mainly on the example of the US and based on material contained in open sources.

Shows the latest scientific and technical programs to develop laser systems for tactical defense, prospects of development of laser weapons. The problems associated with power, thermal capacity and size of the weapons grade.

Keywords: weapons non-lethal action, directed energy weapons, analysis, factors affecting the typical situation of use.

УДК 621.396:519.876 к.т.н., с.н.с. **Жиров Г.Б.** (ВІКНУ)

МЕТОДИ ЦИФРОВОЇ ОБРОБКИ В ЗАДАЧАХ ІДЕНТИФІКАЦІЇ І ПРИДУШЕННЯ ЗАВАД СИГНАЛІВ УКХ ДІАПАЗОНУ

У статті розглянута задача придушення шумової складової корисного сигналу, який передається по радіоканалу УКХ діапазону (VHF), та його подальша ідентифікація засобами вейвлет аналізу. Були експериментально досліджені класичні задачі вейвлет аналізу, а саме вибір базової вейвлет-функції, визначення рівня розкладання (декомпозиції) сигналу, а також проаналізовано задачі вибору алгоритмічної процедури придушення шуму, критерію граничного порогу та виду трешолдінгу.

Експериментальні дані отримані методом математичного моделювання з використанням пакету MatLab.

Ключові слова: вейвлет аналіз, придушення шуму, ідентифікація сигналу, трешолдінг.

Вступ. Прийом радіосигналів завжди супроводжується перешкодами і шумами. При рівні перешкод, близькому до максимального значення сигналу, важко виявити навіть саму присутність корисного сигналу. Більшість сигналів містять випадкові перешкоди і «викиди» значень, тобто зміни сигналу, що різко виділяються які викликані небажаними або винятковими подіями. У системах радіолокації і радіозв'язку перешкоди в часовому ряду корисного сигналу можуть бути викликані різноманітними похибками і шумами, що виникли через наведення при проходженні даного сигналу по каналах зв'язку (білим, імпульсним і іншими видами шумів).

Такі «викиди» значень та шумові складові можуть спотворити результати аналізу істотних періодичних компонент сигналу, його тренда. Подальший аналіз, обробка та прогнозування часових рядів може здійснюватися лише за умови попереднього згладжування. Достовірне прогнозування та відновлення втрачених значень можливо лише при використанні згладжених часових рядів даних [1].

Постановка завдання. В статті розглядається питання придушення шумової складової корисного сигналу та його ідентифікацію з використанням вейвлет аналізу. Розглянуто метод очищення сигналів від шумів за допомогою вейвлетів: Хаара, Мейера, Добеши і Сімлета.

Результати дослідження. На сьогоднішній день революційна глобалізація комп'ютерних та мережевих технологій в промисловості, інтелектуалізація засобів вимірювальної техніки, що досягається впровадженням мікропроцесорної техніки, і лавиноподібний розвиток теорії вейвлет-аналізу, який супроводжується її широким залученням до вирішення проблем, що становлять коло сучасних практичних потреб, а саме забезпечення створення сприятливих умов для вирішення завдань обробки вимірювальної інформації та, зокрема, завдання придушення шуму. Поява ряду методологічних парадигм щодо придушення шуму, а також побудованих на їх основі програмних і апаратних реалізацій, в значній мірі просунули вирішення завдання придушення шуму, як однієї з головних завдань обробки. Своїм існуванням дані парадигми зобов'язані групам розробників з різних університетів США і в тому числі Д.Донохо і І.Джонстону (Стенфорд), які першими отримали найбільш цікаві результати, Ж.Керкьячаряну (Аміенс), групам С.Малла (Курант), Р. Койфмана (Єльський університет), М.Хілі (Дартмут), які працювали в напрямку обробки медичних зображень, а також Р.Девору (університет штату Південна Кароліна), Б.Лусье (Пердью), який отримав цікаві рішення задачі обробки сигналів з використанням теорії апроксимації [2].

Сутність вейвлет-аналізу полягає в тому, що сигнал, розкладається на апроксимуючі коефіцієнти – cA_i, які представляють згладжену, основну частину інформації сигналу, і деталізують коефіцієнти – cD_i, що описують уточнюючу інформацію про сигнал

(коливання), на різних рівнях розкладання i, $i = \overline{1, N}$, тобто високочастотні коливання щодо середніх значень [3,4].

Зазвичай передбачається, що сигнал шумової компоненти по модулю менше основного. При виконанні цієї умови найпростіший спосіб очищення сигналу від шуму полягає в присвоєнні нульових значень коефіцієнтів, що не перевищують деякого граничного значення. Ця процедура називається вейвлетною фільтрацією коефіцієнтів по заданому порогу (трешолдінгом) [4,5]. Від вибору порогового рівня фону (оцінки дисперсії шуму) залежить якість придушення шуму, що оцінюється в вигляді відносини сигнал / шум.

Існують різні види трешолдінга: м'який і жорсткий. При жорсткій пороговій обробці зберігаються незмінними всі коефіцієнти, великі або рівні по абсолютному значенню заданого порогу, а менші коефіцієнти обертаються в нуль. При м'якій пороговій обробці поряд з оберненням в нуль коефіцієнтів, по модулю менших порога, відбувається зменшення по модулю всіх інших коефіцієнтів на величину порога. Поріг може бути глобальним або різним для кожного рівня декомпозиції, в залежності від частотних особливостей сигналу що обробляється. Від вибору порогового рівня залежить якість згладжування сигналу.

Вейвлет-функції володіють властивість частотно-часової локалізації сигналів, а також швидкими обчислювальними алгоритмами. Таким чином, навіть в умовах нестаціонарності сигналів, наявності в них деякого вимушеного фону робить вейвлет-функції найкращим базисом для вирішення поставленого завдання. Дійсно, недостатня здатність аналізу Фур'є локалізувати сингулярності сигналів, необхідність введення в часовій області вікон даних і, як наслідок, розмивання спектру сигналів за рахунок появи помилкових пелюсток обумовлюють природний рух практики обробки сигналів до методів, що забезпечує краще частотно-часову роздільну здатність.

Рішення завдання придушення шуму, в загальному вигляді, незалежно від природи інформації, що оброблюється, та має комплексний характер, оскільки розділяється на вирішення цілого ряду підзадач. Серед таких підзадач можна відзначити, наприклад, перевірку достовірності гіпотези про гауссову статистику і спектральний склад шумовий компоненти, вибір типу функції порогової обробки (трешолдінга) і разом з цим критерію розрахунку самого порога, а також стандартні питання вейвлет-аналізу, що носять загальний характер: вибір найбільш підходящого вейвлет-базису, встановлення необхідної глибини розкладання даних і т.п.

Зупинимося детальніше на деяких часткових завданнях, а саме на виборі найбільш підходящого вейвлет-базису і глибини деталізації (декомпозиції) при придушенні шуму на виході приймача.

В якості еталонного сигналу, виступав прийнятий RTL SDR УКХ приймачем на стандартну антену сигнал на частоті ≈ 148 МГц (кількість відліків еталонного сигналу становить 249600 відліків). Даний сигнал був прийнятий і записаний на комп'ютер за допомогою ПЗ SDRSharp. Подальша обробка здійснювалась з використанням математичного пакету MatLab.

Як шумова складова (перешкода) був обраний білий Гаусовий шум. Даний вид шуму був промодельований в пакеті MatLab з кількістю відліків, який дорівнює кількості відліків еталонного сигналу (`su=0.1*randn(1,249600)`).

Досліджуваний сигнал отримали шляхом складання еталонного і шумового сигналів, що показано на рис 1.

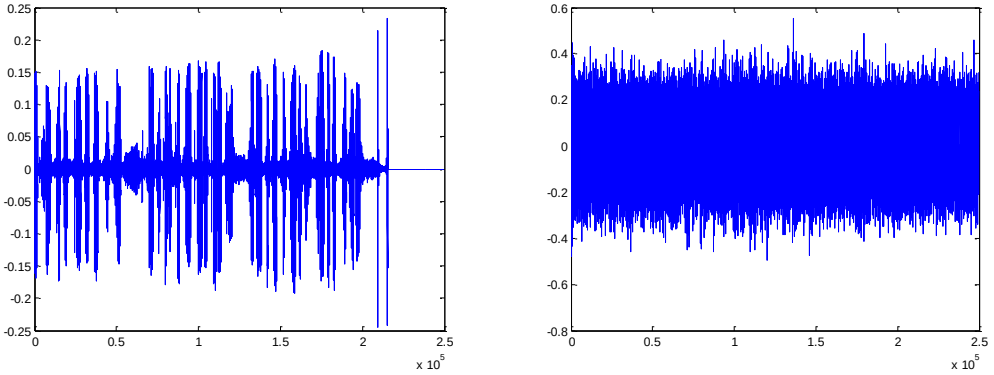
Експеримент по ідентифікації і придушення шуму проходив за такою методикою:

1. Декомпозиція сигналу. Обирається вейвлет і рівень розкладання N. Обчислюється вейвлет-розкладання вихідного сигналу до заданого рівня N.

2. Порогова обробка деталізують коефіцієнтів. Для кожного рівня вибирається поріг і застосовується порогова обробка деталізують коефіцієнтів.

3. Реконструкція сигналу. Проводиться вейвлет-реконструкція, яка заснована на початкових апроксимуючих коефіцієнтах і перетворених деталізуючих коефіцієнтах.

4. Визначається: найкращий вейвлет, рівень декомпозиції, критерій вибору порога і виду трешолдінга на основі обчислення коефіцієнта кореляції зразкового і реконструйованого сигналів, використовуючи команду `R = corrcoef` пакету MatLab.



а) б)

Рис. 1. Графіки еталонного (а) і досліджуваного сигналів (б)

I. Як базові, використовувалися вейвлети Хаара «haar», Добеши: «db2», «db4», «db8», дискретні апроксимації вейвлетів Мейєра «dmey» та сімплет «sym8».

II. В якості правила вибору порогового рівня застосовувалися критерії:

– адаптивної незміщеної оцінки ризику Штейна (Rigorous Sure), команда «rigrsure»;

– модифікований евристичний критерій Штейна (Heuristic Sure), команда «heursure»;

– універсальний критерій Донохью-Джонстона команда «sqtwolog»;

– мінімаксний критерій, команда «minimaxi»;

III. Як вид трешолдінга був використаний, як м'який (параметр 's'), так і жорсткий (параметр 'h') тредшолдінг.

В якості програмних процедур (функцій) придушення шуму та ідентифікації були використані: функція автоматизованого придушення шуму сигналу (wden); функція придушення шуму / стиснення (wdencmp); трешолдінг вейвлет-пакета (wptcoef). При використанні функції автоматизованого придушення шуму сигналу, як параметр були використані параметри мультиплікативного перемасштабування порога: значення 'mln' - дозволяє вказати необхідність використання порога, перераховується для кожного з рівнів розкладання даних; значення 'sln' - вказати необхідність використання порога, перерахованого тільки для першого рівня розкладання; значення 'one' - необхідність використання порога, єдиного для всіх рівнів розкладання. Також, на відміну від інших публікацій за подібною тематикою, при проведенні експерименту не застосовувався GUI Wavelet Toolbox пакету MatLab.

Результати експерименту. 1. Функція автоматичного придушенням шуму (без перемасштабування). На рис. 2 зображені графіки значень коефіцієнта кореляції двох сигналів від рівня декомпозиції. Найліпша подібність сигналів виявилася при розкладанні сигналу до 2-го рівня, а найліпшими базовими вейвлет-функціями виявились: «db8», «dmey» та «sym8». Вейвлет «dmey» виявився найкращім при усіх реалізаціях експерименту, а «db8» та «sym8» почергово займали другу ліпшу позицію.

Перемасштабування. На рис. 2 зображені графіки значень коефіцієнта кореляції двох сигналів від рівня декомпозиції. Найліпша подібність сигналів виявилася при розкладанні сигналу до 2-го рівня, а найліпшими базовими вейвлет-функціями виявились: «db8», «dmey» та «sym8». Вейвлет «dmey» виявився найкращім при усіх реалізаціях експерименту, а «db8» та «sym8» почергово займали другу ліпшу позицію.

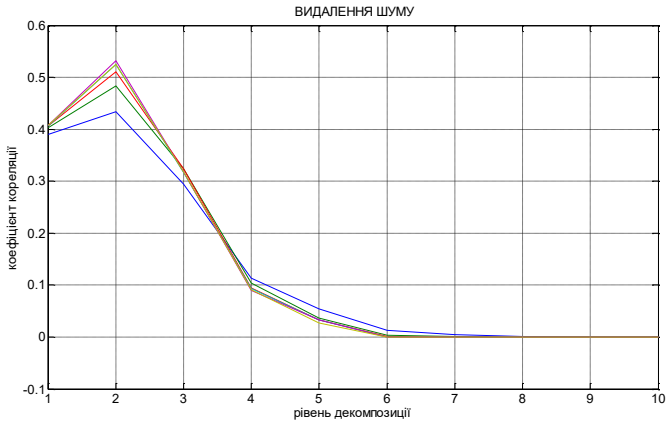


Рис. 2. Графік залежності коефіцієнта кореляції функція `wden`, параметр `'one'`

Суттєвих розбіжностей при переборі критеріїв вибору граничного рівня не було, кращій результат: модифікований евристичний критерій Штейна «`heursure`» з жорстким параметром трешолдінгу '`h`'.

2. Функція автоматичного придушення шуму (з використанням перемасштабування). Результати експерименту приведені на рис. 3, 4.

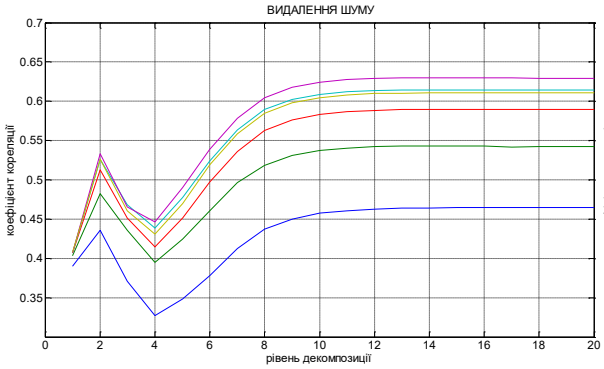


Рис. 3. Графік залежності коефіцієнта кореляції, функція `wden`, параметр `'sln'`

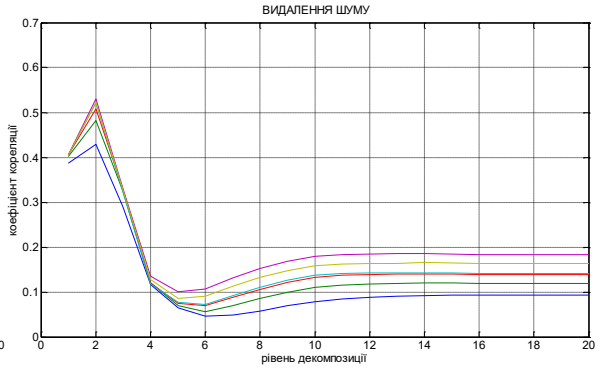


Рис. 4. Графік залежності коефіцієнта кореляції, функція `wden`, параметр `'mln'`

Результати (рис. 3), відповідають випадку застосування критеріїв адаптивної незміщенної оцінки ризику Штейна «`rigrsure`», та модифікованому евристичному критерію Штейна «`heursure`», а результати (рис.4) – критерію Донохо-Джонстона «`sqtwolog`»та мінімаксному критерію «`minimaxi`». Вибір виду трешолдінгу (м'який, жорсткий) для даних умов виявився не критичним. Найліпші результати при переборі вейвлетів отримані за допомогою вейвлетів: «`db8`», «`dmey`» та «`sym8`».

3. Функція придушення шуму/стиснення (`wdencmp`). Результати приведені на рис. 5.

4. Функція трешолдінгу вейвлет-пакета (`wptcoef`). Результати приведені на рис. 6.

Аналіз експериментальних даних показує: найліпший рівень декомпозиції дорівнює – 2-му рівню, а базова вейвлет-функція – «`dmey`». Також гарні результати отримані при застосування вейвлетів «`db8`», та «`sym8`». Вибір критерію визначення граничного порогу, як і для попередніх результатів, виявився не критичним. Найліпші результати при виборі функції (`wdencmp`): вейвлет - «`dmey`», критерій - адаптивної незміщенної оцінки ризику Штейна «`rigrsure`», а при функції (`wptcoef`): вейвлет - «`dmey`», критерій – мінімаксний «`minimaxi`».

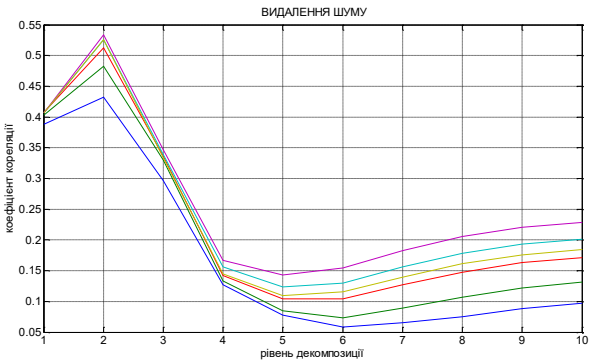


Рис. 5. Графік залежності коефіцієнта кореляції, (`wdencmp`)

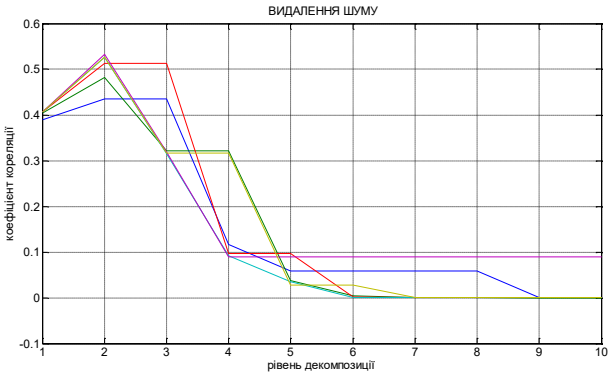


Рис. 6. Графік залежності коефіцієнта кореляції, (`wptcoef`)

Основний скрипт, який був використаний при дослідженні:

```
load SDRSharp_1;
su=0.1*randn(1,249600);%шум
SUS=SDRSharp_1+su;%Образцовый сигнал+шум
for i=1:1:10;
   SUS_H=wden(SUS,'heursure','h','one',i,'dmey');
   R=corrcoef(SDRSharp_1,SUS_H);
   RR_dmey(1,i)=R(1,2);
end
```

Висновки. При вирішенні задачі придушення шумової складової в сигналі УКХ приймача з подальшою ідентифікацією засобами вейвлет аналізу, можна зробити наступні висновки:

1. На підставі проведеного аналізу існуючих підходів до фільтрації нестаціонарних сигналів в якості математичного апарату обраний кратномасштабного вейвлет-аналіз, застосування якого дозволяє виділити і зберегти локальні особливості сигналу.

2. Материнський вейвлет для проведення фільтрації повинен мати властивість ортогональності і можливістю реконструкції сигналу.

3. В якості «материнського» вейвлету доцільно використовувати дискретну аппроксимацію вейвлетов Мейера «`dmey`», а також Добеши «`db8`» та симплет «`sym8`».

4. Декомпозиція сигналу до другого рівня виявилася найліпшою, практично при усіх експериментах.

5. Вибір критерію щодо визначення порогу та виду трешолдінгу суттєво не впливають на результати ідентифікації.

6. При наявності суттєвих вимог по швидкодії аналізу, вейвлет «`dmey`» використовувати не доцільно т.я. для нього недоступні швидкі алгоритми.

ЛІТЕРАТУРА:

1. Белов А.А Сглаживание временных рядов на основе вейвлет-преобразования в системах автоматизированного экологического мониторинга / А.А. Белов, А.Ю.Проскуряков.// Методы и устройства передачи информации.– 2010. – Вып.12. – С.21-24.

2. Алексеев К.А. Теория и практика шумоподавления в задаче обработки сейсмоакустических сигналов. http://matlab.exponenta.ru/wavelet/book5/index.php

3. Солонина А.И. Цифровая обработка сигналов. Моделирование в MATLAB / А.И. Солонина, С.М. Арбузов. – СПб.: БХВ. Петербург, 2008. – 816 с.

4. Смоленцев Н.К. Основы теории вейвлетов. Вейвлеты в MATLAB. / Н.К.Смоленцев. – М.:ДМК Пресс, 2005. – 304 с.

5. Московский С.Б. Очистка сигнала от шумов с использованием вейвлет-преобразования / С.Б.Московский, А.Н.Сергеев, Н.А.Лалина // Universum: Технические науки: электрон. научн. журн. 2015. № 2 (15) URL: http://7universum.com/ru/tech/archive/item/1958

REFERENCES:

1. Belov A.A Sglazhivanie vremennyh riadov na osnove veivlet-preobrazovaniia v sistemah avtomatizirovannogo ekologicheskogo monitoringa / A.A. Belov, A.Iu.Proskuriakov.// Metody i ustroistva peredachi informatsii. – 2010. – Vyp.12. – S.21–24.

2. Alekseev K.A. Teoriia i praktika shumopodavleniia v zadache obrabotki seismoakusticheskih signalov. http://matlab.exponenta.ru/wavelet/book5/index.php

3. Solonyna A., Arbuzov A. Cyfrovaja obrabotka sygnalov. Modelyrovanye v MATLAB (2008), S. – SPb.: BHV. Peterburg, 816.

4. Smolentsev N. Osnovy teorii veivletov. Veivlety v MATLAB. (2005), M.:DMK Press, 304.

5. Moskovskii S.B. Ochistka signala ot shumov s ispol'zovaniem veivlet-preobrazovaniia / S.B.Moskovskii, A.N.Sergeev, N.A.Lalina // Universum: Tehnicheskie nauki: elektron. nauchn. zhurn. 2015. № 2 (15) URL: http://7universum.com/ru/tech/archive/item/1958.

Рецензент: д.т.н., проф. Жердєв М.К., Військовий інститут телекомунікації та інформатизації

к.т.н., с.н.с. Жиров Г.Б.

МЕТОДЫ ЦИФРОВОЙ ОБРАБОТКИ В ЗАДАЧАХ ИДЕНТИФИКАЦИИ И ПОДАВЛЕНИЯ ПОМЕХ СИГНАЛОВ УКВ ДИАПАЗОНА

В статье рассмотрена задача подавления шумовой составляющей полезного сигнала, который передается по радиоканалу УКВ диапазона (VHF), и его дальнейшая идентификация средствами вейвлет анализа. Были экспериментально исследованы классические задачи вейвлет анализа, а именно выбор базовой вейвлет-функции, определение уровня разложения (декомпозиции) сигнала, а также проанализированы задачи выбора алгоритмической процедуры подавления шума, критерия предельного порога и вида трешолдинга.

Экспериментальные данные получены методом математического моделирования с использованием пакета MatLab.

Ключевые слова: вейвлет анализ, подавление шума, идентификация сигнала, трешолдинг.

Ph.D. Zhyrov G.B.

METHODS OF DIGITAL PROCESSING IN THE PROBLEM OF IDENTIFICATION AND SUPPRESSION NOISE SIGNALS VHF

In the article the problem of noise suppression component signal, which is transmitted via radio VHF, and its subsequent identification by means of wavelet analysis. Were experimentally studied classical problem of wavelet analysis, namely the choice of basic wavelet function, determine the level of decomposition (decomposition) signal, and analyzes the problem of choice algorithmic procedure suppress noise limit threshold criterion and type thresholding.

Experimental data obtained by using mathematical modeling package MatLab.

Keywords: wavelet analysis, noise suppression, identification signal thresholding.

УДК 621.396.6

к.т.н. **Коваленко І.Г.** (НЦЗІ ВІТІ)
Міщенко А.О. (НЦЗІ ВІТІ)
Вавасова О.С. (НЦЗІ ВІТІ)

АНАЛІЗ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ ЗАСОБІВ РАДІОЗВ'ЯЗКУ

У статті запропоновані методики аналізу електромагнітної сумісності (ЕМС), що призначені для визначення можливого взаємного впливу групи радіоелектронних засобів (РЕЗ) зв'язку. Запропоновані методики базуються на сучасних рекомендаціях Міжнародного союзу електрозв'язку (МСЕ). Особливістю розроблених методик є їх орієнтація на практичну реалізацію для отримання комплексного рішення задачі аналізу електромагнітної сумісності засобів зв'язку. Також, особливістю методик є зменшення складності розрахунків шляхом поділення аналізу на два етапи – попередній та детальний. На попередньому етапі здійснюється вибір і аналіз ЕМС РЕЗ за частотно-територіальною ознакою. На етапі детального аналізу проводяться розрахунки ЕМС з урахуванням можливого впливу побічних та інтермодуляційних випромінювать, а також можливості блокування приймачів при розташуванні групи РЕЗ в обмеженому просторі. Запропоновані методики передбачають зменшення обсягу складних розрахунків для окремих складових задач аналізу ЕМС, які вимагають надлишок точних вихідних даних, при відсутності частини яких складні розрахунки за запропонованими МСЕ методиками можуть привести до неприйнятних результатів.

Ключові слова: радіоелектронний засіб, електромагнітна сумісність.

Актуальність. Останнім часом спостерігається тенденція перевантаження радіочастотного спектру внаслідок розвитку радіотехнологій, збільшення кількості радіозасобів. Тому постає актуальною задача забезпечення якісного функціонування цих засобів у спільних та суміжних діапазонах радіочастот [1-4]. Для вирішення цієї задачі необхідно застосовувати методи та методики прогнозування електромагнітної обстановки та аналізу електромагнітної сумісності (ЕМС).

Загальні підходи та окремі методики вирішення задач даного класу викладені в множині рекомендацій Міжнародного союзу електрозв'язку (МСЕ) [2]. Але запропоновані рекомендації не дають комплексного рішення задачі аналізу електромагнітної сумісності засобів зв'язку, дозволяють проводити окремі складні розрахунки для складових (часткових) задач аналізу ЕМС та вимагають багато точних вихідних даних (щодо параметрів устаткування, рельєфу, параметрів розповсюдження радіохвиль тощо). При відсутності частини цих вихідних даних (або зниженні їх точності) складні розрахунки за запропонованими МСЄ методиками можуть привести до неприйнятних результатів, що ускладнює оперативного вирішення задач даного класу.

Задача дослідження – розробка методик, призначених для аналізу електромагнітної сумісності радіоелектронних засобів шляхом проведення практичних розрахунків її параметрів.

Вихідні дані. В запропонованих методиках використовуються наступні вихідні дані.

1. Множина з РЕЗ з відповідними технічними характеристиками:

- тип РЕЗ (аналоговий, цифровий сигнал);
- потужність пристрою, що передає, P, дБВт;
- спектральні характеристики сигналу, що випромінюється $S(f)$;
- коефіцієнт підсилення антени G, її тип, поляризація випромінювання і втрати в антенно-фідерному тракті η;
- характеристика спрямованості антени $g(\alpha)$;
- клас випромінювання;
- ширина смуги пропускання приймача по проміжній частоті на рівні –30 дБ, МГц і форма амплітудно-частотної характеристики;
- чутливість приймача, дБВт, мВ/м, (коефіцієнт шуму, дБ);

- швидкість цифрового потоку, біт/с;

- припустимий рівень помилок і величина захисного відношення для заданого відсотку часу.

2. Смуги частот, які використовуються.

3. Характеристики місць розташування об'єктів РЕЗ:

- географічні координати місця розташування РЕЗ, градуси, хвилини, секунди північної широти, східної довготи;

- висота основи РЕЗ над рівнем моря, м;

- висота підвісу антени над рівнем Землі, м.

4. Характеристики місцевості: висота над рівнем моря та покриття (вода, рослинність тощо).

Для виконання завдань з аналізу електромагнітної сумісності засобів радіозв'язку (ЗР) в залежності від типу РЕЗ, умов їх функціонування та розташування пропонується використовувати ряд пов'язаних між собою розроблених методик (рис.1):

I. Методика аналізу ЕМС засобів радіозв'язку фіксованої радіослужби (ФР) [5].

II. Методика аналізу ЕМС засобів радіозв'язку рухомої радіослужби (РР) [6].

III. Методика аналізу об'єктової ЕМС засобів радіозв'язку [7].

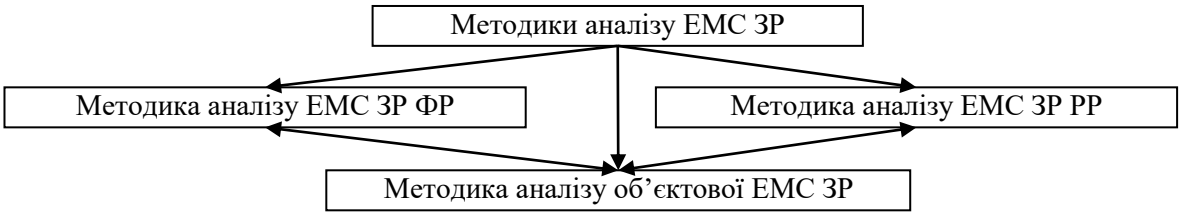


Рис. 1

Основним критерієм для визначення електромагнітної сумісності РЕЗ в розроблених методиках використовується *енергетичний критерій*, який виражається відношенням сигнал/(шум+завада) при заданих показниках якості, що представляється у вигляді коефіцієнта ослаблення завад (коефіцієнта втрат) при вирішенні задач ЕМС РЕЗ [8-11]:

$$P_c \big/ P_з = A(\Delta f) = A_0 N(\Delta f), \qquad (1)$$

де $A(\Delta f)$ – захисне відношення при заданій частотній розлад Δf між корисним сигналом і завадою для визначеного відсотку часу; A_0 – захисне відношення по суміщеному каналу для визначеного відсотку часу; $N(\Delta f)$ – коефіцієнт, який характеризує ослаблення завади в залежності від частотного розладу між корисним сигналом і завадою; P_c – потужність корисного сигналу на вході приймача, який зазнає впливу завад, яка дорівнює (в вільному просторі).

Необхідні захисні відношення $A(\Delta f)$, A_0 в (1) залежать від флуктуації рівнів сигналів на вході приймача, які є випадковими величинами, їх закон розподілення для різних відсотків часу точно невідомий. В Рекомендаціях МСЭ-R приведені наближені залежності відсотку часу перевищення глибини завмирань для найгіршого місяця року.

В загальному випадку, наприклад, для аналогових РРЛ з частотною модуляцією (ЧМ), коли безперервна частина спектру сигналу завади не повністю співпадає з смугою пропускання приймача, ослаблення завади в лінійній частині приймача, за рахунок розладу, враховується коефіцієнтом $N(\Delta f)$. В цьому випадку захисне відношення для 20 % часу дії завад виражається формулою [10]: $A(20\%, \Delta f) = 55+N(\Delta f)$, а для 0,001 % часу дії завад відповідно: $A(0{,}001\%, \Delta f) = 25+N(\Delta f)$. Для практичних розрахунків параметрів ЕМС аналогових РРЛ найбільш доцільно використовувати довідкові дані захисних відношень [12].

Для більшості типів аналогових РРЛ необхідне захисне відношення для 20% складає 55 дБ, а для 0,001% відповідно 25 дБ [12].

На відміну від аналогових РРЛ для цифрових систем показниками якості є допустима величина вірогідності помилок $P_{ош}$, яка не повинна перевищувати задане значення протягом визначеного відсотку часу любого місяця року, та відповідне необхідне захисне відношення $A_0(P_{ош})$. В [12] наведені вирази якісних параметрів систем з різними типами цифрової модуляції. Так, для РРЛ з фазо-імпульсним модульованим сигналом величина захисного відношення для 20 % часу, визначається емпіричною формулою [18] $A(20\%, \Delta f)=15+N(\Delta f)$, а для 0,001 % часу відповідно: $A(0{,}001\%, \Delta f)=18+N(\Delta f)$, для цифрових РРЛ величина захисного відношення для 0,001 % часу розраховується згідно виразу: $A(0{,}001\%, \Delta f)=25+N(\Delta f)$. Значення величин захисних відношень та значення коефіцієнта $N(\Delta f)$ надані в [12].

Другим критерієм ЕМС для цифрових систем є допустима величина *вірогідності помилок* $P_{пом}$, яка не повинна перевищувати задане значення протягом відповідного відсотку часу любого місяця року при відповідному необхідному захисному відношенні $A_0(P_{пом})$. Так, відповідно до Рекомендації МСЕ-Р F.594 [13] значення імовірності помилок 10^{-3} наприкінці гіпотетичної цифрової РРЛ, довжиною 2500 км, яка складається з 50 прольотів, не повинне перевищувати протягом більш $P_т$ = 0,054% часу будь-якого місяця року, а значення імовірності помилок $P_{пом}=10^{-6}$ відповідно протягом більш $P_т$ = 0,4% часу будь-якого місяця року. Допустимі значення $P_т$ визначені в Рекомендації МСЕ-Р F.634 [14].

Розрахунок послаблень радіосигналів за рахунок розповсюдження

В залежності від частот та умов рельєфу місцевості в методиках використовуються окремі алгоритми розрахунку [5]*:*

Розрахунок послаблень радіосигналів за рахунок розповсюдження в діапазонах 30-1000 МГц істотно залежить від конкретного профілю траси [10]. Так, наприклад, у випадку відкритої траси втрати ($L_{вт}$) являють собою втрати вільного простору, що визначені відповідно до формули:

$$L_{вт} = 32{,}5+20\cdot\lg(f)+20\cdot\lg(d),$$

де f – частота, МГц; d – протяжність траси, км.

Розрахунок послаблень радіосигналів за рахунок розповсюдження в діапазонах вище 1000 МГц пропонується проводити відповідно Рекомендації МСЕ-R Р.452 [10], у якій містяться рекомендації щодо урахування наступних механізмів розповсюдження радіохвиль: розповсюдження у вільному просторі; дифракція; тропосферне розсіювання; аномальне розповсюдження радіохвиль, а також втрати за рахунок забудови (там, де це необхідно).

Формули розрахунків за рекомендаціями МСЕ-R значно спрощуються, якщо врахувати, що в розроблених методиках практичне значення для розрахунків мають, по-перше, медіанні значення потужності сигналу та завади та, по-друге, відстань між передавачем, що заважає, (або джерелом корисного сигналу) та приймачем не більше 150 км. Перше означає, що $L=L(p=50\%)$; друге – що втратами за рахунок аномального розповсюдження для РРЛ можна знехтувати, так як вони становляться сумірними з втратами за рахунок тропосферного розсіювання та дифракції на трасах протяжністю більше 250-300 км ($10^{-0{,}2\,La} = 0$ дБ) [12].

Урахування характеристик та спрямованості антен при розрахунку параметрів ЕМС

Параметри та діаграми спрямованості (ДС) антен, які входять у вирази для розрахунку параметрів ЕМС РЕЗ, найбільш вірогідно визначаються на підставі виміру електродинамічних параметрів антен в конкретному місці установки. Однак при аналізі параметрів ЕМС РЕЗ таких даних найчастіше не буває. Тому для розрахунку ДС пропонується використовувати або аналітичні вирази (відомі з теорії антен та рекомендацій МСЕ), або вирази, що представляють собою апроксимації статистично усереднених ДС антен. В останньому випадку ДС визначається з деяким невеликим запасом, що, у свою чергу, призводить до більш жорстких умов дотримання ЕМС РЕЗ.

І. Методика аналізу електромагнітної сумісності засобів радіозв'язку фіксованої радіослужби

При побудові методики та відповідного алгоритму були враховані наступні фактори: практичне призначення методики і відповідного алгоритму розрахунків ЕМС РЕЗ та необхідність проведення великої кількості розрахунків. В запропонованій методиці для зменшення часу аналізу (розрахунків) в алгоритмі використано кілька етапів відбору потенційно завадових випромінювань (по частоті, по відстані, по попередньо визначеному рівню сигналу) і виключення з аналізу джерел завад, які не представляють небезпеки функціонуванню приймачу.

Методика включає в себе декілька ***етапів***, з яких будується відповідний алгоритм (рис. 2).

1. Введення вихідних даних (груп передавачів, приймачів, джерел корисного сигналу та їх характеристик, розташування тощо).

2. Визначається рівень корисного сигналу. Якщо рівень корисного сигналу не відомий, використовується чутливість приймача, в іншому випадку – розраховується очікуване значення сигналу для приймача, що аналізується.

3. Проводиться відбір РЕЗ, які потенційно можуть створювати завади, за критерієм максимального частотно-територіального рознесення (по заданій максимально можливій відстані та перетином частотних діапазонів між джерелом і рецептором завад). З усього угруповання РЕЗ виділяються РЕЗ, які підлягають подальшому аналізу ЕМС.

4. Для оцінки рівня завад на вході приймача організується проведення почергового аналізу впливу завад окремих випромінювачів (завад) на кожний приймач в угрупованні РЕЗ.

5-7. Проводиться *енергетичний відбір* для обраної пари *передавач-приймач.* Для цього оцінюється рівень сигналу, що заважає, на вході приймача і поріг добору, які визначаються відповідно розділу 1 загального опису методики. Селективні властивості приймача по частоті до уваги не беруться. Після порівняння рівнів завад з порогом, виключаються з розгляду випромінювачі, сигнали яких лежать нижче порогу. На цьому ж етапі виділяються і запам'ятовуються сигнали, які можуть бути причиною нелінійних ефектів (інтермодуляції і гармонік до *n*-го порядку включно) у приймачі. Розрахунки проводяться окремо для поточного приймача (тільки після завершення аналізу й оцінки ЕМС РЕЗ, до складу якого входить даний приймач, виконується вибір нового приймача і процес аналізу сумісності повторюється з пункту 2).

8-10. На етапі *частотного відбору* встановлюються можливі канали проникнення завади (основний або суміщений канали), розраховується рівень завади на вході приймача, з урахуванням селективних властивостей приймача і знову виконується порівняння з порогом. При цьому слід відмітити, що нелінійні ефекти (гармоніки, інтермодуляція і т. і.) можуть проявлятися при розміщенні РЕЗ на локальних об'єктах (на близьких відстанях). Для спрощення урахування небажаних випромінювань використовується заданий рівень побічних випромінювань передавача (-60 дБ).

11-12. Сигнали, які заважають і пройшли цей етап відбору, підлягають додатковому аналізу і їхній рівень корегується з урахуванням наявних у приймачі засобів подавлення або захисту від завад. Для завад, які визнані потенційно небезпечними, після всіх етапів добору, розраховується необхідне захисне відношення і прогнозоване відношення сигнал/завада відповідно розділу 1 загального опису методики. Потім, виконується їхнє порівняння. Якщо відношення сигнал/перешкода менше необхідного захисного відношення, то розраховується необхідне додаткове ослаблення завади.

13-15. Після завершення аналізу впливу окремих випромінювачів по основному і побічному каналах прийому, у разі необхідності, проводиться розрахунок параметрів нелінійних ефектів, які можуть виникнути в приймачі від сигналів, що заважають, виділених на першому етапі аналізу.

16. Несприятливі результати аналізу, у тому числі й аналізу взаємодії сигналів, що заважають, зберігається для подальшого використання з зазначенням виду нелінійного ефекту і джерел завад, які їх породжують. Інформація про небезпечний випромінювач, канал проникнення завади і необхідне її ослаблення надається посадовій особі, що приймає рішення про надання висновку щодо електромагнітної сумісності РЕЗ. Останній етап методики закінчується після завершення аналізу якості роботи всіх приймачів угруповання РЕЗ, інакше здійснюється перехід до пункту 2.

II. Методика аналізу електромагнітної сумісності засобів радіозв'язку рухомої радіослужби

Запропонована методика передбачає використання моделі розрахунку, що містить парну і групову оцінку при простій логіці взаємного впливу РЕЗ в угрупованні, яка заснована на імовірнісному (статистичному) підході до оцінки [1]. Проста логіка припускає, що кожен з пристроїв у групі можна розглядати як функціонально незалежний від інших засобів. Запропонована методика може використовуватись при ЧТП для оцінки можливості застосування частотних присвоєнь.

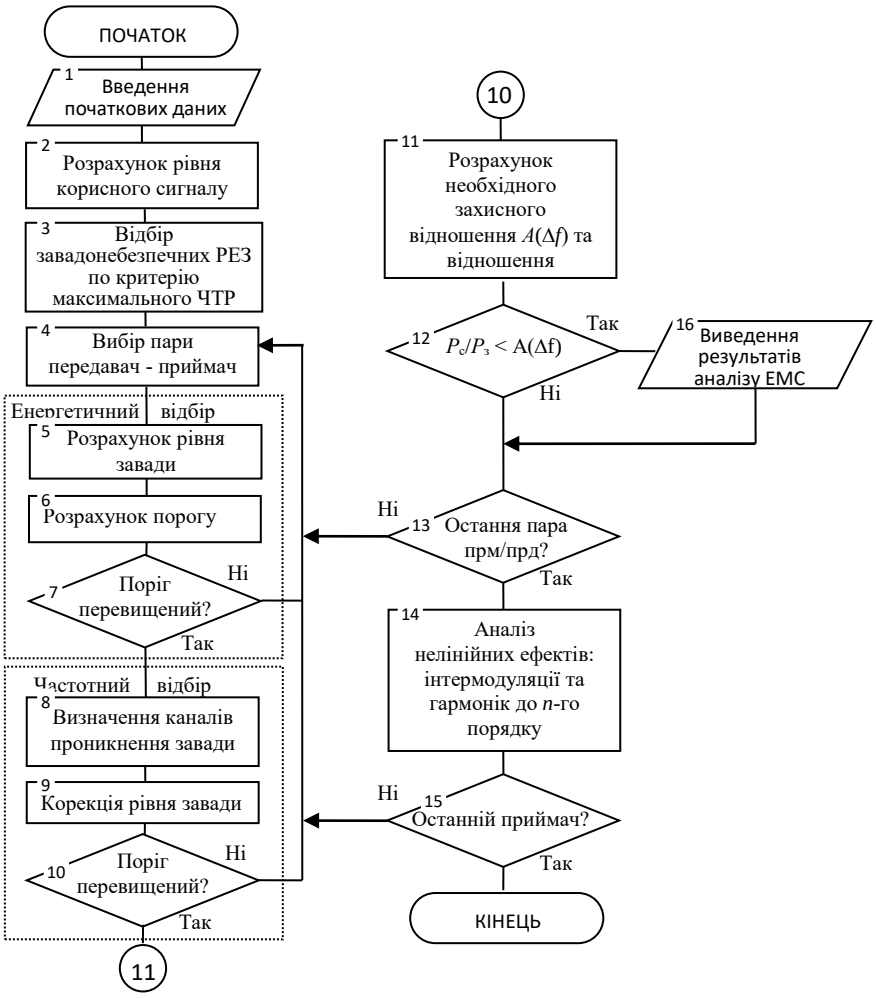


Рис. 2. Загальний алгоритм аналізу ЕМС РЕЗ фіксованої радіослужби

Розрахунок ЕМС РЕЗ виконується в наступному порядку:

вибір РЕЗ по територіальній ознаці, які розміщені в межах обмеженої зони дослідження;

добір з РЕЗ, обраних по територіальній ознаці, що потенційно можуть заважати новому частотному присвоєнню РЕЗ по частотній ознаці:

визначення можливих джерел завад по основному каналу;

визначення можливих джерел завад по першому сусідньому каналу;

визначення можливих джерел завад інтермодуляції 3-го порядку;

розрахунок рівня завад на вході приймача:

- по основному каналу;
- по першому сусідньому каналу;
- інтермодуляції 3-го порядку;

аналіз отриманих результатів і ухвалення рішення за результатами розрахунків про можливість частотного присвоєння з урахуванням впливу множинної завади або необхідності вибору іншої частоти.

Для оптимізації розрахунків пропонується аналіз ЕМС проводити в два етапи: попередній та детальний. На попередньому етапі проводиться попередній відбір та аналіз ЕМС для визначених частот. При детальному аналізі проводиться розрахунок ЕМС з урахуванням впливу побічних випромінювань, можливостей блокування приймача та впливу інтермодуляційних складових завад.

Етапи методики

Загальний алгоритм проведення частото присвоєння та аналізу ЕМС для РЕЗ рухомої радіослужби (рис. 3) містить:

1. Введення початкових даних.
2. Вибір вільної частоти f_{new} в межах розрахункової зони.
3. Вибір діючих РЕЗ в межах розрахункової зони. Вибираються станції, які знаходяться в подвійному радіусі зони обслуговування станції d, для якої визначається частота (рис 4.). Зона обслуговування визначається відповідно до стандарту для даного виду зв'язку і діапазону частот [4].

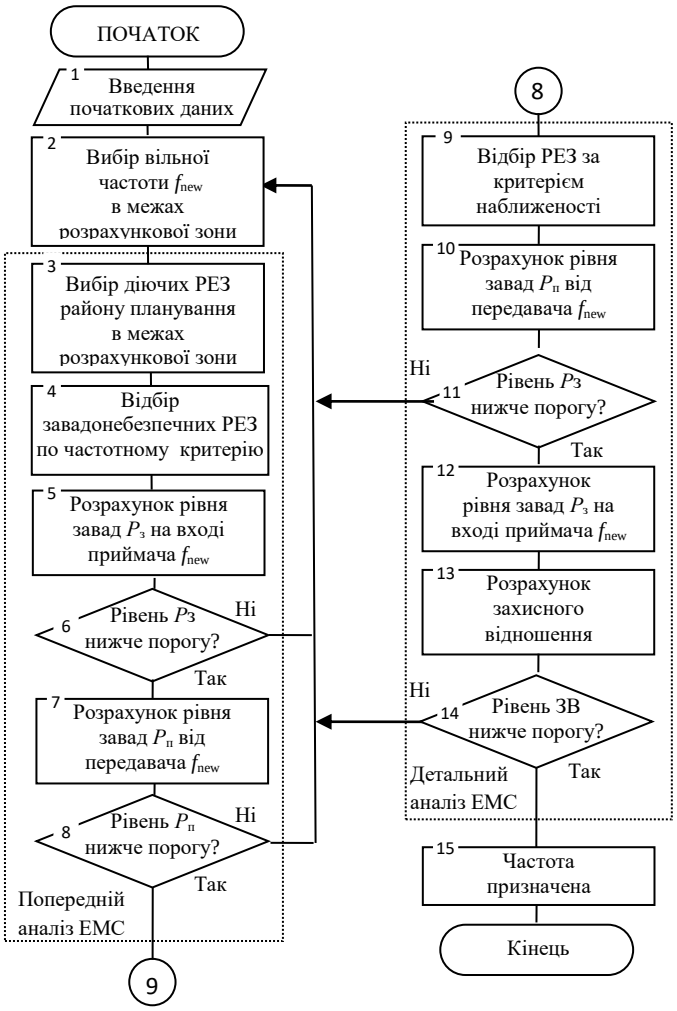


Рис. 3. Загальний алгоритм проведення частото присвоєння та аналізу ЕМС для РЕЗ рухомої радіослужби

4. Відбір завадо небезпечних РЕЗ по частотному критерію проводиться на основі аналізу завадових ситуацій. Базова станція (БС), для якої проводиться частотне планування, разом з мобільною станцією (МС), можуть створювати завади іншим базовим або рухомим станціям, а також зазнавати від них. Тому можуть виникати такі завадові ситуації, які вимагають наступних різних способів розрахунку.

Базова станція БС$_i$ створює завади іншій базовій станції БС. Для визначення відношення сигнал/завада джерело сигналу МС визначається на максимально можливій відстані від БС в межах зони обслуговування (рис. 5). Тоді очікуваний корисний сигнал $P_к$ і завада $P_з$ будуть визначатись:

$$P_{\text{к}} = P_{\text{МС}} - L_{\Sigma}\,,\; P_{\text{з}} = P_{\text{БС}_i} - L_{\Sigma_i}$$

де $P_{\text{МС}}$ – потужність передавача рухомої станції, $P_{\text{БС}i}$ – потужність передавача базової станції, яка заважає; L_{Σ} – сумарні втрати розповсюдження сигналу, L_{Σ_i} – сумарні втрати розповсюдження завади.

Базова станція БС$_i$ створює завади мобільній станції МС. Для визначення відношення сигнал/завада рівень прийому рецептора завад МС визначається на лінії, що з'єднує базові станції, на максимальній відстані від джерела сигналу БС і на мінімальній відстані від джерела завади БС$_i$ у межах своєї зони обслуговування (рис. 6). Очікуваний корисний сигнал $P_к$ і завада $P_з$ будуть визначатись:

$$P_{\text{к}} = P_{\text{БС}} - L_{\Sigma}\,,\; P_{\text{з}} = P_{\text{БС}_i} - L_{\Sigma_i}\,,$$

де $P_{\text{БС}}$ – потужність передавача базової станції.

У випадку якщо зона обслуговування невідома і неможливо визначити рівень очікуваного корисного сигналу, від приймається рівним чутливості МС.

Мобільна станція МС$_i$ створює заваду БС. Для визначення відношення сигнал/завада джерело сигналу МС визначається на максимальній відстані від базової станції БС, а джерело завад МС$_i$ визначається на лінії, що з'єднує базові станції, на максимальній відстані від джерела сигналу БС і на мінімальній відстані від джерела завади БС$_i$ у межах своєї зони обслуговування (рис. 7). Тоді очікуваний корисний сигнал $P_к$ і завада $P_з$ будуть визначатись:

$$P_{\text{к}} = P_{\text{МС}} - L_{\Sigma}\,,\; P_{\text{з}} = P_{\text{МС}_i} - L_{\Sigma_i}\,,$$

де $P_{\text{МС}_i}$ – потужність передавача мобільної станції завади.

У випадку якщо зона обслуговування невідома і неможливо визначити рівень очікуваного корисного сигналу, він приймається рівним чутливості базової станції.

Мобільна станція МС$_i$ створює заваду іншій мобільній станції МС. Для визначення відношення сигнал/завада рівень сигналу на вході рецептору завад МС визначається на максимальній відстані від джерела сигналу БС і на мінімальній відстані від джерела завади МС$_i$ в межах своєї зони ослуговування (рис. 8). Тоді очікуваний корисний сигнал $P_к$ і завада $P_з$ будуть визначатись:

$$P_{\text{к}} = P_{\text{БС}} - L_{\Sigma}\,,\; P_{\text{з}} = P_{\text{МС}_i} - L_{\Sigma_i}\,.$$

У випадку коли зона обслуговування невідома і неможливо визначити рівень очікуваного корисного сигналу, від приймається рівним чутливості рухомої станції

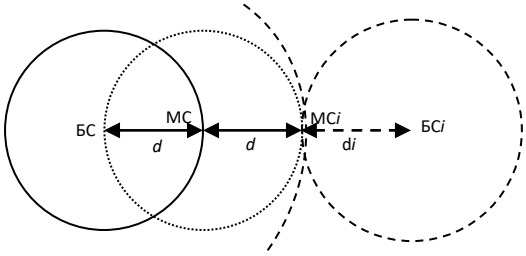


Рис. 4

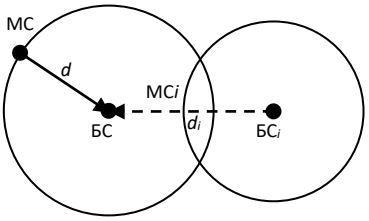


Рис. 5

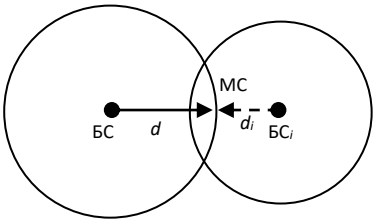


Рис. 6

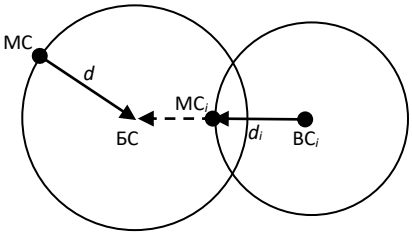


Рис. 7

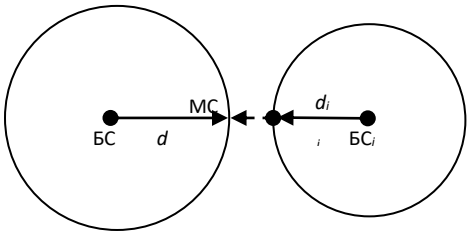


Рис. 8

5. Розрахунок рівня завад $P_з$ на вході приймача по основному і сусідньому каналах визначається для всіх випадків, визначених в п.4 коли станція, що планується, є станцією приймачем(передавачем) корисного сигналу. У випадку декількох станцій, що заважають, для визначення сумарної завади пропонується використовувати метод складання потужностей [6]:

$$E = 20 \lg \sum_{i=1}^{n} 10^{\frac{E_i}{20}},$$

де E_i – значення напруженості поля для кожного з джерел завад, n – число джерел завад, E – ефективне значення сумарної завади.

6. Аналіз отриманих результатів попереднього розрахунку містить розрахунок відношення сигнал/завада для кожного виду завад. Якщо відношення сигнал/завада нижче визначеного захисного відношення, здійснюється вибір наступної вільної частоти (п.2).

7. Розрахунок рівня завад від передавача аналогічний п.5 для випадків, визначених в п.4 коли завадою є станція, що планується.

8. Аналіз отриманих в п.7 результатів попереднього розрахунку містить розрахунок відношення сигнал/завада. Якщо відношення сигнал/завада нижче визначеного захисного відношення, здійснюється вибір наступної вільної частоти (п.2), інакше здійснюється перехід до детального аналізу.

9. Здійснюється відбір РЕЗ за критерієм наближеності. Для подальших розрахунків обираються РЕЗ в межах радіусу зони обслуговування.

10. Проводиться розрахунок можливих завад від відібраних в п.9 станцій по сусіднім та дзеркальним каналам, завадам на гармоніках та інтермодуляційним завадам. Розрахунок сумарної завади $P_{з\sum}$ для кожної станції в межах визначеної зони проводиться відповідно методиці [7] і містить наступні етапи:

розрахунок (вимір) величин і форм спектрів завад на вході приймача.

розрахунок сумарної потужності завад на вході підсилювача радіочастоти.

визначення сполучень завад, які формують на виході підсилювача радіочастоти продукти інтермодуляції на частотах основного та дзеркального каналів.

визначення величин і форм спектрів продуктів інтермодуляції на виході підсилювача радіочастоти.

визначення сумарної потужності продуктів інтермодуляції на виході фільтра ПЧ.

порівняння розрахованих значень сумарних потужностей завад із допустимими:

$$P_{\text{п}} < P_{\text{пд}} \text{ та } P^{\text{і}} < P_R - A_{\text{о}},$$

де $P_{\text{п}}$ ($P_{\text{п}}$) – сумарний (допустимий) рівень завад на вході приймача, P^{i} – сумарний рівень інтермодуляційних складових завад; P_R – чутливість приймача; A_0 – захисне відношення.

При одночасному виконанні вищевказаних умов робиться висновок про виконання умов ЕМС відносно розглянутого приймача по блокуванню та інтермодуляції. При невиконанні кожної з вищевказаних нерівностей робиться вивід про невиконання відповідних умов ЕМС.

11. Якщо нове частотне присвоєння призводить до перевищення порогу сумарною завадою, здійснюється перехід до вибору нової частоти (п.2).

12. Окремо проводиться аналіз об'єктової електромагнітної сумісності для приймача РЕЗ, що планується, відповідно методиці [7] (аналогічно п.10).

13. Визначається необхідне захисне відношення для приймача РЕЗ, що планується, з урахуванням частотної вибірковості приймача.

14. При перевищенні сумарною завадою визначеного рівня порогу для завад, здійснюється перехід до вибору нової частоти (п. 2).

15. Робиться позитивний висновок про можливість частотного призначення.

III. Методика аналізу об'єктової електромагнітної сумісності засобів зв'язку

Запропонована методика призначена для визначення можливого взаємного впливу групи РЕЗ, що розташовані в умовах обмеженого простору [7]. Вона може використовуватись для оцінки можливих завад приймачу внаслідок блокування та інтермодуляції при відсутності завад, що попадають безпосередньо в головний канал прийому.

Відповідно до методики пропонується проводити аналіз для кожного окремого приймача з розглянутої групи РЕЗ. У рамках розглянутого завдання використовується модель приймача, структурна схема якого зображена на рис. 8.

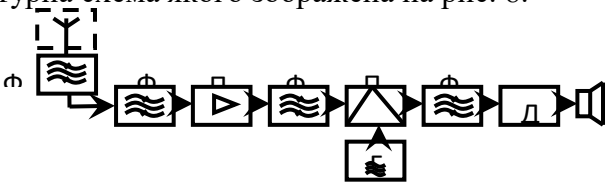


Рис. 9. Структурна схема приймача

На рис. 9 позначені: Ф1 – фільтр, що моделює частотну залежність коефіцієнта підсилення антени, Ф2 – фільтр попередньої селекції, П – підсилювач радіочастоти, Ф3 – фільтр радіочастоти, Ф4 – фільтр проміжної частоти, що реалізує основну вибірковість приймача, ПЧ – перетворювач частоти (змішувач), Г – гетеродин, Д – демодулятор.

В якості критеріїв виконання умов ЕМС пропонується використовувати нерівності:

$$P_{\text{п}} < P_{\text{пд}} \quad \text{та} \quad P_{\text{іо}} + P_{\text{із}} < P_{\text{ід}},$$

де: $P_{\text{п}}$ та $P_{\text{пд}}$ – сумарна та максимальна припустима сумарна потужність завад на вході підсилювача радіочастоти; $P_{\text{іо}}$, $P_{\text{із}}$ – сумарна потужність складових інтермодуляції на виході фільтра проміжної частоти, що надійшла на вхід змішувача на частоті відповідно основного та дзеркального каналів; $P_{\text{ід}}$ – максимальна припустима сумарна потужність продуктів інтермодуляції на виході фільтра проміжної частоти.

Етапи методики

Вирішення завдання оцінки умов виконання об'єктової ЕМС розділяється на наступні етапи:

1. Розрахунок (вимір) величин і форм спектрів завад на вході приймача.

2. Розрахунок сумарної потужності завад на вході підсилювача радіочастоти.

3. Визначення сполучень завад, які формують на виході підсилювача радіочастоти продукти інтермодуляції на частотах основного та дзеркального каналів.

4. Визначення величин і форм спектрів продуктів інтермодуляції на виході підсилювача радіочастоти.

5. Визначення сумарної потужності продуктів інтермодуляції на виході фільтра ПЧ.

6. Порівняння розрахованих значень потужностей завад із припустимими.

При одночасному виконанні наступних умов: $P_{\text{п}} < P_{\text{пд}}$ та $P^{\text{і}} < P_R - A_{\text{о}}$ робиться висновок про виконання умов ЕМС відносно розглянутого приймача по блокуванню та інтермодуляції. При невиконанні кожного з нерівностей робиться вивід про невиконання відповідних умов ЕМС.

Висновки. Запропоновані методики базуються на сучасних рекомендаціях Міжнародного союзу електрозв'язку. Особливістю розроблених методик є їх орієнтація на практичну реалізацію для отримання комплексного рішення задачі аналізу електромагнітної сумісності засобів зв'язку. Особливістю методик також є зменшення складності розрахунків шляхом поділення аналізу на два етапи – попередній та детальний. На попередньому етапі здійснюється вибір і аналіз ЕМС РЕЗ за частотно-територіальною ознакою. На етапі детального аналізу проводяться розрахунки ЕМС з урахуванням можливого впливу побічних та інтермодуляційних випромінювать, а також можливості блокування приймачів при розташуванні групи РЕЗ в обмеженому просторі. Також запропоновані методики передбачають зменшення обсягу складних розрахунків для окремих складових (часткових) задач аналізу ЕМС, які вимагають надлишок точних вихідних даних (щодо параметрів устаткування, рельєфу, параметрів розповсюдження радіохвиль тощо), при відсутності частини яких (або зниженні їх точності) складні розрахунки за запропонованими МСЄ методиками можуть привести до неприйнятних результатів.

На основі запропонованих методик проводиться розробка алгоритмів та спеціального програмного забезпечення (ПЗ) аналізу ЕМС РЕЗ для подальшого використання користувачами РЧР України.

В подальших дослідженнях пропонується удосконалити методики та відповідні алгоритми для врахування особливостей та характеристик окремих РЕЗ.

ЛІТЕРАТУРА:

1. Седельников Ю.В. Электромагнитная совместимость радиоэлектронных средств. — Казань. ЗАО "Новое знание, 2006. – 304 с.

2. Бузов А.Л. Управление радиочастотным спектром и электромагнитная совместимость радиосистем / Под редакцией Быховского М.А. – М.: Эко-Трендз. – 2006. – 376 с.

3. Теорія і практика управління використанням радіочастотного ресурсу/ За ред. В.Г.Кривуци та Т.М.Наритника. – К.:ДУІКТ, 2012.

4. Регламент радиосвязи. Международный союз электросвязи. – Женева, 2012.

5. Коваленко І.Г. Методика аналізу електромагнітної сумісності засобів радіозв'язку фіксованої радіослужби спеціального призначення // Збірник наукових праць ВІТІ НТУУ "КПІ", 2014. – № 1. – С. 21 – 29.

6. Коваленко І.Г. Методика аналізу електромагнітної сумісності засобів радіозв'язку рухомої радіослужби спеціального призначення // Збірник наукових праць ВІТІ НТУУ "КПІ", 2015. – № 1. – С. 35 – 41.

7. Коваленко І.Г. Методика аналізу об'єктової електромагнітної сумісності засобів зв'язку // Збірник наукових праць ВІТІ НТУУ "КПІ", 2013. – № 2. – С. 28 – 33.

8. Рекомендация МСЭ-R P.370-7 (1995). VHF FND UHF PROPAGATION CURVES FOR THE FREQUENCY RANGE FROM 30 MHz TO 1000 MHz.

9. Рекомендация МСЭ-R P.526-10 (2007). Распространение волн за счет дифракции.

10. Рекомендация МСЭ-R P.452-15 (2013). Процедура прогнозирования для оценки микроволновых помех между станциями, находящимися на поверхности Земли, на частотах выше приблизительно 0,7 ГГц.

11. Рекомендация МСЭ-R P.341-5 (1999). Концепция потерь передачи для радиолиний.

12. Промежуточный отчет о НИР "Радиочастотное обеспечение создания системы спутниковой связи Украины", НПВФ "Банкомсвязь", Киев, 1994.

13. Рекомендация МСЭ-R F.594-4 (1997) Допустимые коэффициенты ошибок по битам на выходе гипотетического эталонного цифрового тракта для радиорелейных систем, которые могут составлять часть цифровой сети с интеграцией служб.

14. Рекомендация МСЭ-R F.634-4 (1997) Показатели качества по ошибкам для реальных цифровых радиорелейных линий, составляющих часть цепи высокого качества в цифровой сети с интеграцией служб.

REFERENCES:

1. Sedel'nykov Ju.V. Эlektromagnytnaja sovmestymost' radyoэlektronnыh sredstv. — Kazan'. ZAO "Novoe znanye, 2006. – 304 s.

2. Buzov A.L. Upravlenye radyochastotnым spektrom y эlektromagnytnaja sovmestymost' radyosystem / Pod redakcyej Выhovskogo M.A. – M.: Эko-Trendz. – 2006. – 376 s.

3. Teorija i praktyka upravlinnja vykorystannjam radiochastotnogo resursu/ Za red. V.G.Kryvucy ta T.M.Narytnyka. – K.:DUIKT, 2012.

4. Reglament radyosvjazy. Mezhdunarodnыj sojuz эlektrosvjazy. – Zheneva, 2012.

5. Kovalenko I.G. Metodyka analizu elektromagnitnoi' sumisnosti zasobiv radiozv'jazku fiksovanoi' radiosluzhby special'nogo pryznachennja // Zbirnyk naukovyh prac' VITI NTUU "KPI", 2014. – № 1. – S. 21 – 29.

6. Kovalenko I.G. Metodyka analizu elektromagnitnoi' sumisnosti zasobiv radiozv'jazku ruhomoi' radiosluzhby special'nogo pryznachennja // Zbirnyk naukovyh prac' VITI NTUU "KPI", 2015. – № 1. – S. 35 – 41.

7. Kovalenko I.G. Metodyka analizu ob'jektovoi' elektromagnitnoi' sumisnosti zasobiv zv'jazku // Zbirnyk naukovyh prac' VITI NTUU "KPI", 2013. – № 2. – S. 28 – 33.

8. Rekomendacyja MSЭ-R P.370-7 (1995). VHF FND UHF PROPAGATION CURVES FOR THE FREQUENCY RANGE FROM 30 MHz TO 1000 MHz.

9. Rekomendacyja MSЭ-R P.526-10 (2007). Rasprostranenye voln za schet dyfrakcyy.

10. Rekomendacyja MSЭ-R P.452-15 (2013). Procedura prognozyrovanyja dlja ocenky mykrovolnovыh pomeh mezhdu stancyjamy, nahodjashhymysja na poverhnosty Zemly , na chastotah vыshe pryblyzytel'no 0,7 GGc

11. Rekomendacyja MSЭ-R R.341-5 (1999). Koncepcyja poter' peredachy dlja radyolynyj.

12. Promezhutochnыj otchet o NYR "Radyochastotnoe obespechenye sozdanyja systemы sputnykovoj svjazy Ukraynы", NPVF "Bankomsvjaz"', Kyev, 1994.

13. Rekomendacyja MSЭ-R F.594-4 (1997) Dopustymые koэffycyenty oshybok po bytam na vыhode gypotetycheskogo эtalonnogo cyfrovogo trakta dlja radyorelejnыh system, kotorые mogut sostavljat' chast' cyfrovoj sety s yntegracyej sluzhb.

14. Rekomendacyja MSЭ-R F.634-4 (1997) Pokazately kachestva po oshybkam dlja real'nыh cyfrovыh radyorelejnыh lynyj, sostavljajushhyh chast' cepy vыsokogo kachestva v cyfrovoj sety s yntegracyej sluzhb.

Рецензент: д.т.н., с.н.с., Сова О.Я., начальник кафедры "Бойового застосування автоматизованих систем управління військами" Військового інституту телекомунікацій та інформатизації

к.т.н. Коваленко И.Г., Мищенко А.А., Вавасова О.С.

АНАЛИЗ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ СРЕДСТВ РАДИОСВЯЗИ

В статье предложены методики анализа электромагнитной совместимости (ЭМС), предназначенные для определения возможного взаимного влияния группы радиоэлектронных средств (РЭС) связи. Предложенные методики базируются на современных рекомендациях Международного союза электросвязи (МСЭ). Особенностью разработанных методик является их ориентация на практическую реализацию для получения комплексного решения задачи анализа электромагнитной совместимости средств связи. Также, особенностью методик является уменьшение сложности расчетов путем деления анализа на два этапа - предварительный и детальный. На предварительном этапе осуществляется выбор и анализ ЭМС РЭС по частотно-территориальному признаку. На этапе детального анализа проводятся расчеты ЭМС с учетом возможного влияния побочных и интермодуляционных Излучатели, а

также возможности блокировки приемников при расположении группы РЭС в ограниченном пространстве. Предложенные методики предусматривают уменьшение объема сложных расчетов для отдельных составляющих задач анализа ЭМС, требуют избыток точных исходных данных, при отсутствии части которых сложные расчеты по предложенным МСЭ методиками могут привести к неприемлемым результатам.

Ключевые слова: радиоэлектронное средство, электромагнитная совместимость.

Ph.D. Kovalenko I.Г., Mishchenko A.A., Vavasova O.S.

ANALYSIS OF ELECTROMAGNETIC COMPATIBILITY TELECOMMUNICATION MEANS

The article proposed methodology for analyzing electromagnetic compatibility (EMC), which is designed to assess whether the mutual influence of radio electronic facilities (REF) connection. The proposed methods are based on the current recommendations of the International Telecommunication Union (ITU). The feature developed techniques is their focus on practical implementation for integrated analysis solution EMC communications. Also, the feature of the methods is to reduce the complexity of calculation analysis by division into two phases - preliminary and detailed. At the preliminary stage the selection and analysis of EMC for frequency-territorial basis. At the stage of detailed analysis calculations EMC considering the possible impact of adverse Radiators and intermodulation and blocking receivers at the location of the RECs in tight spaces. Proposed methods include reduction of complex calculations for individual components EMC analysis tasks that require excess accurate baseline data in the absence of complicated calculations on the proposed ITU techniques can lead to unacceptable results.

Keywords: radio electronic facilities electromagnetic compatibility.

УДК 519.24

д.т.н., проф. **Кошевой Н.Д.** (НАКУ «ХАИ»)
д.т.н., доц. **Костенко Е.М**. (ПГАА)
Кошевая И.И. (НАКУ «ХАИ»)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ СИНТЕЗА ОПТИМАЛЬНЫХ ПО СТОИМОСТНЫМ (ВРЕМЕННЫМ) ЗАТРАТАМ ПЛАНОВ МНОГОФАКТОРНОГО ЭКСПЕРИМЕНТА

Проведен сравнительный анализ модифицированных и примененных для синтеза оптимальных по стоимостным (временным) затратам планов многофакторных экспериментов таких методов дискретной оптимизации, как анализ перестановок (полный перебор), случайный поиск, метод ветвей и границ, последовательного приближения, симплекс-метод, муравьиные алгоритмы, метод имитации отжига, жадный алгоритм, ближайшего соседа, генетические алгоритмы, табу-поиск, метод вложенных разбиений, а также разработанных методов: символьных последовательностей, комбинаторно-графовый метод, методы синтеза оптимальных планов дробного и полного факторных экспериментов, основанные на применении кода Грея, метод итерационного планирования для оптимизации композиционных планов. Приведен перечень программ, реализующих эти методы синтеза, и перечень реальных объектов, на которых апробированы программы. Выданы рекомендации по применению методов синтеза оптимальных по стоимостным (временным) затратам планов многофакторных экспериментов.

Ключевые слова: анализ, метод, алгоритм, оптимальный план, стоимость, время.

Постановка задачи. Для синтеза оптимальных по стоимостным (временным) затратам модифицированы и применены следующие методы дискретной оптимизации: анализ перестановок (полный перебор), случайный поиск, метод ветвей и границ, последовательного приближения, симплекс-метод, муравьиные алгоритмы, метод имитация отжига, жадный алгоритм, ближайшего соседа, генетические алгоритмы, табу-поиск, метод вложенных разбиений (рис. 1).



Рис. 1. Методы оптимального по стоимостным (временным)

затратам планирования экспериментов

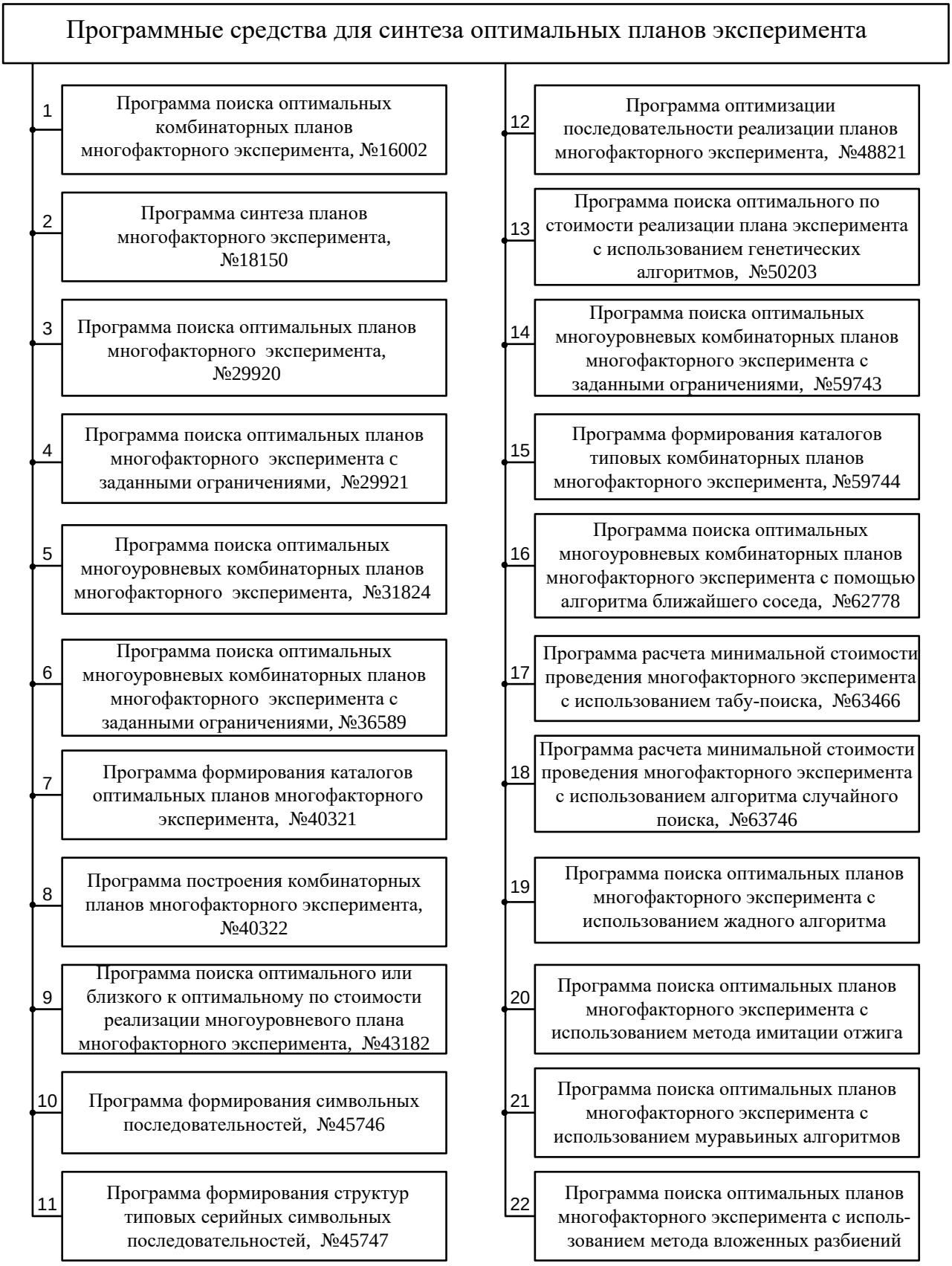


Рис. 2. Программное обеспечение для синтеза оптимальных планов эксперимента

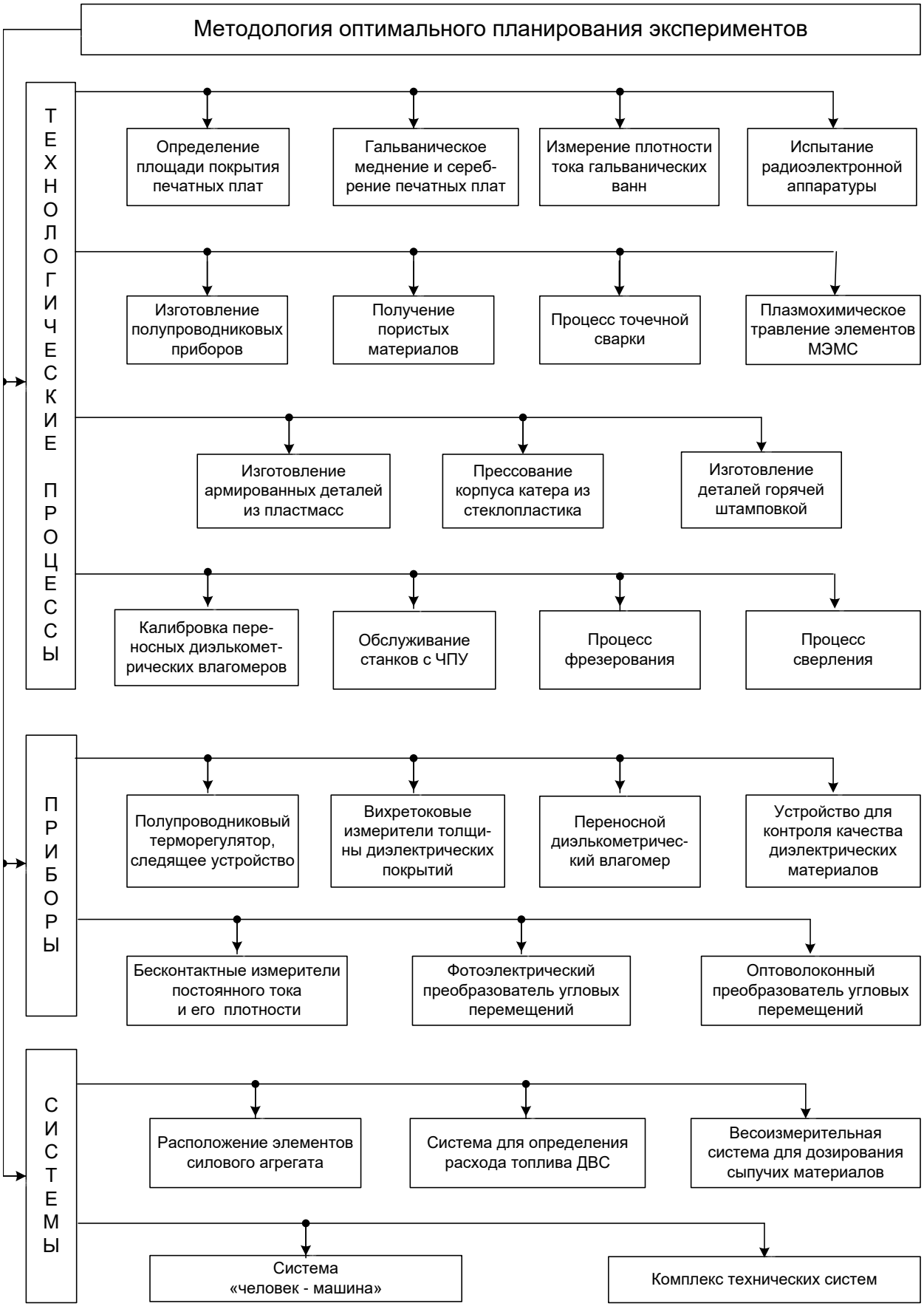


Рис. 3. Перечень объектов, на которых апробировалась методология оптимального планирования экспериментов

Задача оптимизации комбинаторных планов МФЭ имеет определенную специфику, и для ее решения были разработаны следующие методы: символьных последовательностей, комбинаторно-графовый метод, методы синтеза оптимальных планов дробного факторного эксперимента (ДФЭ) и полного факторного эксперимента (ПФЭ), основанные на применении кода Грея, метод итерационного планирования для оптимизации композиционных планов (см. рис. 1).

Перечисленным методам присущи как достоинства, так и недостатки. Для их практического применения целесообразно провести сравнительный анализ по критериям величины выигрыша по стоимости (времени) реализации плана эксперимента и быстродействия решения задачи синтеза.

Анализ последних исследований и публикаций. Известны некоторые примеры проведения сравнительного анализа методов оптимизации планов многофакторных экспериментов [1,2]. Недостатком этих исследований является ограниченный перечень сравниваемых методов оптимизации: анализ перестановок, случайный поиск, метод ветвей и границ, метод последовательных приближений.

Цель статьи. Выполнить сравнительный анализ методов оптимизации по стоимостным (временным) затратам планов многофакторных экспериментов, перечисленных в постановке задачи.

Основные материалы исследования. Для реализации и сравнения указанных методов оптимизации по стоимостным (временным) затратам планов многофакторных экспериментов было разработано программное обеспечение. Перечень созданных программ представлен на рис. 2.

Для оценки эффективности применения указанных методов проведены исследования на ряде объектов, перечень которых представлен на рис. 3.

По результатам указанных исследований можно сделать следующие рекомендации.

1. К методам, которые позволяют получить оптимальные по стоимостным (временным) затратам планы многофакторных экспериментов, можно отнести: полный перебор, метод символьных последовательностей, комбинаторно-графовый метод, методы, основанные на применении кода Грея. При этом полный перебор для любых видов эксперимента позволяет получить оптимальное решение, однако его целесообразно применять для планов с количеством факторов $k \leq 3$, так как при большем k значительно увеличивается число перестановок и временные затраты на поиск, а при современном уровне вычислительной техники эту задачу не всегда можно решить.

Метод символьных последовательностей дает точное решение при оптимизации только планов ПФЭ с количеством факторов $k \leq 3$.

Комбинаторно-графовый метод позволяет синтезировать оптимальные по стоимостным (временным) затратам планы только полного факторного эксперимента с количеством факторов $k \leq 4$.

Методы, основанные на применении кода Грея, позволяют строить оптимальные по стоимостным (временным) затратам планы дробного и полного факторных экспериментов для любого количества факторов.

2. К методам, которые позволяют получить оптимальные или близкие к оптимальным планы многофакторных экспериментов, следует отнести: анализ перестановок (ограниченный перебор), случайный поиск, методы ветвей и границ, последовательного приближения, итерационного планирования эксперимента, имитации отжига, вложенных разбиений, симплекс-метод, муравьиные алгоритмы, жадный алгоритм, ближайшего соседа, генетические алгоритмы, табу-поиск.

Характерными особенностями этих методов являются следующие: применимы для любых видов эксперимента; количество факторов, для которых возможно применение метода, ограничено только вычислительными возможностями ЭВМ; при получении лучшего из рассмотренных вариантов (близкое к минимальному по стоимости (времени)

реализации) степень «близости» оценить нельзя; невозможно создание каталогов типовых решений.

3. В результате проведенных исследований [3], в которых для оптимизации по стоимостным(временным) затратам планов многофакторных экспериментов использовались такие методы, как анализ перестановок (ограниченный перебор), случайный поиск, методы последовательного приближения и ветвей и границ, наибольшие выигрыши в стоимости (времени) реализации получали в основном при применении метода ветвей и границ.

При применении ограниченного перебора и случайного поиска зачастую лучшие результаты давал случайный поиск, позволяющий уходить от локальных оптимумов.

4. Методы, позволяющие получать оптимальные или близкие к оптимальным планы любых многофакторных экспериментов, следует применять для объектов с количеством факторов k>3. При этом по результатам исследований можно сделать следующие выводы:

– при исследовании объектов с количеством факторов k=3 результаты оптимизации планов МФЭ приближенными алгоритмами, как правило, совпадают с оптимальным решением, полученным методом полного перебора. Это, в свою очередь, подтверждает правильность разработанных алгоритмов и программ. Иногда исключение составляют методы случайного поиска, ветвей и границ, симплекс - метод, жадный и ячеистый генетический алгоритмы;

– при исследовании объектов с количеством факторов k≥4 предпочтение необходимо отдавать муравьиным и генетическим алгоритмам, иногда хорошие результаты дает алгоритм ближайшего соседа;

– при оптимизации композиционных планов МФЭ целесообразно использовать метод итерационного планирования эксперимента и комбинированный метод, основанный на применении жадного алгоритма и метода имитации отжига. Неплохие результаты получаются и при применении генетических алгоритмов и симплекс-метода;

– при оптимизации трехуровневых планов 3^k хорошие результаты получаются при использовании генетических алгоритмов, симплекс-метода и табу-поиска.

– по быстродействию решения задачи оптимизации планов МФЭ методы можно расположить следующим образом: симплекс-метод, табу-поиск, ближайшего соседа, жадный алгоритм, имитации отжига, метод вложенных разбиений, генетические алгоритмы.

Выводы. В данной статье приведен сравнительный анализ методов, которые можно применить для оптимизации по стоимостным (временным) затратам планов многофакторных экспериментов. Приведен перечень программ, которые реализуют методы поиска оптимальных планов эксперимента. По результатам оптимизации планов МФЭ для исследования ряда реальных объектов выданы рекомендации по применению проанализированных методов для решения данных задач.

ЛИТЕРАТУРА:

1. Кошевой Н.Д. Сравнительный анализ методов оптимизации многофакторных планов эксперимента / Н.Д. Кошевой, О.Л. Бурлеев, Е.М. Костенко // Автоматизированные системы управления и приборы автоматики. – Вып.150. – Харьков: ХНУРЭ. – 2010. – С.60-64.

2. Кошевой Н.Д. Сравнительный анализ алгоритмов оптимизации композиционных планов второго порядка / Н.Д. Кошевой, Е.М. Костенко, А.С. Чуйко // Зб. наук. пр. військ. ін-ту Київського нац. ун-ту ім. Тараса Шевченка. – Вип. 30. – К.: ВІКНУ, 2010. – С.40-45.

3. Кошевой Н.Д. Оптимальное по стоимостным и временным затратам планирование эксперимента / Н.Д. Кошевой, Е.М. Костенко. – Полтава: издатель Шевченко Р.В., 2013. – 317 с.

REFERENCES:

1. Koshevoy N.D. Sravnitelnyiy analiz metodov optimizatsii mnogofaktornyih planov eksperimenta / N.D. Koshevoy, O.L. Burleev, E.M. Kostenko // Avtomatizirovannyie sistemyi upravleniya i priboryi

avtomatiki. – Vip.150. – Harkov: HNURE. – 2010. – S.60-64.

2. Koshevoy N.D. Sravnitelnyiy analiz algoritmov optimizatsii kompozitsionnyih planov vtorogo poryadka / N.D. Koshevoy, E.M. Kostenko, A.S. Chuyko // Zb. nauk. pr. viysk. In-tu Kiyivskogo nats. un-tu im. Tarasa Shevchenka. – Vip. 30. – K.: VIKNU, 2010. – S.40-45.

3. Koshevoy N.D. Optimalnoe po stoimostnyim i vremennyim zatratam planirovaniya eksperimenta / N.D. Koshevoy, E.M. Kostenko. – Poltava:izdatel Shevchenko R.V., 2013. – 317 s.

Рецензент: д.т.н., проф. **Угрюмов М.Л.,** профессор кафедры информатики Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ»

д.т.н., проф. Кошовий М.Д., д.т.н., доц. Костенко О.М., Кошова І.І.

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ СИНТЕЗУ ОПТИМАЛЬНИХ ЗА ВАРТІСНИМИ (ЧАСОВИМИ) ВИТРАТАМИ ПЛАНІВ БАГАТОФАКТОРНОГО ЕКСПЕРИМЕНТУ

Проведено порівняльний аналіз модифікованих і застосованих для синтезу оптимальних за вартісними (часовими) витратами планів багатофакторних експериментів таких методів дискретної оптимізації, як аналіз перестановок (повний перебір) випадковий пошук, метод гілок і меж, послідовного наближення, симплекс-метод, мурашині алгоритми, метод імітації відпалу, жадібний алгоритм, найближчого сусіда, генетичні алгоритми, табу-пошук, метод вкладених розбиттів, а також розроблених методів: символьних послідовностей, комбінаційно-графовий метод, методи синтезу оптимальних планів дробних і повних факторних експериментів, основаних на застосуванні коду Грея, метод ітераційного планування для оптимізації композиційних планів. Наведено перелік програм, які реалізують ці методи синтезу, і перелік реальних об'єктів, на яких опробувалися програми. Видані рекомендації по застосуванню методів синтезу оптимальних за вартісними (часовими) витратами планів багатофакторних експериментів.

Ключові слова: аналіз, метод, алгоритм, оптимальний план, вартість, час.

prof. Koshevoy N.D., prof. Kostenko E.M., Koshevaya I.I.

THE COMPARATIVE ANALYSIS OF THE METHODS OF SYNTHESIS OF MULTIFACTORIAL EXPERIMENT'S OPTIMAL PLANS IN COST (TIME)

For synthesis of multifactorial experiment's optimal plans in cost (time) the comparative analysis of the modified and applied methods of discrete optimization such as a random search, branch and bound method, successive approximation, the simplex method, ant algorithms, the method simulated annealing, greedy algorithm, nearest neighbor, genetic algorithms, taboo search, nested partitions were carried out. Also the developed methods: character sequences, combinatorial and graph method, methods of synthesis of optimal plans of fractional and full factorial experiments based on the use of Gray code, method iterative planning to optimize composite plans were compared.

The list of programs that implement these methods of synthesis, and the list of real objects, on which the programs were tested, were given.

The guidelines of using the methods of synthesis of multifactorial experiment's optimal plans in cost (time) were published.

Keywords: analysis, method, algorithm, optimal plan, cost, time.

УДК 355.457

д.т.н., доц. **Лисий М.І.** (НАДПСУ)
к.т.н., доц. **Балицький І.І.** (НАДПСУ)
к.т.н **Бабій Ю.О.** (НАДПСУ)
Поліщук В.В. (НАДПСУ)

УЗАГАЛЬНЕННЯ КЛАСИФІКАЦІЇ ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ ОХОРОНИ ТА ЗАХИСТУ КОРДОНУ

На сьогоднішній день одним із перспективних напрямків розвитку системи інженерно-технічного контролю, з метою постійного висвітлення обстановки на державному кордоні та вчасного реагування на її зміни, є удосконалення технічних засобів охорони кордону, як єдиного достовірного джерела інформації про правопорушення на державному кордоні.

Попри численні дослідження науковців та серйозну увагу, що приділяється посадовими особами Державної прикордонної служби України, актуальним завданням залишається пошук перспективних шляхів функціонування системи інженерно-технічного контролю. Тому, метою даної статті є загальний аналіз і класифікація технічних засобів для охорони і захисту кордону.

У статті проведено аналіз нормативно-правових документів, наукових праць, що визначило невідповідності класифікації технічних засобів охорони та захисту державного кордону, на основі чого уперше розроблено узагальнену їх класифікацію. На відміну від діючої класифікації виділено клас засобів захисту кордону, сигналізаційних засобів охорони позицій, мобільних радіокерованих засобів, розширено клас технічних засобів спостереження сейсмолокаційними, акустичними, георадарними засобами, при узагальнені всіх засобів у клас технічних засобів охорони і захисту державного кордону.

Ключові слова:класифікація, технічні засоби охорони та захисту кордону.

Постановка проблеми. Наслідком тривалого недостатнього фінансування інженерно-технічного забезпечення щодо закупівлі технічних засобів охорони (ТЗО) кордону стала відсутність потреби у дослідженні питань їх розвитку і, зокрема, класифікації таких засобів. Кардинально стан справ змінився після прийняття Кабінетом Міністрів України в 2015 р. документів, які конкретизують інженерно-технічне облаштування рубежу основних інженерних споруд державного кордону технічними засобами [1]. Разом з тим, стрімкий розвиток ТЗО у світі, поява нових загроз і небезпек у прикордонній сфері проявили низку невідповідностей зіставлення сучасного стану техніки загрозам і небезпекам, які виявляються і яким можна протидіяти в прикордонній сфері із застосуванням таких технічних засобів. Це потребує переосмислення, удосконалення, узагальнення класифікації технічних засобів, які можуть застосовуватись для охорони та захисту кордону.

Як приклад невдалої класифікації можна навести списання книжок з фонду бібліотеки, які на вигляд наче тільки з видавництва, з новою палітуркою і стиснутими сторінками після порізки і брошурування. Некоректний пошук, внаслідок неадекватної класифікації, залишив книги ні разу не прочитаними. Саме коректна класифікація як технічних засобів, так і загроз національній безпеці дозволить здійснити адекватний вибір нових технічних рішень і засобів для виявлення і протидії загрозам і небезпекам у прикордонній сфері, рис. 1.

Аналіз останніх досліджень. Нормативно-правовими документами визначені завдання із забезпечення ефективної реалізації політики безпеки у сфері захисту кордону та охорони державного кордону України (ДКУ); визначені цілі розвитку ДПСУ, в тому числі, забезпечення складових системи охорони ДКУ, те, що стосується технічних засобів охорони (ТЗО). У документах [5-10] визначені роль та значення системи інженерно-технічного контролю (СІТК) в сучасній моделі охорони ДКУ.

Попри численні дослідження науковців та серйозну увагу, що приділяється посадовими особами ДПСУ, актуальним завданням залишається пошук перспективних шляхів функціонування СІТК.



Рис. 1. Загальна модель класифікації технічних засобів для виявлення і протидії загрозам і небезпекам у прикордонній сфері

Формулювання мети статті. Нормативно-правовими документами визначені завдання із забезпечення ефективної реалізації політики безпеки у сфері оборони, захисту та охорони державного кордону (ДК) [2; 3], визначені цілі розвитку Державної прикордонної служби України (ДПСУ) на найближчу перспективу, в тому числі, щодо забезпечення ТЗО як складових СІТК [4].

Аналіз та класифікацію загроз, небезпек у прикордонній сфері є окремим науковим завданням, що буде розглянуто у послідуючому. Загальний аналіз і класифікація технічних засобів для охорони і захисту кордону становить **мету роботи.**

Виклад основного матеріалу. Більше двох десятків найменувань ТЗО кордону застосовувались в минулому у прикордонних військах для виявлення правопорушників (ПП). На сьогодні такий перелік дещо зменшився і в основному стосується тепловізорів та оптико-електронних приладів. Звісно, що широка номенклатура засобів не є критерієм забезпечення ефективного посилення охорони кордону. Проте, порівнюючи світовий ринок технічних засобів, які можна розглядати як потенційні технічні засоби охорони та захисту державного кордону (ТЗОЗДК) із прийнятою їх класифікацією у ДПСУ, встановлено невідповідність між:

потребою у логічному, ієрархічному структурованому поданні переліку типів технічних засобів для охорони і захисту та практично відсутній їх загальної класифікаційної моделі;

наявними типами технічних засобів охорони та захисту і відсутністю окремих типів у діючій системі класифікації ТЗО кордону;

віднесенням технічних засобів захисту до класу ТЗО кордону і потребою виокремлення їх в окремий клас технічних засобів;

потребою в однозначності назв окремих типів технічних засобів, стандартизації їх в різних галузях і неоднозначності у понятійному апараті щодо ТЗО кордону.

Дамо коротку характеристику встановлених невідповідностей. Щодо першого пункту, то на сьогодні загальної класифікаційної моделі, структури ТЗО кордону немає. ТЗО кордону поділяють на радіолокаційно-прожекторні, сигналізаційні, оптичні, оптико-електронні. У зазначених класах ТЗО ще здійснюється розподіл за ступенем мобільності, протяжності охорони, що звісно є по суті лише вершиною ієрархічної класифікаційної моделі множини ТЗО.

Щодо другої невідповідності, то, наприклад, взагалі відсутній клас засобів підповерхневої локації типу георадарів. Проте, такі засоби досить успішно застосовуються в ДПСУ з 2014 року. Очевидно, за наявної адекватної класифікації ТЗО, дані засоби, які більше десятиліття застосовують у інших галузях [5; 6] могли бути набагато раніше застосовуванні і у ДПСУ. Це безумовно не дозволило б перерости окремим випадкам

прокладання тунелів, трубопроводів через державний кордон у відносно нову загрозу національній безпеці, породжену саме у прикордонній, але реалізуємій у воєнній, соціальній, економічній сферах. Також, наприклад, застосування тактичних безпілотних літальних апаратів (БПЛА) в охороні кордону логічно розглядати з позиції експлуатації ТЗО, а не як вид авіаційних засобів. Адже їх відрізняє лише носій ТЗО, а експлуатація і її організація фактично є складовою інженерно-технічного забезпечення. Особливо така невідповідність може загостритися при застосуванні БПЛА за викликом, за даними первинного виявлення ПП засобами охорони. Тому, доречним невеликі, тактичні БПЛА розглядати як клас ТЗО.

Щодо третьої невідповідності, то, наприклад, застосування у прикордонних військах раніше електрошокових засобів ИЕ-200, ГИ-1 здійснювалось комплексно із ТЗО, до яких їх відносили, проте, призначення електрошокових засобів – це захист кордону. На сьогодні такі засоби швидко розвиваються, здебільшого їх називають засобами нелетального впливу, а їх клас все більше розширюється [7-8].

Причини недосконалості класифікації ТЗО і захисту кордону слід шукати не тільки у бурхливому розвитку радіоелектроніки у галузі охорони, а й у невизначеності понятійного апарату щодо оперативно-службової діяльності ДПСУ стосовно таких функцій як охорона, захист кордону. Така невизначеність загострилась з початком агресії на Півдні і Сході країни. Чи повинна ДПСУ захищати кордон, які технічні засоби захисту застосовуються, в чому відмінність захисту від охорони? Відповідь слід шукати після аналізу визначень понять «охорона, захист кордону», поданих у сучасній публікації [10]:

Охорона державного кордону України – система прикордонних, технічних та інших заходів щодо забезпечення недоторканності державного кордону України й захисту національних інтересів держави у прикордонному просторі у мирний час;

Захист державного кордону України – комплекс заходів, який проводить командування з метою припинення збройних та інших провокацій на державному кордоні у мирний час.

Зазначені визначення не набагато зменшують ентропію поняття, це ж стосується і енциклопедичних визначень. Порівнюючи дані визначення, відзначимо, що охорона переходить у захист, коли локально ПП починає застосовувати силу та зброю. Стосовно технічного аспекту, то ТЗО, по суті, виявляють ПП, а технічні засоби захисту впливають фізично на ПП, ускладнюють пересування на рівні з інженерними загородженнями. Прогнозовано, що саме технічні засоби для захисту кордону набудуть у перспективі пріоритет у застосуванні, яке не потребує виявлення ПП і послідуючого затримання, якщо ПП рухається до нас і змінив свої наміри через вплив засобів захисту кордону. Тобто, процес охорони кордону із обов'язковим виявленням, спостереженням, затриманням ПП може трансформуватися у процес захисту кордону із нелетальним впливом і спостереженням за зоною впливу, затримання ПП. При цьому, суттєвим є те, що будуть відсутні дорогі, складні, високочутливі технічні засоби для виявлення ПП, рис. 2.



Рис. 2. Процес функціонування системи технічного контролю і сил охорони при застосуванні технічних засобів

Щодо останньої невідповідності, то, наприклад, згідно різних державних стандартів сигналізаційні комплекси відносять до засобів охорони периметрів, до територіально-розподілених радіотехнічних систем охорони, до ТЗО протяжних ділянок кордону [11;12].

Так, у ДСТУ [11] дано таке визначення «системи охорони»: охоронна теле (відео) система – це система, що складається з електромеханічного та оптико-електронного обладнання.

В ДСТУ [12]: система охоронної сигналізації – це електричне обладнання, що є складовою частиною системи тривожної сигналізації, призначене для виявляння та попереджування про наявність нападу та/або проникнення в підохоронні зони чи об'єкти.

Розглянуті визначення щодо охорони кордону стосуються СІТК, рис. 3.



Рис. 3. Структура і склад системи інженерно-технічного контролю

Особливістю структури СІТК є потенційна різноманітність технічних засобів підсистеми технічного контролю, яка є організаційною системою і включає ТЗО і технічні засоби захисту. Близьким до поняття контроль є моніторинг. Але термін «monitor» (анг.) перекладається як контролюючий і за сутністю поєднує в собі отримання інформації та її обробку. Таке тлумачення даного поняття співпадає із визначенням його у теорії озброєння. Тому, логічно запропонувати назву для всього спектру технічних засобів, що можуть застосовуватись для посилення охорони і захисту кордону як технічні засоби охорони та захисту державного кордону (ТЗОЗ ДК) [13].

Загалом розрізняють декілька ознак загальної класифікації об’єктів: за домінуючою ознакою, функцією, властивістю; поєднання назв, комплексування назв; введення нової назви, класу; назви класу відповідно спорідненого ДСТУ; назви класу відповідно традиціям у певній галузі.

Виділити якусь одну домінуючу функцію є не логічним. Їх є дві – охорона і захист. Введення нових назв тільки додає проблем у дослідженні. ДСТУ в галузі охорони кордону не

має. Традиційно під контролем розуміють застосування технічних засобів, тобто і охорону, і захист кордону. Враховуючи зазначене вище, клас ТЗОЗ ДК слід трансформувати у таку ієрархію, рис. 4.

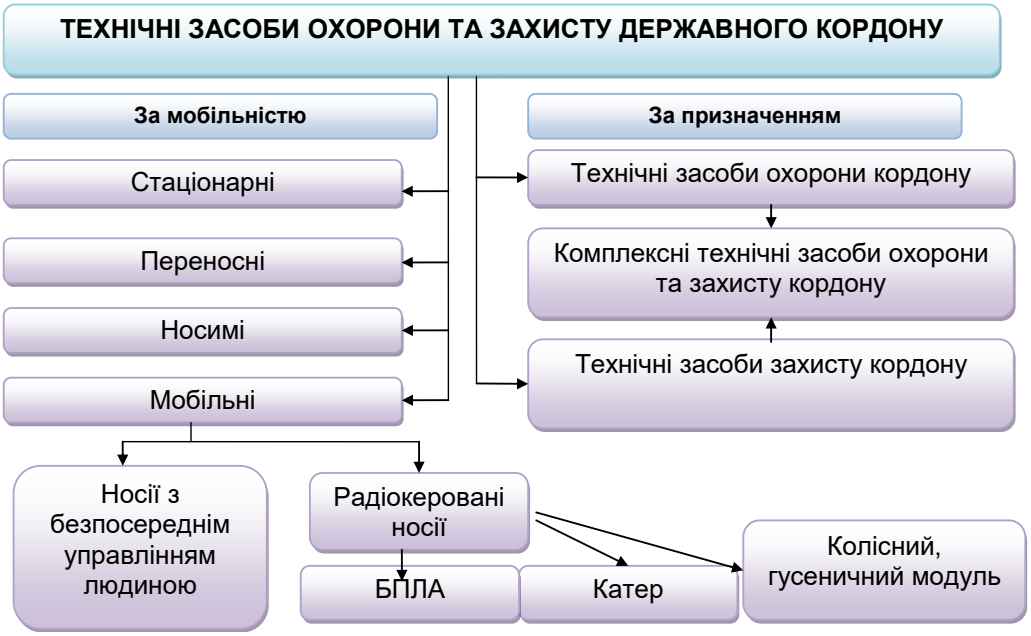


Рис. 4. Класифікація технічних засобів охорони і захисту державного кордон

Дані рис. 4 уточнюють дані рис. 3 щодо виділення узагальненого класу технічних засобів – ТЗОЗ ДК, до якого віднесено всі технічні засоби, що посилюють охорону і захист державного кордону. Також, виділено у окремий підклас комплексні технічні засоби охорони і захисту кордону, що забезпечують одночасно і виявлення, і ускладнення пересування ПП.

Прикладом може бути застосування засобів охорони з електрошоковим загородженням (HAGROY). Очевидно, назву такого виду технічних засобів для охорони і захисту протяжних ділянок кордону доцільно подати, поєднуючи назви основних функцій, а саме: комплекс сигналізації і захисту, а віднести його до класу ТЗОЗДК. Якщо подібний комплекс складатиметься із засобів спостереження і електрошокових засобів, то доцільно віднести до того ж класу, а назвати – комплекс спостереження і захисту. Очевидно, необхідно більш детальніше розглянути класифікацію ТЗО. Основною ознакою розподілу ТЗО кордону є їх функціональне призначення, рис. 5.

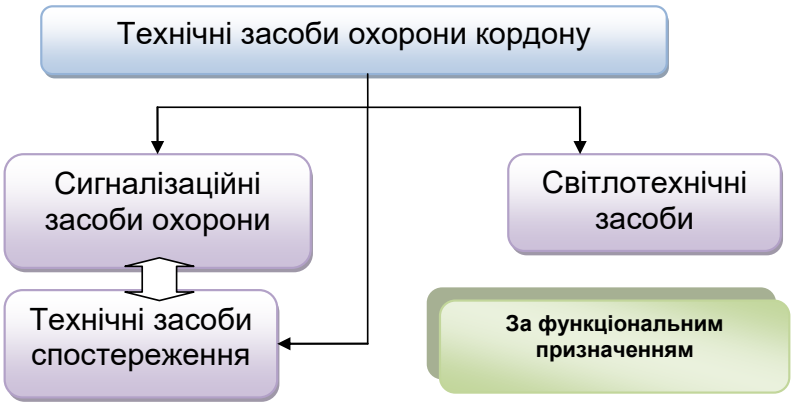


Рис. 5. Класифікація технічних засобів охорони кордону

У результаті аналізу визначень поняття «сигналізаційні засоби» [11; 12] можна відзначити, що дані засоби характеризуються виробленням сигналу тривоги. Отже, сигналізаційні засоби охорони (СЗО) – це ТЗО кордону, що видають сигнал тривоги при появі рухомого об’єкта в зоні охорони або зміни об’єкта охорони. За об’єктом охорони сигналізаційні засоби охорони поділяють, рис. 6, на: сигналізаційні засоби охорони локальних ділянок кордону; сигналізаційні засоби охорони протяжних ділянок кордону; об'єктова сигналізація.

Проте, така класифікація є не завершеною. Досвід бойових дій висвітлив потребу у розвитку такого типу засобів охорони, які б забезпечували охорону позицій, блок-постів. По суті, це є сигналізаційні засоби охорони локальних ділянок кордону, але останні, через недосконаліть класифікації, а, відповідно, і відсутності вимог до окремих характеристик, не забезпечують необхідних функцій охорони зазначених об’єктів.

Локальна ділянка кордону не має чіткого визначення, але можна вважати її протяжність до 1-3 км, беручи до уваги протяжність лінійної частини таких діючих ТЗО. Периметр польового парку, місць тимчасової стоянки, табору теж має такі розміри і може взятися під охорону сигналізаційними засобами охорони локальних ділянок кордону.

Але позиція, пост спостереження або радіозв’язку у вигляді тимчасової споруди, окремого автомобіля або замаскованої ділянки місцевості у декілька квадратних метрів для спостереження, застосування групової зброї буде мати відносно невеликий периметр, менше 1 км. Також, стосовно охорони кордону важливо знати напрям руху і дальність до місця порушення. Що ж стосується позиції, то важливим є напрямок на порушника або ж просто сам факт завчасної появи на позиції рухомого об’єкта. Тому, до таких засобів повині бути дещо інші тактико-технічні вимоги, а засоби доцільно виділити в окремий вид, загальну ж класифікацію сигналізаційних засобів подати як на рис. 6.

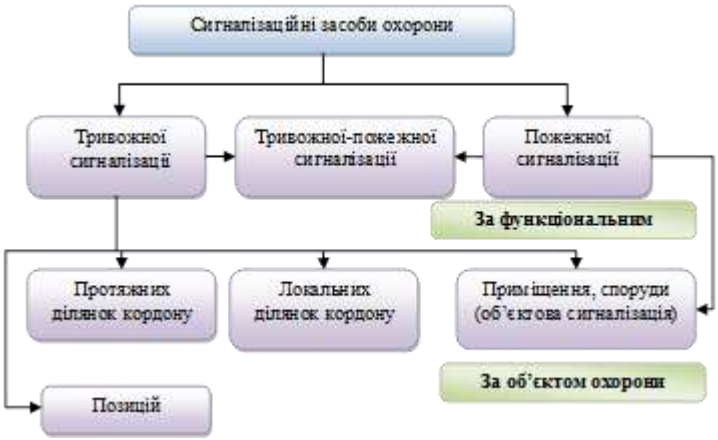


Рис. 6. Класифікація сигналізаційних засобів охорони

Технічні засоби спостереження (ТЗС) – це засоби, які дозволяють відслідковувати переміщення рухомих об’єктів (РО) в зоні спостереження. Таке узагальнене визначення дано на основі аналізу публікацій [13]. Такі засоби, наприклад, як тепловізори, відеокамери при наявності відповідного програмного забезпечення можуть автоматично видавати сигнал тривоги при появі РО, що вказує на наявність спільної ознаки з СЗО. Тому, ТЗС досить широко застосовують як датчики в СЗО, а от зворотне застосування здебільшого носить характер охорони самих ТЗС, саме так слід розуміти вказаний зв'язок між СЗО і ТЗС на рис. 5. Класифікацію ТЗС подано на рис. 7.

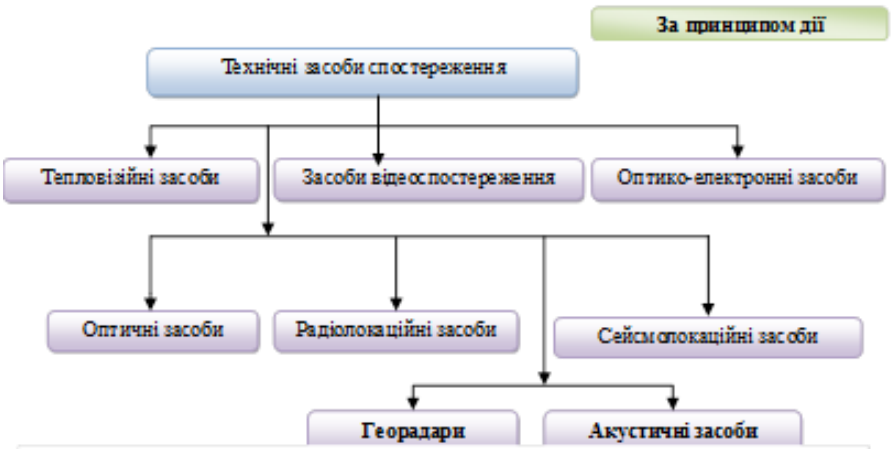


Рис. 7. Класифікація технічних засобів сигналізації за принципом дії

Виходячи з даного визначення ТЗС, відслідковування переміщення РО можна за допомогою органів зору, слуху. Здебільшого відслідковування РО забезпечує і визначення місцеположення (ВМП) РО. Слід відмітити, що СЗО теж можуть ВМП, але відслідковувати (спостерігати) за переміщенням РО СЗО забезпечують у разі наявності в їх структурі ТЗС.

Відносно новими ТЗС є сейсмолокаційні засоби, акустичні, георадари. Із зазначених засобів сейсмолокаційні є більш універсальними, що забезпечують виявлення і ВМП РО в повітрі, на землі і під поверхнею землі, що робить цей клас ТЗС досить перспективним у виявленні не тільки людей, автотранспорту, а й ВМП зброї, що здійснює постріли, визначення руху об'єктів у ґрунті. Хоча на сьогодні, наприклад, для виявлення підповерхневих комунікацій застосовують ефективно тільки георадари. Однією із нових небезпек є проліт БПЛА, як датчик виявлення таких порушників очевидно доцільно застосовувати радіолокаційні і акустичні ТЗС в складі СЗО протяжних ділянок кордону, а саме, у складі комплексів сигналізаційних.

Світлотехнічні засоби, рис. 5, класифікують за призначенням і мобільністю, рис. 8.

Такі засоби як прожекторні станції очевидно остаточно будуть у перспективі витісненні із застосування тепловізорами.

Технічні засоби захисту кордону, призначені для ускладнення пересування, впливу фізичного на ПП, їх можна класифікувати так, рис. 9.

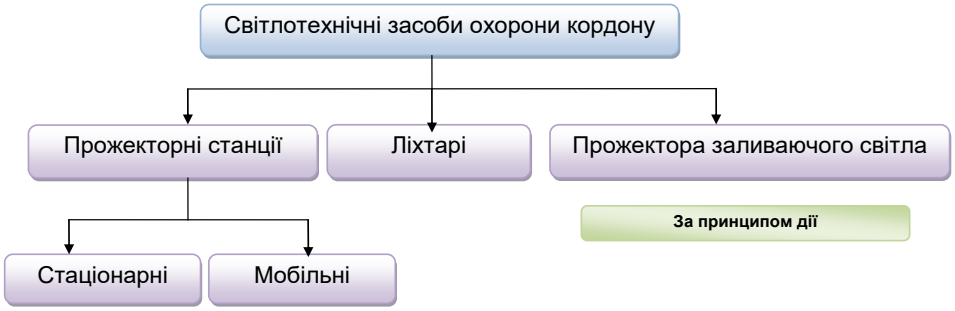


Рис. 8. Класифікація сигналізаційні технічні засоби охорони кордону

Для охорони ділянок кордону досить перспективним є застосування електричних мін, що забезпечують нелетальний вплив через крокову напругу. Також, можливим перспективним напрямком є застосування електрошокових засобів з неконтактною однополярною електризацією тіла людини, що діє навіть при застосуванні діелектричного взуття чи одягу ПП.

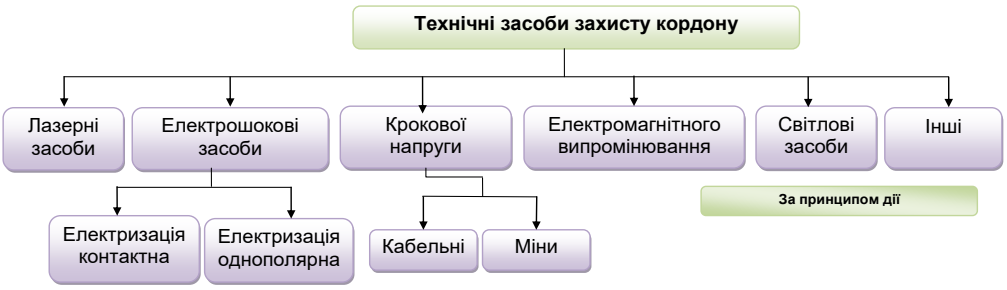


Рис. 9. Класифікація технічних засобів захисту кордону

Висновки. Уперше розроблено узагальнену класифікацію технічних засобів охорони та захисту кордону. Сутність наукової новизни полягає у введенні і виокремленні нових типів засобів охорони та захисту кордону при їх класифікації. На відміну від діючої класифікації, виділено клас засобів захисту кордону, сигналізаційних засобів охорони позицій, мобільних радіокерованих засобів, розширено клас технічних засобів спостереження сейсмолокаційними, акустичними, георадарними засобами, при узагальнені всіх засобів у клас технічних засобів охорони і захисту державного кордону. Це дозволить обґрунтувати більш коректніше загальні вимоги до виділених нових класів технічних засобів.

Подальшим напрямком дослідження є розробка концепції формування структури СІТК сухопутного кордону України.

ЛІТЕРАТУРА:

1. Бінькowський О.А. Сутність наукового супроводу технічного оснащення підрозділів охорони державного кордону / О. А. Бінькowський, О. В. Боровик, М.І. Лисий // Науковий вісник: щоквартальний науково-практичний альманах ДПСУ, 2016. – №2. – С. 3-6.

2. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про стратегію національної безпеки України»: Указ Президента України 6 травня 2015 р. №287/2015.

3. Концепція розвитку сектору безпеки і оборони України. Проект. [Електронний ресурс]. – Режим доступу: http://www.mil.gov.ua/content/public_ discussion/proj_conc.pdf. – Заголовок з екрану.

4. Про схвалення Концепції Державної цільової правоохоронної програми «Облаштування та реконструкція державного кордону» на період до 2020 року: розпорядження Кабінету Міністрів України від 11 листопада 2015 р. №1179-р.

5. Методические рекомендации по применению георадаров при обследовании дорожных конструкций / Введены в действие письмом Росавтодора № ОС-28/477 от 28.01.2004. – М.: Росавтодор, 2004.

6. Помозов В.В. Новые типы георадаров: разработка и применение / В.В. Помозов, О.А. Поцепня, Н.П. Семейкин. – М.:Разведка и охрана недр, 2002. – N 2. – С.19-21.

7. Удимцев Д.Н. Электризуемые заграждения неконтактного принципа действия / Д.Н. Удимце. – М.: Специальная техника, 2002 – № 3 – С. 12-14.

8. Охранно-защитная инженерно-техническая система нелетального электрошокового воздействия. [Електронний ресурс]. – Режим доступу: http://alfamet.pro/tehnicheskie-sredstva-ohrany/sistema-neletalnogo-elektroshokovogo-vozdejstviya-snev. – Заголовок з екрану

9. Обзор технических средств активного противодействия вторжениям на объекты различной категории. [Електронний ресурс]. – Режим доступу: http://mx1.algoritm.org/arch/84/84_8.pdf. Заголовок з екрану

10.Золотов В.П. Охорона, захист, прикриття державного кордону України / В.П. Золотов // Науковий вісник: щоквартальний науково-практичний альманах ДПСУ, 2016. – №3. – С. 45-49.

11. ДСТУ 4000-2000. Системи тривожної сигналізації. Охоронні теле(відео)системи і системи контролювання доступу.

12. ДСТУ 3960-2000. Системи тривожної сигналізації. Системи охоронної і охоронно-пожежної сигналізації. Терміни та визначення.

13. Теорія озброєння. Науково-технічні проблеми та завдання: монографія: Технічні засоби. Військові системи дистанційного моніторингу навколишнього простору щодо рухомих об'єктів: методологічні аспекти обґрунтування вимог / П.М. Сніцаренко, С.В. Лапицький, А.А. Гультяєв, О.О. Головін, А.Ю. Гупало. – К: Видавничий дім Дмитра Бураго, 2016. – 480 с.

REFERENCES:

1. Binkovskyi O.A. (2016) Sutnist naukovoho suprovodu tekhnichnoho osnashchennia pidrozdiliv okhorony derzhavnoho kordonu [The essence of the scientific support units of technical equipment of the state border]. Naukovyi visnyk: shchokvartalnyi naukovo-praktychnyi almanakh DPSU, no. 2, pp. 3-6.

2. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku «Pro stratehiiu natsionalnoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy 6 travnia 2015 r. no. 287/2015.

3. Kontseptsiia rozvytku sektoru bezpeky i oborony Ukrainy. Proekt. [Elektronnyi resurs]. – Rezhym dostupu: http://www.mil.gov.ua/content/public_ discussion/proj_conc.pdf. – Zaholovok z ekranu.

4. Pro skhvalennia Kontseptsii Derzhavnoi tsilovoi pravookhoronnoi prohramy "Oblashtuvannia ta rekonstruktsiia derzhavnoho kordonu" na period do 2020 roku: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 11 lystopada 2015 r. no. 1179-r.

5. Rosavtodor (2004) Metodicheskie rekomendatsii po primeneniyu georadarov pri obsledovanii dorozhnykh konstruktsiy [Guidelines on the application of GPR in the inspection of road constructions], Moscow: Rosavtodor no. OS-28/477.

6. Pomozov V.V. (2002) Novye tipy georadarov: razrabotka i primenenie [New types of radars: design and application]. Moscow: Razvedka y okhrana nedr, no. 2, pp. 19-21.

7. Udimtsev D.N. (2002) Elektrizuemye zagrazhdeniya nekontaktnogo printsipa deystviya [Electrified fences non-contact operating principle]. Moscow: Spetsialnaya tekhnika, no. 3, pp. 12-14.

8. Okhranno-zashchitnaya inzhenerno-tekhnicheskaya sistema neletalnogo elektroshokovogo vozdeystviya. [Yelektronniy resurs]. – Rezhim dostupu: http://alfamet.pro/tehnicheskie-sredstva-ohrany/sistema-neletalnogo-elektroshokovogo-vozdejstviya-snev. – Zagolovok z ekranu

9. Obzor tekhnicheskikh sredstv aktivnogo protivodeystviya vtorzheniyam na obekty razlichnoy kategorii. [Yelektronniy resurs]. – Rezhim dostupu: http://mx1.algoritm.org/arch/84/84_8.pdf. Zagolovok z ekranu

10. Zolotov V.P. (2016) Okhorona, zakhyst, prykryttia derzhavnoho kordonu Ukrainy [Security, protection, cover the state border of Ukraine]. Naukovyi visnyk: shchokvartalnyi naukovo-praktychnyi almanakh DPSU, no. 3, pp. 45-49.

11. DSTU 4000-2000. Systemy tryvozhnoi syhnalizatsii. Okhoronni tele(video)systemy i systemy kontroliuvannia dostupu.

12. DSTU 3960-2000. Systemy tryvozhnoi syhnalizatsii. Systemy okhoronnoi i okhoronno-pozhezhnoi syhnalizatsii. Terminy ta vyznachennia.

13. Snitsarenko P.M., Lapytskyi S.V., Hultiaiev A.A., Holovin O.O., Hupalo A. Yu. (2016) Naukovo-tekhnichni problemy ta zavdannia: monohrafiia: Tekhnichni zasoby. Viiskovi systemy dystantsiinoho monitorynhu navkolyshnoho prostoru shchodo rukhomykh obiektiv: metodolohichni aspekty obgruntuvannia vymoh [Scientific and technical problems and tasks: monograph: Facilities. Military remote monitoring of space on moving objects: methodological aspects study claims]. Kyiv: Vydavnychyi dim Dmytra Buraho. (in Ukrainian).

Рецензент: д.т.н., проф. Шинкарук О.М., ректор Національної академії Державної прикордонної служби України імені Богдана Хмельницького

д.т.н., доц. Лысый Н.И., к.т.н., доц. Балицкий И.И., к.т.н Бабий Ю.А., Полищук В.В.

ОБОБЩЕНИЕ КЛАССИФИКАЦИИ ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ОХРАНЫ И ЗАЩИТЫ ГРАНИЦ

На сегодняшний день одним из перспективных направлений развития системы инженерно-технического контроля, с целью постоянного освещения обстановки на государственной границе и своевременного реагирования на ее изменения, является

совершенствование технических средств охраны границы, как единого достоверного источника информации о правонарушениях на государственной границе.

Несмотря на многочисленные исследования ученых и серьезное внимание, уделяемое должностными лицами Государственной пограничной службы Украины, актуальной задачей остается поиск перспективных путей функционирования системы инженерно-технического контроля. Поэтому, целью данной статьи является общий анализ и классификация технических средств для охраны и защиты границы.

В статье проведен анализ нормативно-правовых документов, научных трудов, что определило несоответствия классификации технических средств охраны и защиты государственной границы, на основе чего впервые разработано обобщенную их классификацию. В отличие от действующей классификации, выделено класс средств защиты границы, сигнализационных средств охраны позиций мобильных радиоуправляемых средств, расширен класс технических средств наблюдения сейсмолокационными, акустическими, георадарными средствами, при обобщении всех средств в класс технических средств охраны и защиты государственной границы.

Ключевые слова: классификация, технические средства охраны и защиты границы.

Ph.D., Assoc. Lisiy N.I., Ph.D. Balitchi I.I., Ph.D. Babi Yu.A., Polishchuk V.V.

SUMMARY OF THE CLASSIFICATION OF TECHNICAL MEANS FOR THE SAFETY AND PROTECTION OF BORDERS

Today one of the most promising directions of development of the system engineering and technical control, with the aim of constant lighting situation at the state border and a timely response to its changes, is the improvement of technical means of border protection, as a single reliable source of information about offences on the state border.

Despite numerous studies of scientists and serious attention by the officials of the State border service of Ukraine, an important task is the search for promising ways of functioning of system engineering and technical control. Therefore, the aim of this article is a general analysis and classification of technical means for protection of the border.

In the article the analysis of normative-legal documents, scientific works, which determined the discrepancy of the classification of technical means of protection of the state border on the basis of which first developed generalized their classification. Unlike the current classification, a class of protection of the border, signaling protection of the positions of mobile radio-controlled funds, expanded the class of surveillance technology seismolocation, acoustic, georadars, in summarizing all funds in the class of technical means of protection of the state border.

Keywords: classification, means of protection and border.

УДК 621.396.967 **к.т.н. Лоза В.Н.** (ВИКНУ)

ПОСТРОЕНИЕ АЛГОРИТМА МНОГОУРОВНЕВОЙ ДИСКРЕТНОЙ ВЕЙВЛЕТ – ФИЛЬТРАЦИИ РАДИОЛОКАЦИОННОГО СИГНАЛА И СИНТЕЗ ОПТИМАЛЬНОГО АЛГОРИТМА ПОСТРОЕНИЯ БАЗЫ ФИЛЬТРОВ

Материал представленный в статье является продолжением исследований по применению вейвлет-технологии в области обработки эхосигнала в радиолокационных системах обнаружения воздушных объектов, а именно решения задачи углового разрешения парной сосредоточенной цели (определённую, как "сверхразрешение") методом пороговой обработки результатов вейвлет-декомпозиции сигналов.

В статье обосновано построение и представлен алгоритм многоуровневой дискретной вейвлет-фильтрации по пирамидальному алгоритму Малла. Разработан синтез оптимального алгоритма построения вейвлет-декомпозиции на основе пакетных вейвлетов.

Ключевые слова: радиолокационный сигнал, вейвлет-анализ, пакетное вейвлет-преобразование.

Введение. Теория вейвлетов является частью прикладной математики. Математический характер многих теоретических положений вейвлет-анализа не позволяет дать прозрачную физическую интерпретацию многих вычислительных процедур, особенно дискретной версии вейвлет-преобразования (ВВП), которая имеет существенные отличия в организации техники вычислительных операций по сравнению с известным дискретным преобразованием Фурье [1].

Понятие вейвлет-фильтр относится к классу адаптивных фильтров с переменными параметрами, то есть не обладающими свойством стационарности, и определяется как последовательности h_n и g_n [2]. Основным элементом системы (банка) фильтровой обработки является пара фильтров: низкочастотный (НЧ) фильтр и высокочастотный (ВЧ) фильтр [3]. С точки зрения теории радиотехнических систем последовательности h и g являются дискретными импульсными характеристиками квадратурно-зеркальных фильтров $h(n)$ и $g(n)$ [4].

Конечной задачей представленных в статье частных результатов исследования является разработка метода распознавания типа принятого сигнала тестового варианта сосредоточенной цели (парной цели) на основании пороговой оценки числового показателя, характеризующего результат вейвлет-декомпозиции эхосигнала. При определении такого показателя задача распознавания – разрешения парной цели решается классическим методом сравнения полученного при обработке показателя с эталонным значением, хранящемся в базе данных, и последующей пороговой обработке.

Построение алгоритма многоуровневой дискретной вейвлет-фильтрации. Дискретное ВВП (ДВВП) реализуется только на основе частотной фильтрации системой дискретных фильтров, позволяющей организовать алгоритм быстрого преобразования. Дискретный вейвлет-анализ позволяет реализовать быстрое ДВВП по пирамидальному алгоритму Малла [4].

Процедура анализа стартует с масштаба $a = 1$ (a – параметр вейвлет-преобразования задающий ширину пакета; $a^{-\frac{1}{2}}\psi_0\left(\frac{t}{a}\right)$, $a > 0$, $a \in R$, где ψ_0 – исходная базовая функция), соответствующего высоким частотам (наиболее сжатый вейвлет) и при увеличении "a" продолжается в сторону низких частот. Процедура свёртки (сигнал×вейвлет) выполняется для всех отсчётов сигнала формируя первую строку масштабно-временной плоскости с коэффициентами cA_1 и cD_1. После полуполосного НЧ фильтра половина отсчётов удаляется операцией децимации. Децимация не изменяет разрешения, так как согласно теореме отсчётов удаляемые отсчёты являются избыточными и не несут информации. На следующем

шаге производится разложение только коэффициентов аппроксимации cA_1 по той же схеме, а коэффициенты cD_1 записываются в выходной сигнал.

Структурная схема алгоритма многоуровневой фильтрации дискретного сигнала приведена на рис. 1.

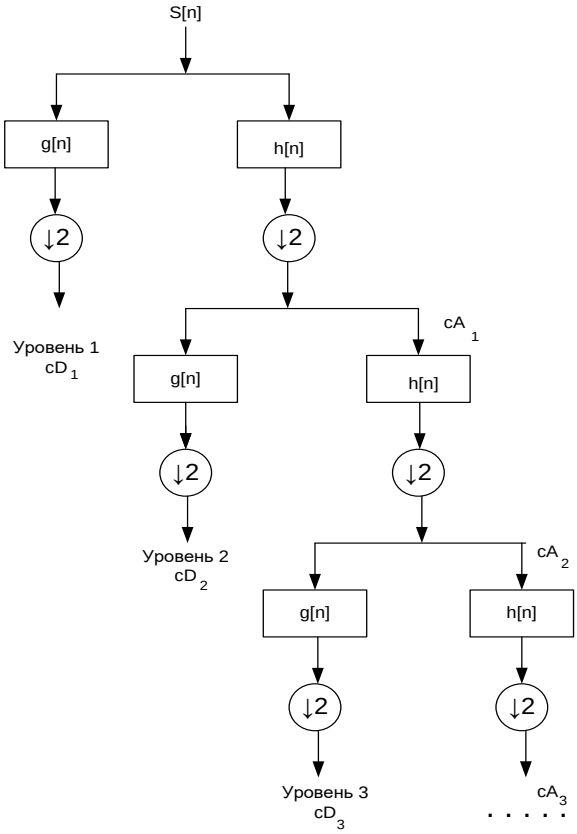


Рис. 1. Структурная схема алгоритма многоуровневой фильтрации дискретного сигнала

Синтез оптимального алгоритма построения вейвлет-декомпозиции на основе пакетных вейвлетов. ДВВП по алгоритму Малла, как следует из схемы рис. 1, на каждом шаге производит октавополосное "расщепление" сигнала на НЧ и ВЧ составляющие и "отсечение" ВЧ составляющих. Причина такого подхода заключается в неявном предположении о том, что НЧ составляющие содержат больше информации. В результате получается однобокое "дерево", которое используется для наглядного представления последовательности операций алгоритма обработки. Вид "дерева" показан на рис. 2 для тестового сигнала и вейвлета Добеши 4 порядка.

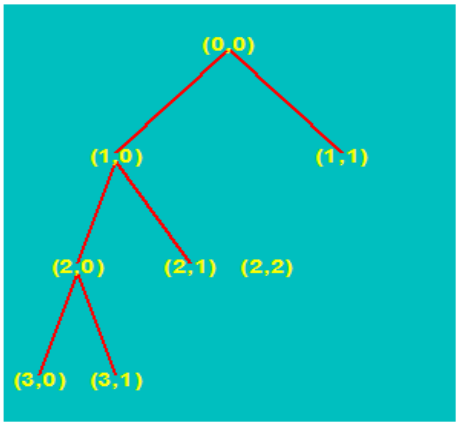


Рис. 2. Вид "дерева" дискретного вейвлет-преобразования по алгоритму Малла для тестового сигнала и вейвлета Добеши 4 порядка

Такой алгоритм построения системы декомпозиции сигнала с точки зрения информативности оценки составляющих оправдан не для всех реальных сигналов, особенно нестационарных и имеющих существенные локальные изменения.

Позднее предложен (Койфман и Викерхаузер) усовершенствованный метод, в котором процесс расщепления применяется как для НЧ, так и ВЧ составляющих. В результате получается полное (бинарное или сбалансированное) "дерево" разложения сигнала. Набор базисов построения такого алгоритма называют вейвлет-пакетами. Преобразование с помощью вейвлет-пакетов является адаптивным, то есть легко приспособляется к особенностям сигнала [5].

Вид "дерева" для того же базового вейвлета и тестового сигнала показано на рис. 3.

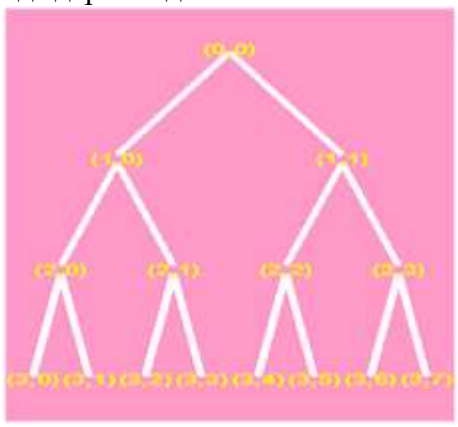


Рис. 3. Вид "дерева" дискретного вейвлет-преобразования с помощью вейвлет-пакетов для тестового сигнала и вейвлета Добеши 4 порядка

Точки расщепления (узлы) обозначены слева – направо и снизу – вверх.

Расчёт графиков рис. 2 и 3 производился для введенного сигнала (*s*) командой-оператором [6]:

$$T = wpdec(s,3,'db4','plot'). \quad (1)$$

Замечание. Команда вывода результатов расчёта (1) определяет формат рисунков, в частности цвет фона. При программном выводе на бумагу рисунок имеет стандартный формат.

Синтез оптимального алгоритма ("дерева") пакетного преобразования. Наилучшее построение "дерева", оптимальное в смысле выбранной функции стоимости, строится с использованием специальных встроенных функций-операторов: *wpsplt (.)* и *besttree (.)* [7].

В качестве функции стоимости используется энтропия [8], которая имеет несколько отличающихся определений. В данной работе выбрано определение энтропии по Шеннону:

$$E = -\sum_i s_i^2 \log(s^2) \quad (2)$$

и через логарифм энергии:

$$E = \sum_i \log(s^2)\,. \quad (3)$$

При большой энтропии декомпозиция сигнала "размазана" по базисным функциям, при малой энтропии большая часть нормы сигнала сосредоточена в малом числе базисных функций, и это даёт возможность существенного сжатия информации. Результаты пакетного разложения с функцией стоимости позволяют получить оптимальное "дерево" декомпозиции с числом ветвей "расщепления", меньше, чем на рис. 3. Программное решение задачи оптимизации выполняется встроенными функциями [9]:

$$besttree(T) \quad \text{и} \quad bestlevt(T), \quad (4)$$

где T – "дерево" стандартного пакетного разложения в соответствии с (1).

Задача решается для сигнальной функции, используемой для разрешения парной цели по структуре соответствующей дискретной биквантованной пачки с флюктуациями в центре.

Результат вычисления оптимального "дерева" пакетной вейвлет-декомпозиции данного сигнала представлен на рис. 4 и 5.

На рис. 4 показано "дерево" пакетной декомпозиции прямоугольной дискретной пачки при стандартном алгоритме (рис. 3). Оно соответствует как нефлюктуирующей (одиночная цель), так и флюктуирующей (парная цель) пачке (на правом рис. 4 показана первая).

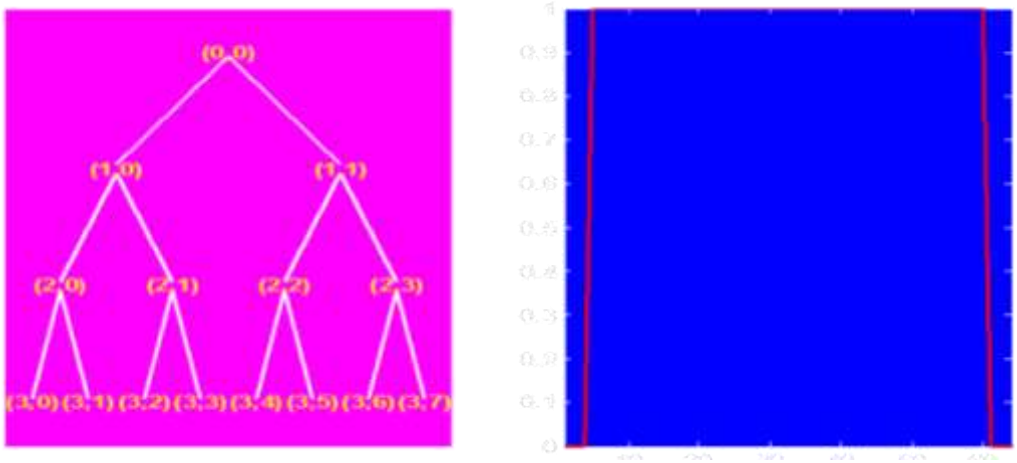


Рис. 4. Вид "дерева" пакетной декомпозиции прямоугольной дискретной пачки при стандартном алгоритме

На рис. 5 показано "дерево" оптимального вейвлет-разложения. В пачке за счёт флюктуаций имеются 2 нулевых отсчёта (M=64). В обоих случаях алгоритм ограничен тремя уровнями (для упрощения).

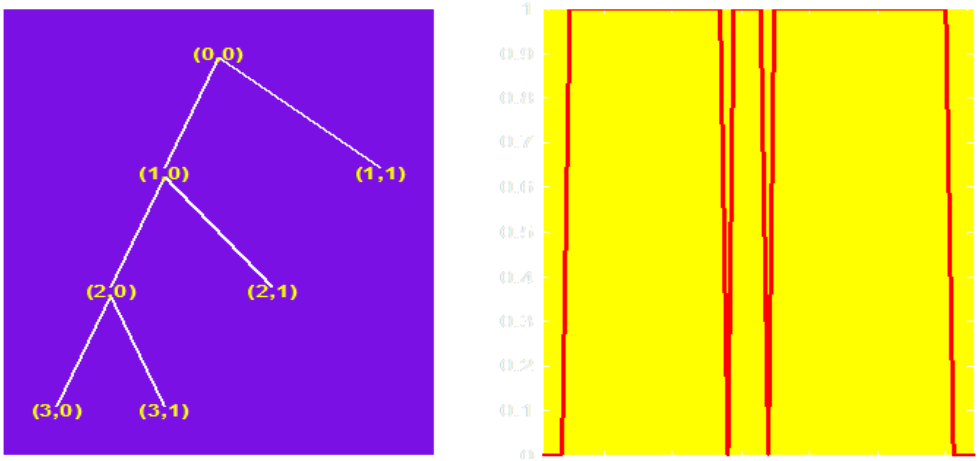


Рис. 5. Вид"дерева" оптимального вейвлет-разложения

Выводы. Сравнительный анализ рис. 4 и 5 показывает, что оптимизация построения алгоритма пакетной декомпозиции сигнала существенно сокращает число операций обработки при обеспечении минимальной энтропии.

Влияние характеристик и параметров предложенного оптимального алгоритма пакетной декомпозиции и сигнала на норму разности сигнальных функций (контрольных), с целью определения требования к виду базисного вейвлета, его порядку, уровню декомпозиции, амплитудно-временным параметрам сигнала и образца, а также допустимой СКВ шума в решении задачи разработки метода распознавания типа принятого сигнала тестового варианта сосредоточенной цели на основании пороговой оценки числового показателя, характеризующего результат вейвлет-декомпозиции эхосигнала, являются предметом дальнейших исследований.

ЛІТЕРАТУРА:

1. Чуи К. Введение в вейвлеты / К. Чуи.– М.: Мир, 2001. – 412 с.

2. Malla, S. A wavelet tour of signal processing / S. Malla. - San Diego: Academic press, 2005. – 577 с.

3. Бурнаев Е.В. Применение вейвлет-преобразования для анализа сигналов – М.:МФТИ, 2007. – 138 с.

4. Долгушин В.П., Лоза В.Н., Борзак А.Н., Жиров Б.Г. Распознавание класса целей методом оценки статистических параметров вектора вейвлет-декомпозиции сигнала // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2014. – № 45. – С. 24 – 33.

5. Лоза В.Н., Ленков Е.С. Особенности применения пакетных алгоритмов вейвлет-анализа при обработке сигналов // Збірник наукових праць "Системи обробки інформації", 2016, випуск 7 (144), с. 66 – 71.

6. Смоленцев Н.К. Вейвлет-анализ в MATLAB – М.: ДМК Пресс, 2010. – 448 с.

7. Дьяконов В.П. MATLAB и SIMULINK для радиоинженеров – М.: ДМК Пресс, 2011. – 976 с.

8. Лоза В.М. Анализ механизма преобразования сигналов с использованием пакетных алгоритмов вейвлет-анализ / Лоза В.М. // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2016. – № 53. – С 35 - 40.

9. Дьяконов В.П., Круглов В.В. Математические пакеты расширений MATLAB. Специальный справочник. – СПб.: Питер, 2001. - 488 с.

REFERENCES:

1. 1. Chui K. Vvedenie v vejvlety / K. Chui.– M.: Mir, 2001. – 412 s.

2. Malla, S. A wavelet tour of signal processing / S. Malla. - San Diego: Academic press, 2005. – 577 с.

3. Burnaev E.V. Primenenie vejvlet-preobrazovanija dlja analiza signalov – M.:MFTI, 2007. – 138 s.

4. Dolgushin V.P., Loza V.N., Borzak A.N., Zhirov B.G. Raspoznavanie klassa celej metodom ocenki statisticheskih parametrov vektora vejvlet-dekompozicii signala // Zbirnik naukovih prac' Vijs'kovogo institutu Kiïvs'kogo nacional'nogo universitetu imeni Tarasa Shevchenka. – K., 2014. – № 45. – S. 24 – 33.

5. Loza V.N., Lenkov E.S. Osobennosti primenenija paketnyh algoritmov vejvlet-analiza pri obrabotke signalov // Zbirnik naukovih prac' "Sistemi obrobki informacii", 2016, vipusk 7 (144), s. 66 – 71.

6. Smolencev N.K. Vejvlet-analiz v MATLAB – M.: DMK Press, 2010. – 448 s.

7. D'jakonov V.P. MATLAB i SIMULINK dlja radioinzhenerov – M.: DMK Press, 2011. – 976 s

8. Loza V.M. Analyz mehanyzma preobrazovanyja sygnalov s yspol'zovanyem paketnыh algorytmov vejvlet-analyz / Loza V.M. // Zbirnyk naukovyh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka. – K., 2016. – № 53. – S 35 - 40.

9. D'jakonov V.P., Kruglov V.V. Matematicheskie pakety rasshirenij MATLAB. Special'nyj spravochnik. – SPb.: Piter, 2001. - 488 s.

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

к.т.н. Лоза В.М.

ПОБУДОВА АЛГОРИТМУ БАГАТОРІВНЕВОЇ ДИСКРЕТНОЇ ВЕЙВЛЕТ-ФІЛЬТРАЦІЇ РАДІОЛОКАЦІЙНОГО СИГНАЛУ І СИНТЕЗ ОПТИМАЛЬНОГО АЛГОРИТМА ПОБУДОВИ БАЗИ ФІЛЬТРІВ

Матеріал поданий у статті є продовженням досліджень щодо застосування вейвлет-технології в області обробки ехосигнала в радіолокаційних системах виявлення повітряних об'єктів, а саме вирішення задачі кутового розрізнення парної зосередженої цілі (визначену, як "надрозрізнення") методом порогової обробки результатів вейвлет-декомпозиції сигналів.

У статті обґрунтовано побудову і представлений алгоритм багаторівневої дискретної вейвлет-фільтрації за пірамідальним алгоритмом Малла. Розроблено синтез оптимального алгоритму побудови вейвлет-декомпозиції на основі пакетних вейвлетів.

Ключові слова: радіолокаційний сигнал, вейвлет-аналіз, пакетне вейвлет-перетворення.

Ph.D. Loza V.N.

CONSTRUCTION OF ALGORITHM MULTI-LEVEL DISCRETE WAVELET - FILTRATION RADAR SIGNAL AND THE SYNTHESIS OF OPTIMAL ALGORITHM FOR CONSTRUCTING BASE FILTERS

The material presented in the article is a continuation of research on the application of wavelet technology in the processing of the echo signal in the radar systems detect air targets, namely, solving the problem of the angular resolution of the pair focused goals by thresholding the results of the wavelet decomposition of signals.

The article substantiates the construction and the algorithm of multi-level discrete wavelet filtering algorithm pyramidal Malla. A synthesis of the optimal algorithm for constructing the wavelet decomposition based on wavelet packet.

Keywords: radar signal, wavelet analysis, wavelet transform batch.

УДК 621.396.967

к.військ.н. **Нікіфоров М.М.** (ВІКНУ)
к.т.н., с.н.с. **Жиров Г.Б.** (ВІКНУ)
к.т.н., доц. **Пампуха І.В.** (ВІКНУ)

МОЖЛИВОСТІ ІНТЕГРОВАННОЇ СИСТЕМИ ПАСИВНОГО МОНІТОРІНГА ПРОСТОРУ В УМОВАХ ЗАСТОСУВАННЯ ВИСОКОТОЧНОЇ ЗБРОЇ

У статті проведений аналіз існуючих систем розвідки, які базуються на використанні різних фізичних властивостей, а також перспективні світові тенденції створення та розвитку інформаційно-розвідувальних систем. Визначено, що використання багато спектральних і багато частотних датчиків, які взаємодоповнюють один одного, дозволяє в процесі моніторингу формувати високоінформативні узагальнені відомості про навколишній простір. При цьому найбільший обсяг інформації про навколишній простір може бути отриманий при спільній комплексній обробці сигналів в рамках інтегрованої розвідувально-інформаційної системи. Розвідувально-інформаційної системи на основі сейсмо-акустичних систем мають багато переваг та домінують за критерієм «ефективність - вартість».

Ключові слова: акустична система розвідки, сейсмічна система розвідки, сейсмоакустична система розвідки, інтегрована розвідувально-інформаційна система.

Вступ. Досвід локальних війн свідчить про необхідність чіткого і ясного розуміння загрози, яку несе високоточна зброя (ВТЗ), а також об'єктивної оцінки рівня оснащеності збройних сил з точки зору протидії ВТЗ. В результаті вивчення принципів побудови і застосування ВТЗ в локальних війнах і конфліктах з'явилася можливість вироблення концептуальних напрямів протидії. Такі напрями передбачають комплексність застосування різнорідних сил і засобів по єдиному задуму і плану, а також багатоцільове їх застосування по об'єктах дії.

Сучасні світові тенденції напрямів розвитку даних засобу розвідки пов'язано з розробкою і впровадженням засобів саме пасивної розвідки (локації), з метою забезпечення максимально можливої скритності військ.

Американська організація "Research and Markets" підготувала звіт під назвою "The Military and Civil Aviation Passive Radar Market : 2013-2023", в якому розглянула ринкові

перспективи пасивних локаторів як для військових застосувань, так і для цивільної авіації на період з 2013 до 2023 року.

З цього звіту виходить, що до кінця 2023 роки очікувані інвестиції в розробку радіолокаторів перевищать 10 млрд. доларів, а в області військових радіолокаторів пасивні локатори займуть долю у розмірі 41% [1]. При цьому, в розробці пасивних локаторів братимуть участь такі лідируючі компанії в цій галузі, як:

1. «Silent Sentry» (Lockheed Martin, USA);
2. «Celldar» (Roke Manor & BAE Systems, UK);
3. «CORA» (FGAN - Die Forschungsgesellschaft fur Angewandte Naturwissenschaften, Germany);
4. «Cristal» (Thales, EU);
5. Cassidian, EADS, Germany.

Постановка завдання. В статті розглядаються питання аналізу існуючих пасивних систем розвідки: сейсмічних, акустичних, сейсмоакустичних та оптико-електронних, а також пропонуються шляхи їх інтегрування, щодо створення багато сенсорного поля розвідки в усіх технічно доступних фізичних середовищах з метою виявлення та пеленгації позицій застосування зброї та пересування особового складу і техніки з подальшою ідентифікацією.

Результати дослідження. Завдання виявлення військової техніки та маловисотних літальних апаратів з використанням різних фізичних властивостей вирішувалася ученими багатьох країн особливо інтенсивно останні 10-15 років. При цьому найбільш успішними є результати, отримані в США, Франції і Ізраїлі [2]. У основі цих розробок лежать фізичні ефекти, пов'язані зі змінами фізичних властивостей (наприклад електростатичного, магнітного, гравітаційного, акустичного, сейсмічного та ін.) при переміщенні в них літальних апаратів.

До пасивних датчиків, що забезпечують отримання інформації про навколишній простір, відносяться системи, що одержують інформацію на основі аналізу електромагнітного поля в різних діапазонах довжин хвиль: оптичні датчики, інфрачервоні, радіометричні; магнітометричні; сейсмічні; акустичні і сейсмо-акустичні датчики та їх інтегрування. Інтегрована спільна обробка інформації, що отримується від декількох датчиків, дозволяє сформувати звідні узагальнені відомості про навколишній простір і прогноз його зміни. Найбільш широке застосування при моніторингу навколишнього простору знайшли дані оптико-електронні, сейсмічні та акустичні датчики та системи.

Сейсмічні системи розвідки. Під сейсмічною розвідкою (СР) розуміється добування інформації шляхом виявлення і аналізу деформаційних та зсувних полів в земній поверхні, що виникають під впливом різних вибухів [3]. СР визначає: координати епіцентру вибуху, потужність і час вибуху, кількість вибухів в групі. Сейсмічний метод виявлення і ідентифікації ядерних вибухів отримав загальне визнання як один з основних, крім вибухів в космосі і в повітрі на великих висотах (понад декілька десятків кілометрів). Сейсмічний метод застосовний для виявлення ядерних вибухів як на малих, так і на великих відстанях, що досягають до 17 000 км.

Сейсмічна розвідка є складною динамічною системою. У ній відбуваються процеси перетворення енергії і інформації, найважливішими з яких є збудження сейсмічним джерелом первинних хвиль, поширення їх в геологічному середовищі з утворенням на неоднорідностях вторинних хвиль, прийом і запис пружних коливань в точках спостереження, обробка і інтерпретація сейсмічних записів.

Історичні успіхи застосування сейсмодатчиків в розвідувально-сигналізаційних приладах (РСП), призначених для розвідки наземних рухомих об'єктів належать США. Висока ефективність застосування РСП привела до оснащення цими приладами збройних сил союзників США, а також до розробки їх аналогів у ряді інших країн. Типовими зразками таких автоматичних систем являються [8]:

1. Система CLASSIC 2000 (фірма Thales, Франція). Система використовується в 42 країнах світу, включаючи 12 країн, що входять до складу НАТО. Сейсмічний датчик системи забезпечує виявлення людини в діапазоні від 1 до 80 метрів, а легкової машини – до 250 метрів;

2. Система REMBASS II (фірма L - 3 Communications - East, США). Система знаходиться на озброєнні сил спеціальних операцій, сухопутних військ і військово-повітряних сил США і Ізраїлю, успішно застосовувалася в Іраку і Афганістані. Комплексний датчик системи, що має сейсмічний і акустичний канали, забезпечує виявлення людини на дальності до 75 метрів, вантажного автомобіля - до 250 метрів, гусеничної машини - до 350 метрів;

3. Система Improved Air Delivered Sensor (IADS) (фірма Northrop Grumman Electronic Systems sector - ATE/Simulation, США), забезпечує виявлення як наземних, так і повітряних об'єктів. Наступний варіант системи IADS II додатково забезпечуватиме вимір координат і розпізнавання об'єктів;

4. Система SEMAG (фірма Hirtenberger AG, Австрія). Система включає сейсмічні і магнітометричні датчики і застосовується для виявлення танків і управління мінами. Ця система є прикладом широкого класу систем управління мінами і мінними полями.

Акустичні системи розвідки. Під акустичною розвідкою розуміється отримання інформації шляхом прийому і аналізу акустичних сигналів інфразвукового, звукового, ультразвукового діапазонів, що поширюються в повітряному середовищі від об'єктів розвідки [4]. Акустична розвідка (АР) забезпечує отримання інформації, що міститься безпосередньо у виголошуваній або відтворній промові (акустична мовна розвідка), а також в параметрах акустичних сигналів, які є супутніми при роботі озброєння і військової техніки, механічних облаштувань оргтехніки і інших технічних систем (акустична сигнальна розвідка).

Сухопутні війська зарубіжних країн широко використовують взаємодоповнюючі (комплексні) системи, що дозволяє ефективно вести розвідку і спостереження у будь-який час доби при будь-якій видимості і погоді.

Попри те, що деякі з існуючих РСП здатні виявляти літальні апарати, останнім часом підвищений інтерес проявляється до нових систем, спеціально сконструйованих для виявлення вертольотів і літаків на малих висотах. Такі системи вже з'явилися на озброєнні сухопутних військ США, Франції і Ізраїлю [2, 8]. До таких систем відносяться:

Американська система MANPAC - 100. Забезпечує виявлення, розпізнавання, визначення азимута і кута місця вертольотів, що летять низько, гвинтових літаків і дистанційно керованих безпілотних літальних апаратів (БЛА). Ця система у кінці 1990-х років проходила польові випробування і призначена для використання сухопутними військами в передових підрозділах протиповітряної оборони, озброєних переносними зенітними ракетними комплексами "Стингер".

Французька система HELISPOT (Balise Acoustique Classification Helicoptere). Система може застосовуватися як окрема акустична система або в групі для утворення " бар'єру" виявлення в широкому секторі. Вона формує пеленги на виявлені об'єкти і з вірогідністю 0.95 забезпечує автоматичне розпізнавання десяти типів вертольотів, акустичні портрети яких закладені в облаштування системи. Інформація про тип і пеленг виявленого вертольота передається вбудованим в систему ультракороткохвильовим (УКВ) передавачем на центральний процесор, що знаходиться на посту спостереження, який може одночасно приймати і обробляти дані від 16 систем. Система забезпечує виявлення легких вертольотів в нормальних погодних умовах на відстані 2 - 5 км, важких, - до 12 км (при сильному вітрі - до 4 км), а також їх пеленгація з точністю від 2 до 20 град., залежною від відстані і умов.

Ізраїльська система HELISPOT. Вона включає акустичний прилад, що розміщується на землі або транспортному засобі. Система забезпечує виявлення, розпізнавання і пеленгацію вертольотів, що летять низько, та БЛА на дальності до 3 км з точністю до 3 град. Акустичний

прилад включає мікрофон і класифікатор, що визначає тип цілі по спектру акустичного сигналу, що приймається. Інформація про виявлену ціль передається по УКВ радіоканалу або дротяній лінії зв'язку на пост збору розвідданих.

Ізраїльська система ROAD використовує акустичний прилад, що забезпечує виявлення середніх вертольотів на відстані 1 - 2 км, великих вертольотів - до 2,7 км, а також вертольотів що зависають на малих висотах - до 2,5-3 км.

Розглянуті системи використовують тільки акустичні хвилі, що поширюються в повітрі. В той же час експериментальні дослідження показують, що нарівні з акустичними хвилями можна ефективно використати і сейсмічні хвилі, що поширюються в землі. Комбінована обробка акустичних і сейсмічних хвиль може істотно підвищити ефективність розвідки. Акустичні хвилі, що поширюються в повітрі, приймаються акустичними мікрофонами, що перетворюють акустичний тиск в електричний сигнал. Аналогічно сейсмічні хвилі поширюються в поверхневому шарі землі і перетворяться сейсмічними датчиками в електричний сигнал, що відповідає коливанням ґрунту.

Поширення акустичних хвиль залежить від стану атмосфери [4], а поширення сейсмічних хвиль - від структури, складу і стану поверхневого шару землі [3].

Сейсмоакустичні системи розвідки. У сухопутних військах США на озброєнні знаходяться розвідувальне-сигналізаційні прибори (РСП) "Рембасс" (REmotely Monitored BAttlefield Sensor System - REMBASS) трьох поколінь [2, 5, 8]. Вони призначені для раннього виявлення, визначення місця розташування і ідентифікації наземних рухливих об'єктів і цілей, в першу чергу мобільних пускових установок оперативно-тактичних ракет, зенітних ракетних комплексів і бойових машин. Системи "Рембасс" усіх поколінь розгортаються в тактичній глибині бойових порядків супротивника, а також у бойових порядках та тилу своїх військ. До їх складу входять РСП, радіоретранслятори, засоби прийому і обробки даних. Розвідувально-сигналізаційні прилади розгортаються на відстані 50-350 м один від одного на найбільш вірогідних напрямах руху мобільних об'єктів (дороги, переправи та ін.). Вони можуть встановлюватися як вручну, так і за допомогою авіації, і артилерії. Кожен РСП включає датчик, радіопередавач, електронний блок і акумуляторну батарею. Деякі прилади можуть бути забезпечені пристроями самоліквідації і фотоелементами для їх включення тільки в темний час доби.

Сейсмічні датчики уловлюють коливання ґрунту, рухи людини, що відбуваються в результаті його руху - до 75м. та транспортного засобу - до 350м. В якості чутливих елементів в них використовуються заглиблені у ґрунт геофони. Дальність дії цих приладів залежить від рівня і характеру фону навколишнього сейсмічного шуму і типу ґрунту.

На озброєнні ЗС Росії знаходиться комплекси розвідувальне-сигналізаційних засобів 1К18 "Реалія", який призначений для дистанційного виявлення пересування особового складу (до 70 м.) та техніки (до 500 м.) у тилу супротивника і на границях вірогідного зіткнення з ним та передачі відомостей про виявлені об'єкти по радіоканалу в масштабі часі, близькому до реального.

Малогабаритна розвідувально-сигналізаційної апаратура 1К124 " Табун" призначена для дистанційного виявлення пересування особового складу - до 50 м. та техніки - до 200 м.

Британська переносна система дистанційного спостереження Tobias має вагу без батарей живлення 6,35 кг і 80 сейсмічних датчиків (вага кожного 0,075 кг), що сполучаються дротами. Дальність виявлення людини, що рухається, до 300 метрів, а сама система перекриває простір радіусом 2,4 км.

Оптико-електронні системи розвідки. Оптико-електронна розвідка – процес добування інформації за допомогою засобів, що включають вхідну оптичну систему з фотоприймачем і електронні схеми обробки електричного сигналу, які забезпечують прийом електромагнітних хвиль видимого та інфрачервоного діапазонів, випромінених або відбитих об'єктами і місцевістю[5, 6, 7].

Оптико-електронна розвідка (ОЕР) призначена для вирішення наступних завдань: виявлення інформативних об'єктів; визначення форми, розмірів, стану інформативних об'єктів; визначення характеру випущеної продукції, її обсягу та ін.; зйомки територій з метою картографування місцевості; розвідки метеообстановки в заданих районах.

Апаратура ОЕР встановлюється на космічних і повітряних носіях, а також може застосовуватися в наземних умовах. Принцип роботи апаратури ОЕР заснований на прийомі власного випромінювання об'єктів і фона або відбитого від них випромінювання сонця, місяця, зоряного неба. Апаратура ОЕР дозволяє відрізняти об'єкт від фону за умови, що яскравість об'єкта перевищує яскравість фону[5].

Серед параметрів оптичних систем впливовими можна в загальному випадку визнати фокусну відстань, робочий діапазон довжин хвиль, а також тип і параметри приймача.

Як фактори, пов’язані з особливостями конструктивних рішень оптико-електричних перетворювачів, визначимо наявність фільтрації та підсилення сигналів, стійкість до електромагнітних завад, здатність генерувати власні шуми.

Принцип дії ОЕП (пасивний, активний, активно-пасивний) однозначно пов'язаний з обраним спектральним діапазоном та параметрами оптичного сигналу. За спектральним діапазоном – у видимому, інфрачервоному та ультрафіолетовому[5, 6, 7].

Подальшим розвитком принципів об'єднання даних, що характеризують окремі об'єкти спостереження, є ідея "поєднання датчиків". Термін "поєднання датчиків" визначається також як "злиття розвідувальних даних" (intelligence fusion) [2, 9].

Поєднання датчиків припускає інтеграцію і аналіз даних від засобів виявлення і є процесом збору і узагальнення даних за визначенням місця розташування і ідентифікації, отриманих від різних датчиків (видовій інформації, РЛС, розпізнавання сигналів (Signal Intelligence SIGINT), виявлення руху), в цілях отримання єдиної комплексної картини навколишнього оточення. Поєднання датчиків, в процесі якого обробляються дані, що поступають від різних джерел, спрямоване на отримання точнішій, надійнішій і повнішій інформації в порівнянні з інформацією, що отримується від окремого джерела індивідуально.

Під інтегрованою системою моніторингу (ІСМ) навколишнього простору розуміють сукупність спільно функціонуючих датчиків, засобів зв'язку, обчислювальних і програмних засобів, засобів управління і індикації, призначених для отримання інформації про різного роду об'єктах, об'єднання інформації, що поступає, від датчиків і відображення результуючої інформації. Найважливішу роль в ІСМ грають інформаційні датчики, тактико-технічні характеристики яких визначають можливості високоефективного функціонування [10].

Інша ситуація може складатися з отриманням відомостей про стан об'єктів або процесів на великій території при обмеженій дальності дії інформаційних датчиків. В цьому випадку доводиться об'єднувати інформацію, що поступає від просторово рознесених датчиків, сукупна зона огляду яких забезпечує перекриття усієї площі території, що контролюється [9].

Найбільш складним є поєднання датчиків в системах геопросторової розвідки (Geospatial Intelligence Systems - GIS), що представляють важливий інструмент ведення бойових дій [2, 9]. Прикладом такої системи є багатозадачна мережева розвідувальна система Imilite ізраїльській компанії Rafael Advancend Defence Systems [2]. Система призначена для використання декількох видових датчиків, отримання і обробки даних в уніфікованому виді для поширення користувачам і клієнтам.

Поєднання датчиків сприяє збільшенню чіткості зображень. Зокрема, коли використовується тільки один тип датчика, то при його функціонуванні в умовах поганої погоди або дії несприятливих чинників, обумовлених веденням бойових дій, отримання чіткого зображення може виявитися неможливим.

Проведений аналіз різнорідних систем розвідки дозволяє виділити сейсмоакустичні системи, як найбільш ефективні для вирішення задач по виявленню та пеленгації позицій стріляючої артилерії та задачі визначення факту порушення кордону з подальшою

ідентифікацією, за умови ведення військової розвідки. Дане твердження базується на тому, що сейсмоакустичні системи володіють наступними перевагами:

1. Вони забезпечують стійке автоматичне функціонування: в складних метео умовах (дощ, сніг, туман); в умовах поганої оптичної видимості (ніч); в напрямках на джерела яскравого світла (сонце); в умовах сильної задимленості і запиленості; в умовах порізаного рельєфу місцевості (пагорби, гірські перевали, ущелини, русла річок та інше);

2. Сейсмоакустичні системи мають повну скритністю, так як не формують зондуючих сигналів, це виключає їх завчасне виявлення. Найважливішим якістю цих систем є збереження працездатності в умовах сучасного радіоелектронного придушення.

3. Такі системи мають малі габарити, низьке енергоспоживання і краще у порівнянні з іншими системи (радіолокаційними, оптико-електронними та ін.) відповідають критеріям «ефективність - вартість».

Таким чином, для вирішення поставлених завдань розвідки пропонується створити інтегровану пасивну систему моніторингу навколишнього простору зі сукупністю спільно функціонуючих сейсмо-акустичних та оптико-електронних датчиків, засобів зв'язку, обчислювальних і програмних засобів, засобів управління і індикації, призначених для отримання інформації про різного роду об'єктах, об'єднання інформації, що поступає, від датчиків і відображення результуючої інформації. Використання трьох різнорідних інформаційних потоків значно зменшує похибку при визначенні координат цілі.

Функціонування такої системи дозволить підвищити живучість, а отже, і ефективність застосування своїх засобів. У цьому випадку ситуація не буде виглядати як дуельна (нападаючому для виключення можливого впливу по ньому буде потрібно нейтралізувати певну безліч об'єктів розвідки, що не завжди піддається реалізації).

Зокрема, використання ресурсів такої системи дає суттєву основу для розробки нових способів застосування як озброєння, так і підрозділів. Таким чином, розвиток сучасних технологій, засобів обробки інформації дозволяють зробити ще один крок у вдосконаленні практики застосування систем озброєння, зокрема виробити нові концептуальні підходи, щодо створення єдиної інформаційної розвідувальної системи.

Висновки

1. Із вищезазначеного можна зробити висновок про те, що в комплексах моніторингу навколишнього середовища інтеграція датчиків здійснюється на різних рівнях об'єднання інформації, доцільність використання яких визначається колом вирішуваних завдань, конкретними умовами застосування комплексів і станом розвитку алгоритмічного і програмного забезпечення обчислювальних систем. При цьому найбільший обсяг інформації про навколишній простір може бути отриманий при спільній комплексної обробці сигналів в рамках інтегрованої розвідувально-інформаційної системи.

2. Сучасний рівень розвитку інформаційних датчиків і розроблене алгоритмічне забезпечення по об'єднанню інформаційних потоків дозволяють створювати інтегровані розвідувально-інформаційної системи, що володіють широкими можливостями для вирішення різноманітних завдань військового призначення.

3. Розвідувально-інформаційної системи на основі сейсмо-акустичних систем мають багато переваг та домінують за критерієм «ефективність - вартість».

ЛІТЕРАТУРА:

1. The Military and Civil Aviation Passive Radar Market: 2013 – 2023/ http://www.researchandmarkets.com/reports/2598562/the_military_and_civil_aviation_passive_radar#pos-0

2. Мосалев В. Системы дистанционного наблюдения за полем боя на базе разведывательно-сигнализационных приборов / Зарубежное военное обозрение. – 2000. – № 2. – С. 21–27.

3. Гурвич И.И., Боганик Г.Н. Сейсмическая разведка: Учебник для вузов. - 3-е изд., перераб. - М.: Недра, 1980. – 551 с.

4. Красильников В.А, Крылов В.В. Введение в физическую акустику: учебное пособие / Под ред. В.А. Красильникова. - М: Наука. Главная редакция физико-математической литературы, 1984. – 400 с.

5. Якушенков Ю.Г. Теория и расчет оптикоэлектронных приборов / Ю.Г. Якушенков. – 4-е изд., перераб, и доп. – М.: Логос, 1999. – 480 с.

6. Москвитин С.В. Теоретические основы оптической локации / С.В. Москвитин, А.И. Стрелков. – Х: ВИРТА ПВО, 1992. – 369 с.

7. Оптические приборы наблюдения, обработки и распознавания объектов в сложных условиях / Б.С. Алешин, А.В. Бондаренко и др. – М: Государственный научно-исследовательский институт авиационных систем, 1999. – 140 с.

8. Ерохин Е.И. Современные средства воздушной разведки и наблюдения США / Е.И.Ерохин, В.А.Чабанов // Научно-техн. информация. Сер. Авиационные системы. – 2014. – №6. – С.18–35.

9. Сочетание датчиков: улучшение ситуационной осведомленности. Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления // Серия: «Техническое оснащение спецслужб зарубежных государств». – 2013. – № 1.

10. Верба В.С. Интеграция данных в многодатчиковых бортовых информационно-управляющих системах / В.С. Верба, В.И. Меркулов, Е.В. Попов, В.С. Чернов // Информационно-управляющие системы. 2014. – № 2. – С.32-43.

REFERENCES:

1. The Military and Civil Aviation Passive Radar Market: 2013 – 2023/ http://www.researchandmarkets.com/reports/2598562/the_military_and_civil_aviation_passive_radar#pos-0

2. Mosalev V. Sistemy distantsionnogo nablyudeniya za polem boya na baze razvedyvatelno-signalizatsionnykh priborov/ Zarubezhnoe voennoe obozrenie. - № 2, 2000. - S. 21 - 27.

3. Gurvich I.I., Boganik G.N. Seysmicheskaya razvedka: Uchebnik dlya vuzov. - 3-e izd., pererab. - M.: Nedra, 1980. - 551 s

4. Krasilnikov V.A, Krylov V.V. Vvedenie v fizicheskuyu akustiku: uchebnoe posobie/ Pod red. V.A. Krasilnikova. - M: Nauka. Glavnaya redaktsiya fiziko-matematicheskoy literatury, 1984. - 400 s.

5. Yakushenkov Yu.G. Teoriya i raschet optikoelektronnykh priborov. / Yu.G. Yakushenkov. – 4-e izd., pererab. i dop. – M.: Logos, 1999. – 480 s.

6. Moskvitin S.V. Teoreticheskie osnovy opticheskoy lokatsii / S.V. Moskvitin, A.I. Strelkov. – Kh: VIR- TA PVO, 1992. – 369 s.

7. Opticheskie pribory nablyudeniya, obrabotki i raspoznavaniya obektov v slozhnykh usloviyakh / B.S. Aleshin, A.V. Bondarenko i dr. – M: Gosudarstvennyy nauchno-issledovatelskiy institut aviatsionnykh sistem, 1999. – 140 s.

8. Yerokhin Ye.I., Chabanov V.A. Sovremennye sredstva vozdushnoy razvedki i nablyudeniya SShA. // Nauchno-tekhn. informatsiya. Ser. Aviatsionnye sistemy. – M.: NITs GosNIIAS. 2014. №6. S. 18-35.

9. Sochetanie datchikov: uluchshenie situatsionnoy osvedomlennosti. Inostrannaya pechat ob ekonomicheskom, nauchno-tekhnicheskom i voennom potentsiale gosudarstv-uchastnikov SNG i tekhnicheskikh sredstvakh ego vyyavleniya. // Seriya: «Tekhnicheskoe osnashchenie spetssluzhb zarubezhnykh gosudarstv». – M.: VINITI. 2013. № 1.

10.Verba V.S., Merkulov V.I., Popov Ye.V., Chernov V.S. Integratsiya dannykh v mnogodatchikovykh bortovykh informatsionno-upravlyayushchikh sistemakh. // Informatsionno-upravlyayushchie sistemy. 2014. № 2. S 32-43

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

к.**воен.н. Никифоров Н.Н., к.т.н., с.н.с. Жиров Г.Б., к.т.н., доц. Пампуха И.В.**

ВОЗМОЖНОСТИ ИНТЕГРИРОВАНОЙ СИСТЕМЫ ПАССИВНОГО МОНИТОРИНГА ПРОСТРАНСТВА В УСЛОВИЯХ ПРИМЕНЕНИЯ ВЫСОКОТОЧНОГО ОРУЖИЯ

В статье проанализированы существующие системы разведки, которые базируются на использовании разных физических свойств, а также перспективные мировые тенденции развития, создания информационно-разведовательных систем. Определенно, что использование

много спектральных и много частотных датчиков, которые взаимодополняют друг друга, позволяет в процессе мониторинга формировать высокоинформативные обобщенные сведения об окружающем пространстве. При этом наибольший объем информации об окружающем пространстве может быть получен при общей комплексной обработке сигналов в рамках интегрированной разведывательно-информационной системы. Разведывательно-информационной системы на основе сейсмо-акустических систем имеют много преимуществ и доминируют по критерию "эффективность - стоимость".

Ключевые слова: акустическая система разведки, сейсмическая система разведки, сейсмо-акустическая система разведки, интегрирована разведывательно-информационная система.

Ph.D. Nikiforov N.N., Ph.D. Zhyrov G.B., Ph.D. Pampuha I.V.

POSSIBILITIES OF ИНТЕГРИРОВАНОЙ OF SYSTEM OF PASSIVE MONITORING OF SPACE IN THE CONDITIONS OF APPLICATION OF HIGH-FIDELITY WEAPON

In the article the existent systems are analysed secret services that are based on the use of different physical properties, and also perspective world progress, creation of the informative secret service systems trends. Certainly, that the use much and many frequency spectral sensors that complement each other allow in the process of monitoring to form the highly informing generalized information about surrounding space. Thus the most volume of information about surrounding space can be got at general complex treatment of signals within the framework of the integrated reconnaissance-informative system. Reconnaissance-informative system on the basis of the seismo of acoustic systems have many advantages and prevail on a criterion "efficiency is a cost".

Keywords: acoustic system of secret service, seismic system of secret service, seismo of acoustic system of secret service, the reconnaissance-informative system is integrated.

УДК 621.396.6

к.т.н., доц. **Радзівілов Г.Д.** (ВІТІ)
к.т.н. **Романенко В.П.** (ІСЗІ НТУУ «КПІ»)
Бригадир С.П. (ВІТІ)

ОЦІНКА ПОКАЗНИКІВ ЯКОСТІ ДІАГНОСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РЕМОНТУ ВІЙСЬКОВОЇ ТЕХНІКИ ЗВ'ЯЗКУ

У статті представлена методика оцінки якості діагностичного забезпечення ремонту техніки зв'язку, яка використовується в Збройних Силах України. Показано, що однією з основних цілей розв'язання даної задачі є підвищення ефективності обслуговування технічних систем, пов'язаного з оптимізацією технологічних процесів, їхнього поточного ремонту та модернізації. Отримані нові функціональні залежності оцінюваних показників діяльності фахівців від керованих змінних з врахуванням можливості виникнення діагностичних помилок, формалізований процес кількісної оцінки показників якості діагностичного забезпечення ремонту військової техніки зв'язку. Також проведено аналіз застосування представленої методики на прикладі діагностування сучасного радіоприймача.

Ключові слова: діагностика, технічне діагностування, технічні системи, ремонт.

Постановка проблеми. Задачі діагностичного забезпечення отримали широке розповсюдження у звязку з появою новітніх великих технічних і організаційно – технічних систем і комплексів, до яких відносяться майже всі сучасні засоби і комплекси зв'язку і управління. Такі об'єкти прийнято називати складними. Необхідно зазначити, що багато негативних впливів, що призводять до відмов складних систем, носять прихований характер і можуть бути виявлені завчасно тільки при використанні ефективних обчислювальних методів обробки даних спостережень за контрольованими змінними та параметрами висококваліфікованими фахівцями.. Безумовно, важливою вимогою до систем технічної діагностики є високоякісне розв'язання задачі прогнозування технічного стану. Однією з основних цілей розв'язання даної задачі є підвищення ефективності обслуговування технічних систем, пов'язаного з оптимізацією технологічних процесів, їхнього поточного ремонту та модернізації. Питання технічного діагностування таких об'єктів потребує нових наукових рішень і технічних підходів.

Задача полягає в забезпеченні потрібного згідно керівних технічних документів по ремонтопридатності значення середнього часу відновлення працездатності військової техніки зв'язку (ВТЗ) без збільшення економічних витрат, а лише за рахунок підвищення якості діагностичного забезпечення (ДЗ) ремонту і впорядкування діяльності екіпажа апаратної зв'язку або технічного забезпечення (АТЗ) в процесі групового пошуку дефектів і усунення викликаних ними несправностей.

Аналіз останніх досліджень в області технічного діагностування складних систем показав, що цією проблемою займаються багато провідних вчених, зокрема – Бідюк П.І., в статті «Формалізація методів побудови штучних імунних систем» піднімає проблематику цих питань, Жердєв М.К. в статті «Напрями розвитку систем контролю технічного стану і діагностування складних технічних систем» розглядає вбудовані системи технічного діагностування та інші, де вказується на необхідність вдосконалення і знаходження новітніх наукових рішень.

Постановка завдання. Таким чином існує необхідність розробки методики, яка дозволить оцінити показники якості діагностичного забезпечення засобів зв'язку ЗСУ за допомогою формалізації процесу кількісної оцінки показників якості діагностичного забезпечення ремонту військової техніки зв'язку на основі використання функціональних залежностей оцінюваних показників від керованих змінних.

Мета статті – розробка методики кількісної оцінки показників якості ДЗ з метою визначення можливості його реалізації в заданих умовах функціонування і оснащення ремонтного органу (РО) при відновленні працездатності ВТЗ в процесі поточного ремонту, а

також при усуненні аварійних і бойових пошкоджень з груповим зонним пошуком кратних дефектів.

Основний матеріал досліджень.

Сутність запропонованої методики полягає у використанні нових аналітичних виразів і формалізації процесу кількісної оцінки показників якості ДЗ ремонту ВТЗ.

Вихідні дані:

глибина пошуку дефектів (L);

алгоритм діагностування (середнє K, мінімальне $K_{\min}$, максимальне $K_{\max}$ число перевірок);

середній час виконання перевірки (t) і усунення несправності (t_y);

ймовірність правильної оцінки результату виконання перевірки (p);

припустимий час відновлення працездатності ($T_{вп}$).

Вихідні дані отримують з аналізу технічної документації ВТЗ і вимог до ремонтопридатності.

Обмеження на використання методики:

ремонт ВТЗ агрегатним методом;

при ремонті використовуються штатні засоби вимірювань (ЗВ) апаратної зв'язку і РО;

глибина пошуку дефектів до типового елементу заміни.

Допущення при використанні методики:

ВТЗ, що ремонтують, містить лише один дефект в зоні пошуку;

при діагностуванні в об'єкті нових дефектів не виникає;

при постановці помилкового діагнозу допускається не більш однієї помилкової оцінки результату виконання перевірки;

ймовірність помилкової оцінки результатів виконання перевірок по умовному алгоритму діагностування (УАД) однакова;

виявлення відмов елементів об'єкту рівноймовірно;

організаційні втрати часу не враховуються;

комплект ЗІП-0 укомплектований повністю;

використовувані ЗВ завідомо справні;

кваліфікація ремонтників відповідає штатному розкладу РО.

Обмеження і допущення відповідають умовам відновлення працездатності ВТЗ в АТЗ або на пункті технічного обслуговування і ремонту (ПТОР) [1, 2].

У основу математичного апарату методики покладені методи теорії ймовірностей і теорії дискретного пошуку [1–7]. Використовувані аналітичні вирази за кількісною оцінкою характеристик ДЗ приведені в табл. 1, а укрупнений алгоритм реалізації методики приведений на рис 1, 2 де додатково прийняті наступні позначення:

g – ймовірність помилкової оцінки результату виконання перевірки ($g = 1 - p$);

P – ймовірність правильної постановки діагнозу;

ρ – математичне очікування відхилення діагнозу при одній помилці в оцінці результату виконання перевірки;

σ_ρ – середньоквадратичне відхилення значення ρ;

l – число дефектів, що виявляються після виконання мінімального числа перевірок;

$C(K) = 0{,}375\lfloor K \rfloor^4 - 3{,}25\lfloor K \rfloor^3 + 10{,}625\lfloor K \rfloor^2 - 14{,}5\lfloor K \rfloor + 6{,}75;$

$E(K) = 0{,}375\lceil K \rceil^4 - 3{,}25\lceil K \rceil^3 + 10{,}625\lceil K \rceil^2 - 14{,}5\lceil K \rceil + 6{,}75;$

$\lfloor K \rfloor$ – ціла частина числа K;

$\lceil K \rceil$ – округлення K у більшу сторону до цілого числа;

$\rho_{\max}$ – максимально можливе значення ρ;

$T_в$ – розрахункове значення середнього часу відновлення ВТЗ.

Таблиця 1

Кількісна оцінка ймовірнісних характеристик бінарних умовних алгоритмів пошуку дефектів

Форма алгоритму	K	P	ρ_{max}	ρ	σ_ρ
Досконала	$\log_2 L$	$p^к$	$gp^{к-1}(L-1)$	$0{,}5(L+K-1)\ gp^{к-1}$	$[0{,}375(к^4-8{,}7к^3+ +28{,}3к^2-38{,}7к+ +18]^{0{,}5}\ gp^{к-1}$
Мінімальні правосторонні	$\lceil к \rceil - l/L$		$(2^{\lceil к \rceil}-1)\ gp^{\lceil к \rceil-1}$ для $2^{\lceil к \rceil} \le L-l \le 2^{\lceil к \rceil}$ $(L-1)\ gp^{к-1}$ для $0<L-l<2^{\lfloor к \rfloor}$	$0{,}5[(2^{[к]}+ \text{ц}к\text{ц}_- - (2^{\lfloor к \rfloor}+1)l/L]\ p^{\lfloor к \rfloor-1}$	$[C(k)(L-l)]^{0{,}5}gp^{\lfloor к \rfloor-1}$ для $0 \le l \le 2^{\lfloor к \rfloor-1}$ $[E(к)(L+l)]^{0{,}5}gp^{[к]-1}$ для $2^{\lfloor к \rfloor-1} \le l \le 2^{\lceil к \rceil}$
Мінімальні симетричні			$gp^{к-1}(2^к-1)$		$\left[\frac{l \cdot C(к)/p+(L-l)\cdot E(к)}{L}\right]^{0{,}5} gp^{\lfloor к \rfloor}$
Максимальна	$\frac{(L-1)(L+2)}{2L}$		$0{,}5L(L-1)g$	$\frac{(L^2-1)g}{6}+\frac{p-(p-g)p^{L-2}}{L}$	–

При невиконанні умов $\rho_{max}<1,\ \rho<0{,}5$ або $T_в<T_{вп}$ доцільно підвищити значення p вибираючи ЗВ з кращими метрологічними характеристиками, понизити значення t, t_y підвищенням кваліфікації фахівців або вдосконаленням технологічного устаткування РО, поліпшити умови праці ремонтників або змінити форму УАД з розміщенням $L-l$ елементів в його центральній частині.

Розглянемо використання методики на прикладі розробки УАД мінімальної форми для діагностування сучасного супергетеродинного приймача з подвійним перетворенням частоти, функціональна схема якого приведена на рис 3, а діагностична модель у вигляді графа інформаційно-енергетичних зв'язків [6] – на рис 4.

Бінарний УАД, побудований по методиці [6] із застосуванням індексів передування методом половинного ділення, показаний на рис. 5 (варіант 1), а з врахуванням розміщення дефектів, що вимагають для виявлення виконання K_{max} перевірок, в центральній частині алгоритму – на рис. 6 (варіант 2). У обох випадках УАД з врахуванням справного стану об'єкту мають однакові значення традиційно оцінюваних показників ДЗ [1, 6]: $L=18;\ K=4{,}3;\ K_{min}=4;\ K_{max}=5;\ l=13.$

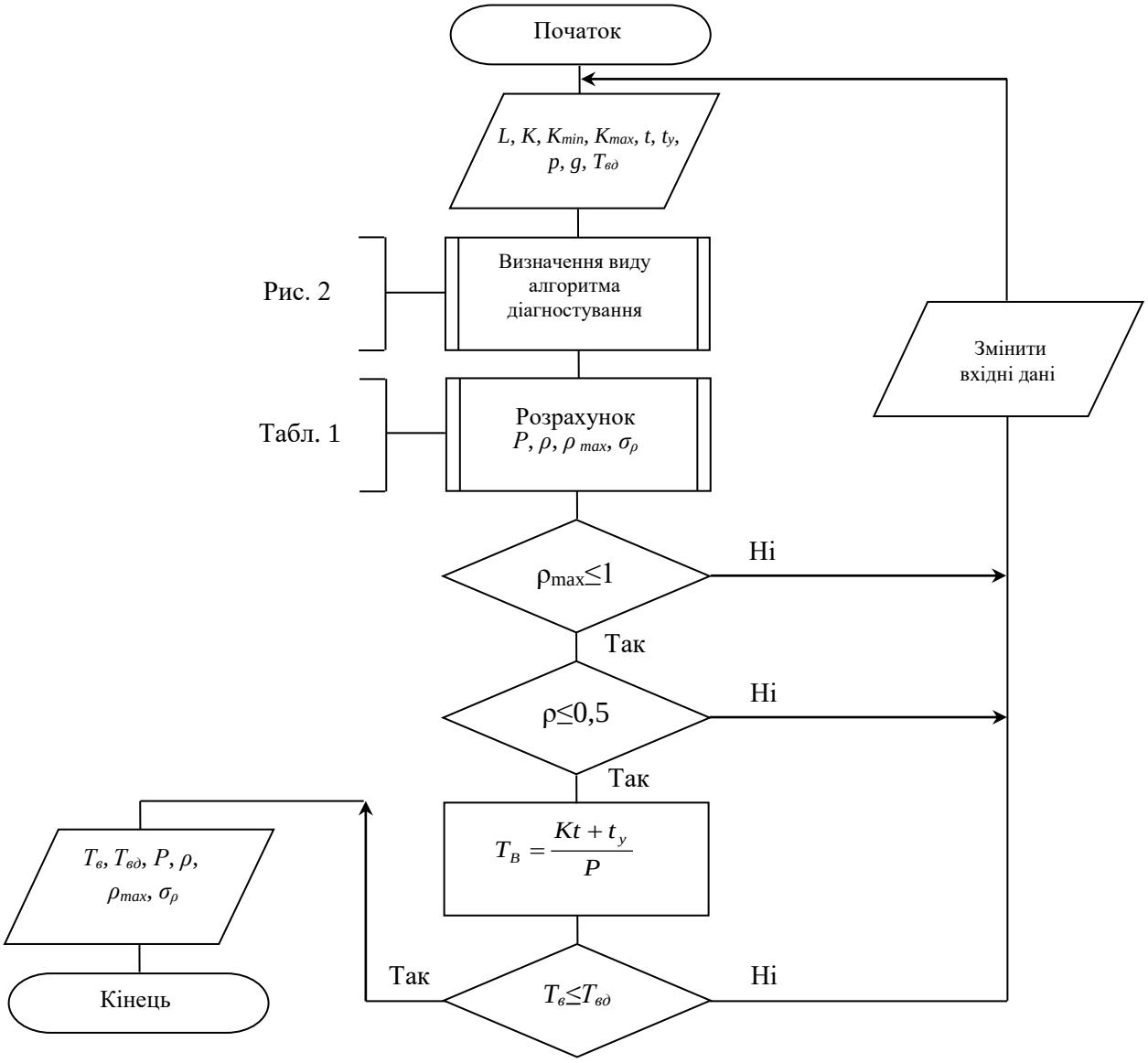


Рис. 1. Блок-схема укрупненого алгоритму кількісної оцінки показників якості діагностичного забезпечення ремонту військової техніки зв'язку

При наступних вихідних даних: $t = 3\ хв; t_y = 5\ хв;\ p = 0{,}99; T_{вп} = 20\ хв$ розрахункове значення середнього часу відновлення працездатності при поточному ремонті радіоприймача

$$T_в = \frac{4{,}3 \cdot 3 + 5}{0{,}99^{4{,}3}} = 19\ хв < T_{вп},$$

що досить.

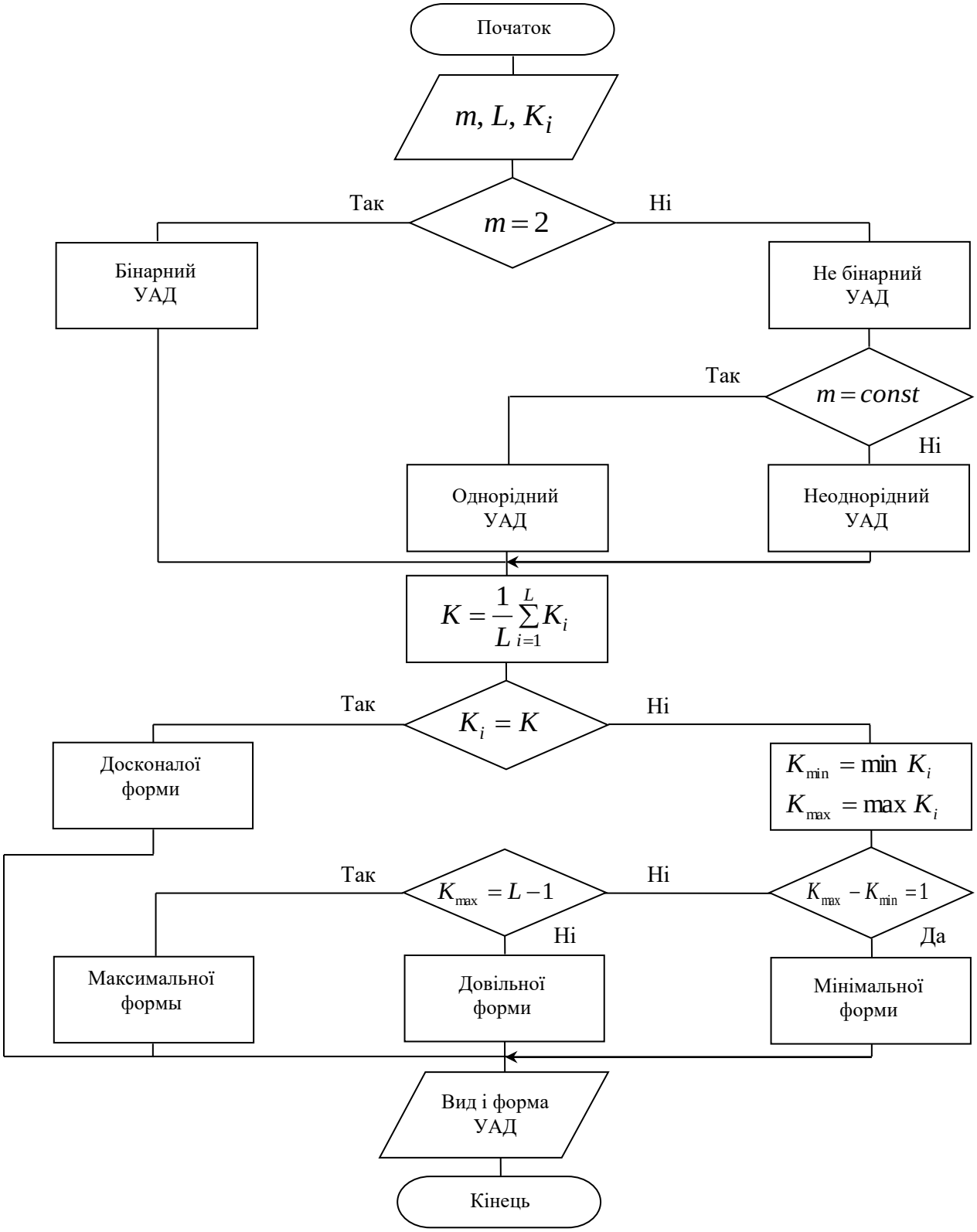


Рис. 2. Ідентифікація виду і форми алгоритму діагностування

Ймовірність постановки правильного діагнозу також однакова, але інші ймовірнісні характеристики істотно відрізняються (табл. 2) (результати прямих обчислень для $p = 0{,}99$).

При практично однакових значеннях інші показники для алгоритму рис. 6 значно понижені: σ_ρ на 40% и ρ_{max} на 25%.

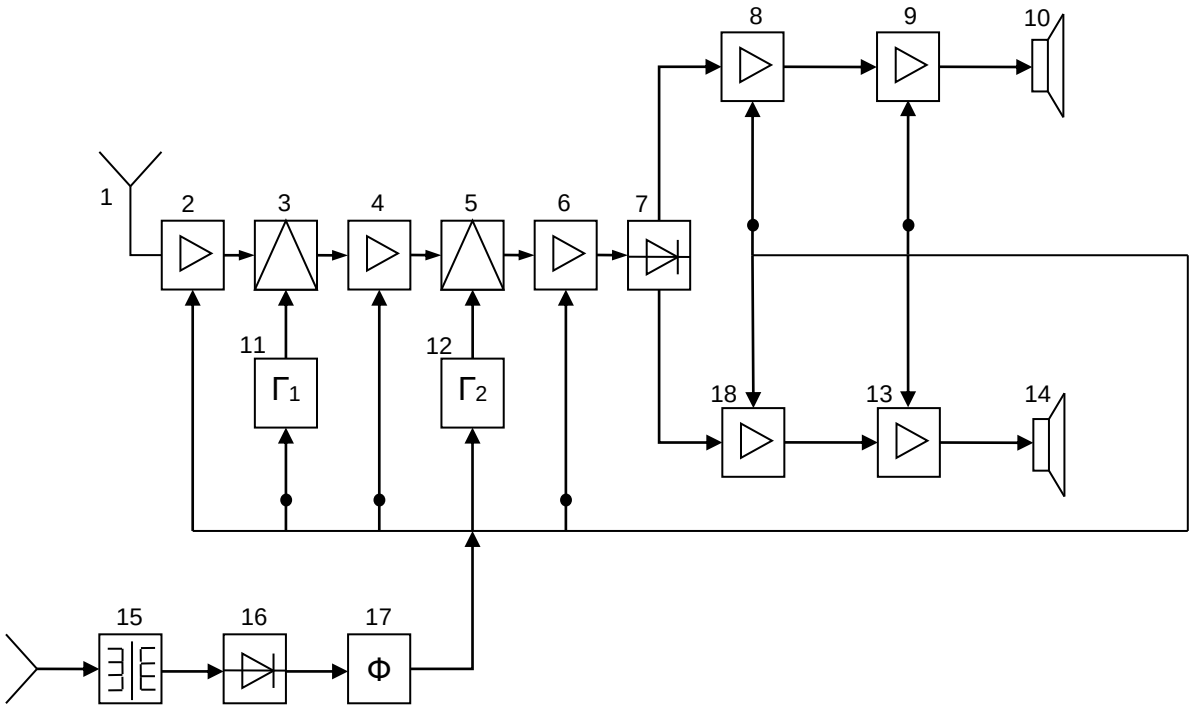


Рис. 3. Функціональна схема радіоприймача

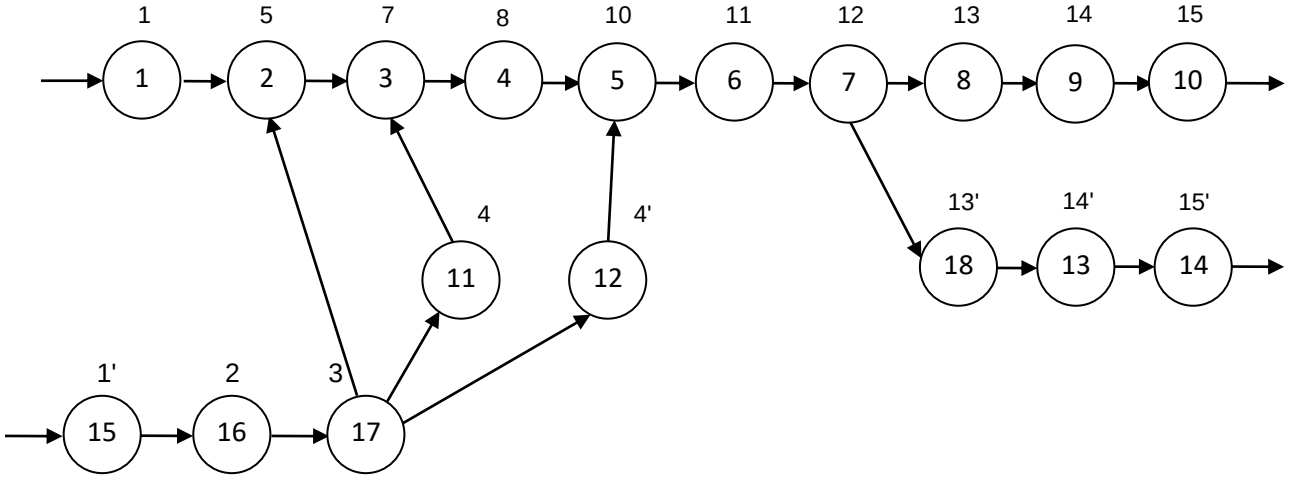


Рис. 4. Діагностична модель радіоприймача

Обчислення значення ρ приводить до результату 0,115 с $\delta_\rho = 1{,}7\%$, розрахункове значення $\rho_{max} = 0{,}164$ практично відповідає достеменному, оцінка σ_ρ рівна 0,027, що на $\delta_\rho = 11\%$ перевищує дійсне значення.

Таблиця 2

Ймовірнісні характеристики алгоритмів діагностування радіоприймача

Варіант алгоритму	ρ	D_ρ	σ_ρ	ρ_{max}
Рис. 5	0,1173	0,0017	0,0412	0,2208
Рис. 6	0,1170	0,0006	0,0249	0,1649

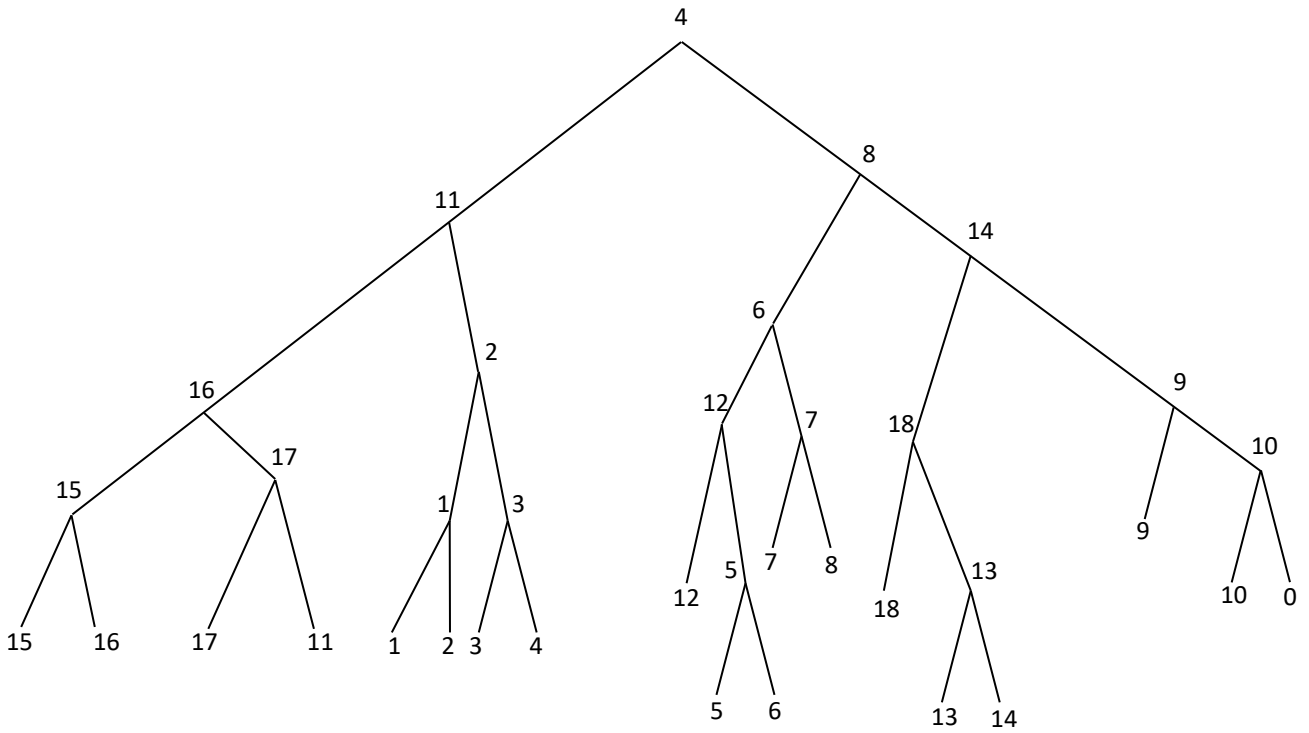


Рис. 5. Умовний алгоритм діагностування радіоприймача (варіант 1)

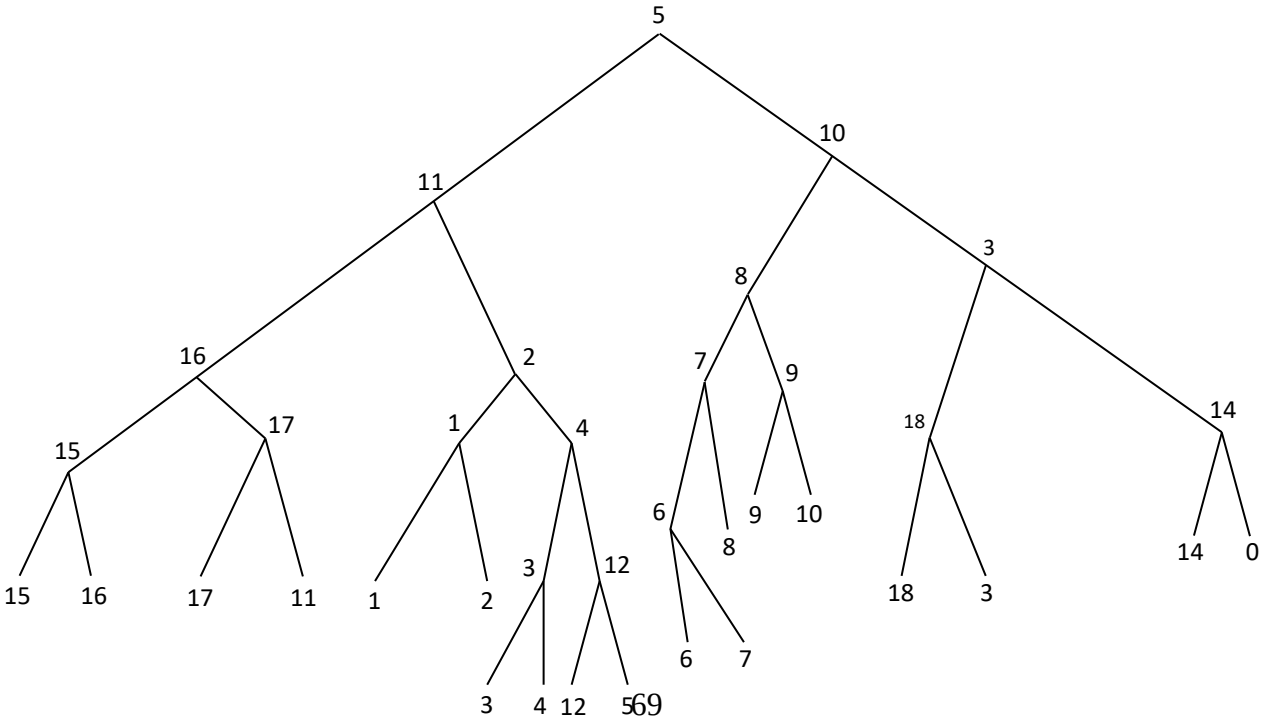


Рис. 6. Умовний алгоритм діагностування радіоприймача (варіант 2)

Висновки. Таким чином, наукова новизна методики полягає у формалізації процесу кількісної оцінки показників якості діагностичного забезпечення ремонту військової техніки зв'язку на основі використання вперше отриманих функціональних залежностей оцінюваних показників від керованих змінних (табл. 1).

Методика відрізняється від відомих [3, 6] порядком оцінки значень показників якості і використовуваним математичним апаратом.

Методика є основою аналітичних і алгоритмічних засобів розробки діагностичного забезпечення перспективних зразків військової техніки зв'язку.

ЛІТЕРАТУРА:

1. Сакович Л.Н. Определение численности специалистов при восстановлении работоспособности техники связи с аварийными повреждениями / Сакович Л.Н., Бобро Р.А. // Зв'язок, 2006. – №1. – С. 41-44.
2. Рижаков В.А. Кількісне оцінювання діагностичних помилок під час поточного ремонту техніки зв'язку / В.А. Рижаков, Л.М. Сакович // Зв'язок, 2005. – № 3. – С.45-50.
3. Розробка пропозицій щодо удосконалення системи технічного обслуговування і ремонту техніки зв'язку і АСУ: Звіт про НДР «Дністер» / в/ч А-0375. – К., 2000. – 151 с.
4. Сакович Л.Н. Количественная оценка вероятностных характеристик диагностических ошибок при ремонте техники связи / Л.Н. Сакович, В.П. Романенко // Зв'язок, 2011. – № 4. – С. 60-62.
5. Сакович Л.Н. Моделювання процесу групового пошуку дефектів під час ремонту техніки зв'язку / Л.Н. Сакович, В.П. Романенко // Зв'язок, 2011. – № 4. – С. 60-62.
6. Ксёнз С.П. Диагностика и ремонтопригодность радиоэлектронных средств / Ксёнз С.П. – М.: Радио и связь, 1989. – 248 с.
7. Вентцель Е.С. Теория вероятностей / Вентцель Е.С. – М.: Высш. шк, 2002. – 575 с.

REFERENCES:

1. Sakovich LN Definition multitude specialists at recovery rabotosposobnosty Technics connection with avaryynыmy INJURIOUS / LN Sakovich, beaver RA // Connect. - 2006. - №1. - P. 41-44.
2. Ryzhakov VA Quantitative Evaluation of diagnostic error during routine maintenance of communications technology / VA Ryzhakov, LM // How Sakovich. - 2005. - № 3. - S.45--50.
3. Developing proposals on improvement of the maintenance and repair of communications technology and ACS: research report "Dniester" / w / h A-0375. - K., 2000. - 151 p.
4. Sakovich LN Kolychestvennaya veroyatnostnыh performance evaluation of diagnostically oshybok connection with repairs technics / LN Sakovich, VP Romanenko // Communication. - 2011. - № 4. - P. 60--62.
5. Sakovich LN Simulation of a group of defects found during the repair of communications technology / LN Sakovich, VP Romanenko // Communication. - 2011. - № 4. - P. 60--62.
6. SP Ksënz Diagnosis and maintainability radyoэlektronnыh funds / SP Ksënz - M .: Radio and Communications, 1989. - 248 p.
7. Wentzel ES Probability Theory / ES Wentzel - M .: High society. HQ, 2002. - 575 p.

Рецензент: к.т.н., доц. Сакович Л.М., доцент кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського

к.т.н., доц. Радзивилов Г.Д., к.т.н Романенко В.П., Бригадир С.П.

ОЦЕНКА ПОКАЗАТЕЛЕЙ КАЧЕСТВА ДИАГНОСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ РЕМОНТА ВОЕННОЙ ТЕХНИКИ СВЯЗИ

В статье представлена методика оценки качества диагностического обеспечения ремонта техники связи, используемая в Вооруженных Силах Украины. Показано, что одной из основных целей решения данной задачи является повышение эффективности обслуживания технических систем, связанного с оптимизацией технологических процессов, их текущего ремонта и модернизации. Получены новые функциональные зависимости оцениваемых

показателей деятельности специалистов от управляемых переменных с учетом возможности возникновения диагностических ошибок, формализованный процесс количественной оценки показателей качества диагностического обеспечения ремонта военной техники связи. Также проведен анализ применения представленной методики на примере диагностики современного радиоприемника.

Ключевые слова: диагностика, техническое диагностирование, технические системы, ремонт.

Ph.D. Radzivslov G.D., Ph.D. Romanenko V.P., Brigader S.P.

EVALUATION OF A DIAGNOSTIC MAINTENANCE REPAIR EQUIPMENT MILITARY COMMUNICATIONS

The article presents a method of estimating a diagnostic software repair communications technology used in the Armed Forces of Ukraine. It is shown that a major objective of solving this problem is to improve the maintenance of technical systems associated with the optimization of processes, their ongoing maintenance and modernization. The resulting new functionality depending on the estimated performance of the professionals of controlled variables taking into account the possibility of diagnostic errors, formalized process quality indicators quantify the diagnostic software repair military equipment provider. Also analyzed the application presented methods for diagnosing example of modern radio.

Keywords: diagnostics, technical diagnostics, technical systems and repair.

УДК 621.391

д.т.н., с.н.с. **Рома О.М.** (ІСЗЗІ КПІ ім. Ігоря Сікорського)
Василенко С.В. (ІСЗЗІ КПІ ім. Ігоря Сікорського)

ВИБІР ПАРАМЕТРІВ АЛГОРИТМУ ВХОДЖЕННЯ В СИНХРОНІЗМ РАДІОЛІНІЇ УПРАВЛІННЯ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ З ПСЕВДОВИПАДКОВИМ ПЕРЕНАЛАШТУВАННЯМ РОБОЧОЇ ЧАСТОТИ

Результати оцінки локальних війн та збройних конфліктів свідчать про зростання ролі безпілотних літальних апаратів (БПЛА) у вирішенні завдань повітряної розвідки.

В умовах впливу противника спостерігаються різні умови придушення каналу зв'язку. Найсильнішому впливу завади піддається радіоелектронне обладнання літального апарату, оскільки він знаходиться на найменшій відстані від завадопостановника. Постає питання захисту радіолінії управління БПЛА.

У якості способу захисту пропонується використання широкосмугових сигналів з псевдовипадковим переналаштуванням робочої частоти (ППРЧ). Оскільки процес входження в синхронізм є первинним по відношенню до обміну інформації, то завадозахищеність радіолінії з ППРЧ характеризується завадозахищеністю алгоритму входження в синхронізм. Оптимальний вибір параметрів даного алгоритму дозволяє забезпечити баланс між завадозахищеністю системи синхронізації та якістю передачі корисної інформації.

Ключові слова: безпілотний літальний апарат (БПЛА), псевдовипадкове переналаштування робочої частоти (ППРЧ), алгоритм входження в синхронізм, завадозахищеність.

Вступ. У ході проведення антитерористичної операції Збройні Сили України переконалися у необхідності мати досконалу систему розвідки, яка повинна оперативно (в

реальному масштабі часу) забезпечувати підрозділи необхідною інформацією з максимальною її повнотою, точністю та достовірністю. Виконання даних функцій може бути покладено на безпілотні літальні апарати (БПЛА). Оскільки БПЛА змушені працювати в складній радіоелектронній обстановці, то постає питання створення завадозахищених каналів зв'язку. Розглядаючи вплив противника, найбільшому ураженню піддається ЛА, оскільки знаходиться найближче до засобів радіоелектронного придушення (РЕП) противника. Отже, виникає необхідність захисту радіолінії управління БПЛА. Одним з ефективних методів підвищення завадозахищеності таких радіоліній є використання широкосмугових систем радіозв'язку (СРЗ) з псевдовипадковим переналаштуванням робочої частоти (ППРЧ) [1].

Аналіз публікацій показав, що завадозахищеність радіолінії з ППРЧ на етапі пошуку складного сигналу характеризується завадозахищеністю алгоритму входження в синхронізм такої радіолінії [2].

Метою статті є визначення оптимальних параметрів алгоритму входження в синхронізм радіолінії управління БПЛА з ППРЧ за критерієм максимальної завадозахищеності.

Виклад основного матеріалу. Беручи за основу 5-канальну систему управління БПЛА, яка передбачає передачу команд в контурах управління рулями висоти, крену, тангажу, дроселя та гіроскопа, а також виходячи з необхідності передачі інформації з частотою, близькою до 15 Гц, мінімально необхідна пропускна спроможність радіоканалу повинна становити не менше 5058 біт/с [3]. Для забезпечення 2-3 кратного запасу з можливістю удосконалення моделі управління доцільно мати в розпорядженні більш високу швидкість. У такому разі доцільно орієнтуватися на найближчу стандартну бітову швидкість $R_\partial = 19,2$ кбіт/с, яка може бути реалізована на частотах, починаючи з УКХ діапазону.

Загальновідомим способом входження в синхронізм радіоліній з ППРЧ є спосіб з використанням незмінного блоку частот входження. Більшість з відомих алгоритмів схожі за своїм принципом дії:

синхронізація відбувається за рахунок збігу у часі неуражених частот прийому та передачі і подальшого правильного прийому синхрокадру цифрової інформації, що передається на частотах входження в синхронізм (чим більше таких збігів із максимально можливих на етапі входження відбудеться, і чим краща сигнально-завадова обстановка на частотах збігу, тим більша ймовірність входження в синхронізм);

для входження в синхронізм використовуються тільки частина робочих частот радіолінії;

використовується фіксований набір частот входження в синхронізм.

Відрізняються алгоритми один від одного своїми кількісними (кількість частот входження в синхронізм у одному підциклі входження, кількість підциклів у одному циклі входження, довжина синхрокадру і т.д.), та часовими (тривалість часу входження в синхронізм, випромінювання підциклу частот входження, переналаштування з однієї частоти на іншу і т.д.) характеристиками. Такі алгоритми можна назвати типовими і аналізувати далі саме типовий алгоритм входження в синхронізм, часова діаграма якого представлена на рис. 1 [2].

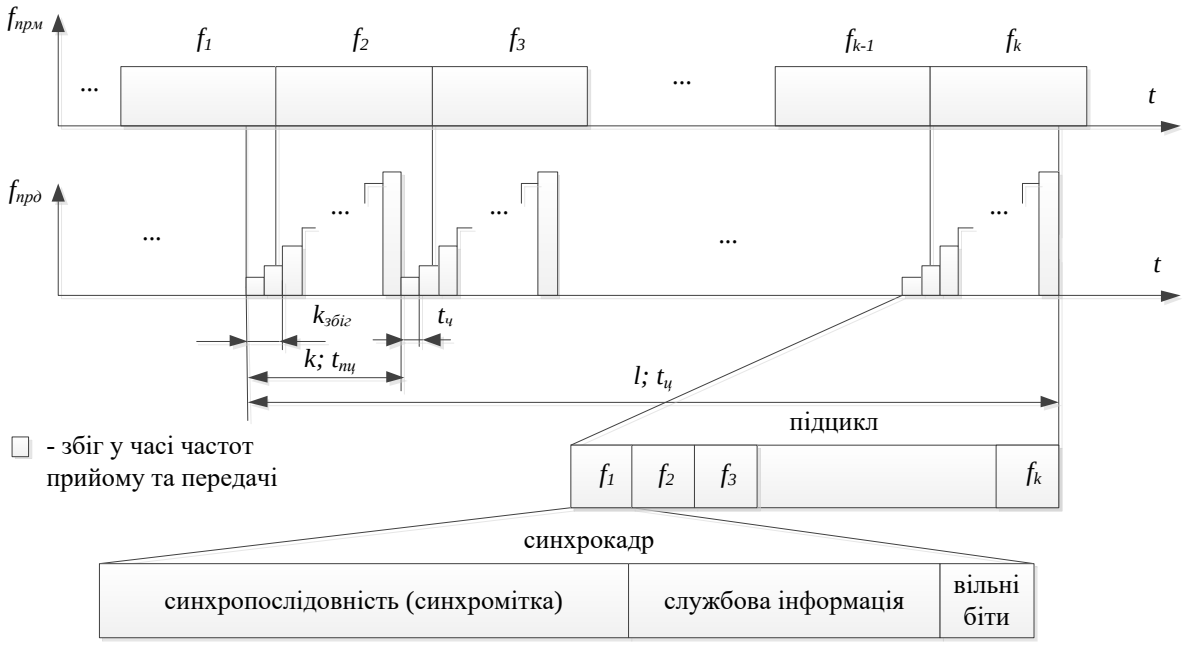


Рис. 1. Типовий алгоритм входження в синхронізм радіолінії зв'язку з ППРЧ

На ньому позначено:

k – кількість частот входження в синхронізм передавача у одному підциклі;

l – кількість підциклів входження в синхронізм передавача у одному циклі;

$k_{збіг}$ – кількість частот входження в синхронізм передавача із загальної кількості частот k, що збігаються з усіма частотами входження в синхронізм приймача за один цикл;

$t_{вх}$ – тривалість часу, відведеного для входження в синхронізм;

$t_ц$ – тривалість часу випромінювання однієї частоти передавачем з урахуванням часу переналаштування;

$t_{пц}$ – тривалість часу випромінювання передавачем одного підциклу частот входження в синхронізм;

$m_{ск}$ – довжина синхрокадру, біт;

$m_{см}$ – довжина синхромітки (синхропослідовності), біт;

$m_{сл.інф.}$ – довжина службової інформації, біт.

Обмеження до системи синхронізації. Головною вимогою до системи входження в синхронізм є необхідність гарантованого входження в синхронізм ($P_{вх} \geq 0,99$) за відведений час ($t_{вх}$). Для розрахунків використовується модель радіоканалу, максимально подібна до реальної, тобто коли $P_{ураж} \in [0;0,4]$, $P_{пом} \in [0;0,2]$. Для аналізу скористаємося методикою [4], де у якості показника оцінки завадозахищеності обрано ймовірність входження в синхронізм за один цикл $P(A)$.

На вибір кількості частот (k) впливає ймовірність ураження противником частот входження в синхронізм та тривалість перебування передавача в одній частотній позиції. Остання також визначає і припустиму кількість підциклів входження в синхронізм (l) виконуючи вимогу, що входження в синхронізм повинно відбутися за нормативно відведений час. Наприклад, якщо стоїть вимога входження в синхронізм за 1 с (1000 мс), то при перебуванні передавача в одній частотній позиції протягом 10 мс ми можемо реалізувати $l = 1000/10k$ підциклів.

Обмежуючись вимогами поставленими до системи синхронізації та швидкості передачі інформації в УКХ діапазоні, обираємо $k=10$, $l=6$. Кількість сумісних комбінацій частот та підциклів у цьому випадку складає 60, що потребує для кодування комбінацій 6 біт.

Відомо, що за умови можливості технічної реалізації час переналаштування передавача з ППРЧ в УКХ діапазоні має порядок одиниць мілісекунд. Для нашого випадку час стрибка передавача при входженні в синхронізм обираємо з 10-кратним запасом, тобто 10 мс. Оскільки пауза між випромінюванням на сусідніх частотах складає близько 10% від часу одноразового використання частоти, то приймемо $t_{ї\ ðë.ï\ ðä.}=1$ мс, а $t_ц=9$ мс. Тривалість одного підциклу входження для даного випадку буде складати:

$$t_{ï\ ö}=k\left(t_{\div}+t_{ï\ ðë.ï\ ðä.}\right)=100 \text{ мс.} \quad (1)$$

Загальна тривалість циклу входження в синхронізм буде дорівнювати:

$$t_ц=lt_{пц}=600 \text{ мс.} \quad (2)$$

Швидкість стрибків передавача на етапі входження в синхронізм для даного випадку становить:

$$N=1/\left(t_ц+t_{прл.прд.}\right)=100 \text{ стр/с.} \quad (3)$$

При цьому на кожній з частот входження в синхронізм передавач здійснює передачу спеціальних кодових комбінацій (синхрокадрів) довжиною до:

$$m_{ск}=\left[R_д\, t_ц\right]=172 \text{ біт,} \quad (4)$$

де $[\ ]$ – ціла частина.

Кожен синхрокадр (рис. 1) складається з синхромітки, яка містить інформацію про номер частоти та номер підциклу входження, та блоку службової інформації (за необхідністю).

Існує багато методів захисту інформації, що передається у широкосмугових СРЗ, від помилок. Дані методи відрізняються один від одного способами реалізації, часовими параметрами та завадозахищеністю. Деякі методи базуються на використанні бінарних псевдовипадкових послідовностей (ПВП), наприклад послідовності Голда, Касамі, М-послідовності, бент-функцій та інші.

У статті для кодування вмісту синхромітки пропонується використання кодів Касамі, які характеризуються досить низьким рівнем бічних пелюсток автокореляційної функції. Дані коди реалізуються за допомогою генераторів М-послідовностей з різними зворотними зв'язками. Довжина такої М-послідовності визначається ємністю n регістру зсуву (у бітах) і складає $N=2^n-1$ біт. Ємність регістру зсуву визначає кількість біт, які можуть бути закодовані однією Касамі.

При прийомі синхросигналу приймач спочатку оцінює синхромітку і за отриманими даними (номер частоти, номер підциклу в циклі) визначає момент часу передачі інформації на частотах входження. Після цього відбувається синхронний запуск генераторів ПВП обох абонентів за робочою програмою з циклом формування кодів ПВП, що дорівнює часу знаходження передавача в одній частотній позиції.

У блоці службової інформації можуть передаватися дані про режим роботи радіостанції, номер абонента, що викликається (у випадку радіомережі), швидкість кодування даних (оскільки канали передачі даних мають різну якість) і т.д. Проблема забезпечення завадозахищеності та завадостійкості цих даних має дуже важливе значення. Це пояснюється тим, що при передачі даних навіть одна помилка (спотворення одного біта) може серйозно вплинути на правильність прийому повідомлення.

Довжина синхромітки типового алгоритму входження в синхронізм СРЗ з ППРЧ УКХ діапазону становить $m_{см} = 63$ біт (тобто $N = m_{см} = 63$біт). Об'єм (кількість) таких вибірок з М-послідовності дорівнює $V = 2^{n/2} = 8$. Кількість інформаційних біт, що будуть використані для передачі корисної інформації буде складати $C = \log_2 8 = 3$ біт. Оскільки кількість комбінацій, що треба закодувати складає 60, то виникає необхідність у включенні до синхромітки ще однієї послідовності Касамі ($63 \times 2 = 126$ біт). У цьому випадку кількість можливих комбінацій збільшується до $8 \times 8 = 64$, що буде достатньо для передачі 6 біт коду ($2^6 = 64 > 6 \times 10 = 60$).

Як відомо, при передачі сигнал піддається впливу завад, що призводить до ураження та втрати деякої кількості інформаційних біт синхромітки. При цьому допускається прийняти невірно (втратити) певну кількість біт ($m_{пор}$). Величина $m_{пор}$ обмежується вимогами до ймовірності входження в синхронізм та якості каналу зв'язку (рис. 2).

З рис. 2 видно, що для забезпечення поставлених вимог щодо входження в синхронізм максимально допустиме значення біт, що можуть бути прийняті невірно становить $m_{пор} = 21$ біт. При подальшому збільшенні значення $m_{пор}$ ймовірність $P(A)$ зменшується, що є не допустимим для даного каналу зв'язку.

Як було зазначено вище, до складу синхрокадру, крім синхромітки, може входити блок службової інформації. У даному блоці може мітитися інформація про режим роботи радіостанцій, швидкість кодування та інші службові дані.

Як відомо, для вдалого прийому синхрокадру необхідно, щоб завадозахищеність вищенаведених компонентів синхромітки по можливості була однаковою (або близькою до однакової). У зв'язку з цим виникає необхідність кодування блоку службової інформації. У даній статті для кодування службової інформації пропонується використання N-кратного мажоритарного коду, що є найбільш зручним при використанні в каналі з ймовірністю помилкового прийому елемента сигналу $P_{пом} > 0,065$ [5]. Суть даного кодування полягає в передачі повідомлення з обмеженою довжиною m-разів. Передані повідомлення зберігаються в пам'яті приймача, де здійснюється їх порозрядне порівняння. Висновок про правильність прийому інформації виноситься за збігом більшості прийнятих повідомлень. Вибір кратності кодування залежить від обсягу інформації, що буде передаватися у блоці службової інформації та вимог до радіолінії (для нашого випадку $m_{сл.інф.} = m_{ск} - 2m_{см} = 46$ біт).

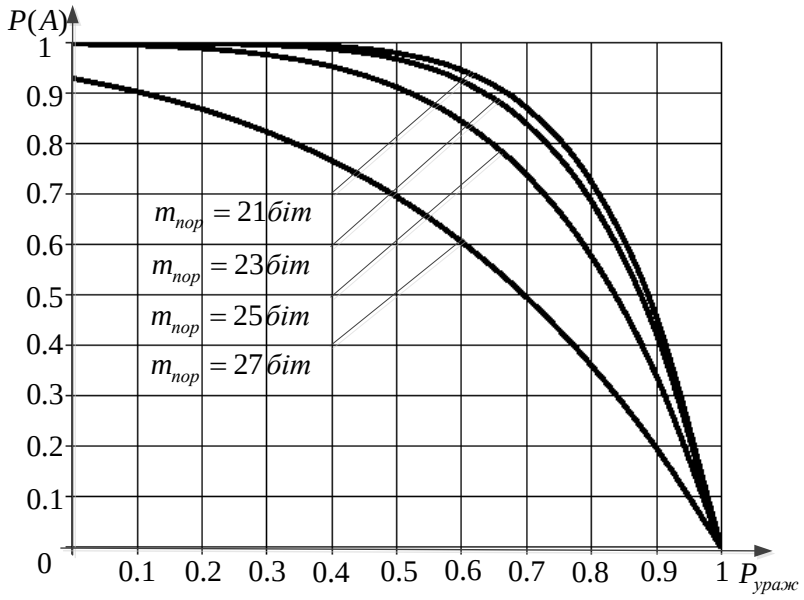


Рис. 2. Графіки залежності $P(A)$ від $P_{ураж}$ для різних значень $m_{пор}$

На рис. 3 представлений графік залежності $P(A)$ від $P_{ураж}$ для різних значень кратності мажоритарного кодування m.

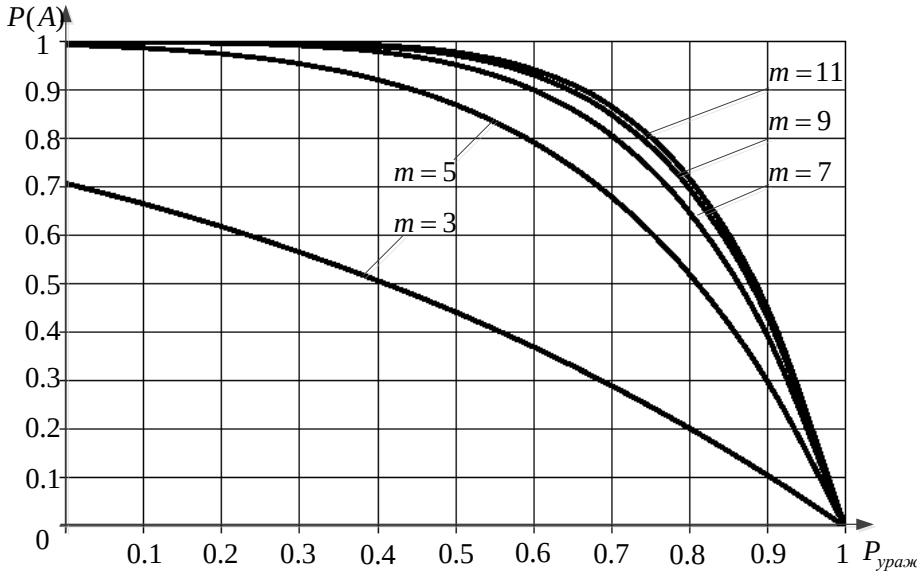


Рис.3. Графіки залежності $P(A)$ від $P_{ураж}$ для різних значень m

З графіка видно, що для того, щоб ймовірність прийому службової інформації приблизно відповідала ймовірності прийому синхромітки необхідно забезпечити не менше як семикратне мажоритарне кодування.

Висновки. У статті проведено вибір оптимальних параметрів алгоритму входження в синхронізм радіолінії управління БПЛА з ППРЧ за критерієм максимальної завадозахищеності в умовах впливу навмисних завад. Наведені параметри дозволяють

забезпечити синхронізацію УКХ-радіолінії управління БПЛА в межах нормативно відведеного часу з ймовірністю близькою до 1. Дане положення зберігається до тих пір, поки значення ймовірності ураження частоти входження в синхронізм буде близьке до прийнятого в методиці [4].

Нажаль в сучасних умовах досить легко виявити постійні частоти входження в синхронізм і організувати на цих частотах навмисну постійну заваду. Тому для подальших досліджень актуальним є напрямок розробки алгоритмів формування змінних наборів частот входження, наприклад за принципом плинної зміни.

ЛІТЕРАТУРА:

1. Борисов В.И., Зинчук В.М., Лимарев А.Е., Мухин Н.П., Шестопалов В.И. Помехозащищенность систем радиосвязи с расширением спектра методом псевдослучайной перестройки рабочей частоты. – М.: Радио и связь, 2000. –384 с.
2. Міщенко В.Г., Єрохін В.Ф. Аналіз завадозахищеності типових алгоритмів входження в синхронізм радіолінії з псевдовипадковим перелаштуванням радіочастоти // Матеріали III Міжнародної науково-технічної конференції "АВІА-2001", 24-26 квітня 2001р., м.Київ // Компакт-диск "III Міжнародна науково-технічна конференція АВІА-2001". – К.: КМУЦА. – 2001.
3. Рома О.М., Василенко С.В. Основи побудови завадозахищеної радіолінії управління безпілотним літальним апаратом // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2015. – Вип. №49. – С. 97-104.
4. Міщенко В.Г., Єрохін В.Ф. Методика оцінки завадозахищеності алгоритмів входження в синхронізм радіолінії з псевдовипадковим перелаштуванням радіочастоти/ Захист інформації, 2001. – № 2. – С. 32-59.
5. Золотарёв В.В. Простые методы исправления ошибок в каналах с большим уровнем шума // Радиотехника, 1991. – №10. – С.79-82.

REFERENCES:

1. Borisov, V.I., Zinchuk, V.M., Limarev, A.E., Mukhin, N.P., Shestopalov, V.I. (2000). Interference immunity of radio systems with spread spectrum by frequency hopping spread spectrum. Moscow: Radio i svyaz' [Radio and Communications], p. 384 (In Russian).
2. Mishhenko, V.Gh., Jerokhin, V.F. (2001). Analysis noise immunity algorithm acquisition radio lines with the frequency hopping spread spectrum. Materialy III Mizhnarodnoji naukovo-tekhnichnoji konferenciji "AVIA-2001", 24-26 kvitnja 2001, Kiev. CD "III Mizhnarodna naukovo-tekhnichna konferencija AVIA-2001", Kiev.: KMUCA.
3. Roma, O.M., Vasylenko, S.V. (2015). Fundamentals of noise immunity radio control unmanned aerial vehicle. Kiev: Zbirnyk naukovykh pracj Vijsjkovogho instytutu Kyjivsjkogho nacionaljnogho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, №49. pp. 97-104.
4. Mishhenko, V.Gh., Jerokhin, V.F. (2001). Method of estimation algorithms by noise immunity radio lines with the frequency hopping spread spectrum. Zakhyst informaciji [Information Security], № 2, pp. 32-59.
5. Zolotarev V.V. (1991). Prostye metody ispravleniya oshibok v kanalakh c bol'shim urovnem shuma. Radiotekhnika [Radio Engineering], №10, pp.79-82.

Рецензент: д.т.н., проф. Сбітнєв А.І., провідний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

д.т.н., с.н.с. Рома А.Н., Василенко С.В.

ВЫБОР ПАРАМЕТРОВ АЛГОРИТМА ВХОЖДЕНИЯ В СИНХРОНИЗМ РАДИОЛИНИИ УПРАВЛЕНИЕ БПЛА С ППРЧ

Результаты оценки локальных войн и вооруженных конфликтов свидетельствуют о росте роли беспилотных летательных аппаратов (БПЛА) в решении задач воздушной разведки.

Рассматривая влияние злоумышленника, мы сталкиваемся с различными условиями подавления канала связи. Сильнейшему влиянию помехи подвергается радиоэлектронное

оборудование летательного аппарата, поскольку он находится на наименьшем расстоянии от помехопостановщика. Следовательно, возникает вопрос защиты радиолинии управления БПЛА.

В качестве способа защиты предлагается использование широкополосных сигналов с псевдослучайной перенастройкой рабочей частоты (ППРЧ). Поскольку процесс вхождения в синхронизм является первичным по отношению к обмену информации, то помехозащищенность радиолинии с ППРЧ характеризуется помехозащищенностью алгоритма вхождения в синхронизм. Оптимальный выбор параметров данного алгоритма позволяет обеспечить баланс между помехозащищенностью системы синхронизации и качеством передачи полезной информации.

Ключевые слова: беспилотный летательный аппарат (БПЛА), псевдослучайная перестройка рабочей частоты (ППРЧ), алгоритм вхождения в синхронизм, помехозащищенность.

Dr. Roma A.N., Vasylenko S.V.

SETTING ALGORITHM ACQUISITION ENTRY INTO RADIOLINE CONTROL UAV WITH FHSS

The evaluation of local wars and armed conflicts indicate an increase in the role of unmanned aerial vehicles (UAVs) in the solution of aerial reconnaissance tasks.

Considering the impact of the attacker, we are confronted with different channel conditions due suppression. Radioelectronic equipment aircraft is exposed to the strongest influence of noise, because it is the closest to the jammer. In such way the issue of UAV radio control protection becomes topical.

In this article using of broadband signals with frequency hopping spread spectrum (FHSS) is suggested as the security method. Since the process of acquisition is primary in relation to the exchange of information, immunity from FHSS radio is characterized by noise immunity algorithm acquisition. The optimal choice of the parameters of the algorithm allows to provide the balance between noise immunity systems of synchronization and the quality of the useful information transmission.

Keywords: unmanned aerial vehicle (UAV), frequency hopping spread spectrum (FHSS), acquisition algorithm, noise immunity.

УДК 004.942

к.т.н., доц. **Чешун В.М.** (ХмНУ)
д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
Прокопчук С.О. (ХмНУ)
к.т.н., с.н.с. **Охрамович М.М.** (ВІКНУ)
Шевченко В.В. (ВІКНУ)

МОДЕЛІ ДИНАМІЧНИХ НЕСПРАВНОСТЕЙ ДИСКРЕТНИХ ІНТЕГРАЛЬНИХ КОМПОНЕНТІВ КОМПЛЕМЕНТАРНОЇ ЛОГІКИ

Проведений аналіз тенденцій розвитку цифрових інтегральних компонентів та засобів їх діагностування показує, що тривалий час основна увага приділялася технологіям на біполярних транзисторах і найбільш актуальною вважалася транзисторно-транзисторна логіка з діодами Шотткі, а елементи комплементарної логіки були на другорядних позиціях. В роботі розглянуто умови актуалізації комплементарної технології виготовлення дискретних інтегральних компонентів та наслідки зміни тенденцій для технічної діагностики цифрових пристроїв і систем, вказані причини збільшення питомої ваги несправностей динамічного типу, надано класифікацію зазначених несправностей компонентів комплементарної логіки та опис характерних ознак їх прояву, запропоновано математичні моделі типових несправностей динамічного типу. Математичні моделі базуються на урахуванні чотирьох можливих станів контрольованих сигналів (логічний 0 і 1, Z-стан і невизначений стан) та часових параметрів їх зміни, призначені для застосування при формуванні множини та моделей несправних станів комплементарних компонентів і побудованих з їх використанням цифрових об'єктів діагностування, розробки методів та алгоритмів діагностування, визначення вимог до технічних засобів діагностування.

Ключові слова: тестова діагностика, цифрові пристрої, комплементарна логіка, математична модель.

Вступ. Поява базових технологій виготовлення дискретних інтегральних компонентів датується відносно невеликим періодом часу з 60-х і до початку 70-х років минулого сторіччя, але історія розвитку і застосування зазначених технологій суттєво відрізняється, що мало відповідний вплив на розвиток методів та засобів діагностування зазначених компонентів цифрової електроніки та побудованих на них пристроїв і систем.

Елементи резисторно-транзисторної (Resistor-Transistor Logic - RTL) і діодно-транзисторної логіки (Diode-Transistor Logic – DTL) досить швидко втратили свої позиції в конкуренції з транзисторно-транзисторною логікою (Transistor-Transistor Logic - TTL), яка, в свою чергу, вже на початку 70-х років почала поступатися новій технології - транзисторно-транзисторній логіці з діодами Шотткі (Schottky TTL - TTLS), що іноді розглядається як діодно-транзисторна логіка з діодами Шотткі.

Елементи емітерно-зв'язаної логіки (Emitter Coupled Logic - ECL), незважаючи на високі показники швидкодії вже в перших зразках, не знайшли широкого самостійного застосування через суттєві недоліки (високе енергоспоживання, потреба використання двох джерел живлення для вхідного та вихідного каскадів окремо тощо).

Розроблена на початку 70-х років інтегрально-інжекційна логіка (Integrated Injection Logic - IIL, I^2L, I2L) відрізнялася економічністю як в енергоспоживанні, так і у вартості виготовлення, але також не набула розповсюдження через малу швидкодію порівняно з елементами TTLS.

Спільною рисою всіх перелічених технологій є їх схемна реалізація на біполярних транзисторах.

Одночасно з технологіями виготовлення дискретних інтегральних компонентів на біполярних транзисторах створюються і розвиваються аналогічні технології на уніполярних транзисторах.

Виготовлені на основі структур метал-оксид-напівпровідник (Metal-Oxide-Semiconductor - MOS) транзистори p-типу і n-типу дають основу двом технологіям

виготовлення мікросхем - p-MOS і n-MOS, а також комбінованій комплементарній технології (Complementary MOS - CMOS). Хоча швидкодія виготовлених за цими технологіями інтегральних компонентів була невисокою, значно менший розмір і спрощена технологія виготовлення уніполярних транзисторів надавали їм переваги і дозволили розробити та реалізувати із їх застосуванням перші зразки мікропроцесорів на одному кристалі: p-MOS процесор Intel8008 та n-MOS процесори Intel8080 і Motorola 6800. При виборі технології виготовлення перших однокристальних мікропроцесорів нищівної критики від фірми Intel зазнає технологія CMOS як така, що відрізняється від p-MOS і n-MOS складнішою технологією виготовлення через потребу формування на одному кристалі транзисторів p-типу і n-типу та забезпечує менший ступінь інтеграції елементів. Лише завдяки надзвичайно малому енергоспоживанню, CMOS-логіка надовго стала лідером застосувань в цифровій електроніці з автономним живленням (калькулятори, годинники тощо).

Наявні обмеження в швидкодії дискретних інтегральних компонентів p-MOS, n-MOS і CMOS протягом тривалого часу зумовлювали їх ігнорування як можливих конкурентів TTLS-елементам. Ситуація починає докорінно змінюватися на межі 1990 року, коли, з підвищенням ступеня інтеграції мікросхем, гостро постала проблема розсіювання енергії на елементах TTLS. Оскільки RTL, DTL і TTL не могли конкурувати з TTLS і були визнані застарілими, а ECL та IIL, через специфічні недоліки, були непридатними для масового застосування, з 90-років спостерігається тенденція до конкуренції і намагань вдосконалення двох технологій виготовлення цифрових елементів:

- транзисторно-транзисторної з діодами Шотткі на зменшення енергоспоживання;
- комплементарної логіки на збільшення швидкодії.

Якщо суттєвих успіхів в зменшенні енергоспоживання TTLS без втрат в швидкодії досягти не вдалося, то прогрес CMOS-логіки був разючим - вже з появою надшвидкісних серій мікросхем CMOS-логіки 74VHC і 74VHCT швидкодія TTL-елементів стає досяжною для комплементарної логіки, а після випуску супер-надшвидкісної серії 74G робочі частоти переходять межі гігагерц і стають недосяжними для TTL-елементів.

Таким чином, наприкінці 20-го сторіччя відбувається перелам в поглядах на перспективи застосування технологій на біполярних і польових транзисторах. Визнана раніше основною технологія TTLS стрімко втрачає позиції, а другорядна до цього технологія CMOS стає основною. Це зумовило в 2009р. відмову фірми Texas Instruments від продовження випуску серій мікросхем з модифікаціями TTL-логіки та TTLS-логіки 54/74 і остаточний вихід в лідери комплементарних технологій.

Такий різкий перехід став суттєвим ударом по технічній діагностиці дискретних компонентів, пристроїв та систем.

З урахуванням описаних пріоритетів, основна увага в 20-му сторіччі приділялася методам діагностики цифрових схем на біполярних транзисторах, які, через малі робочі частоти комплементарних схем, були досить ефективними і для тестування останніх. Специфічних методів і засобів для діагностування комплементарних схем практично не розроблялося.

Стрімкий стрибок на декілька порядків в швидкодії комплементарних цифрових компонентів з декількох мегагерц до гігагерц докорінно змінив ситуацію – в побудованих за комплементарною технологією інтегральних компонентах на перші позиції вийшли несправності, зумовлені специфічними властивостями польових транзисторів. Оскільки розроблені у великій кількості методи діагностування елементів на біполярних транзисторах були малоефективними щодо комплементарних технологій, технічна діагностика виявилась не готовою до подібної революції.

Постановка задачі. Стрімке зростання швидкодії дискретних інтегральних компонентів комплементарної логіки (ДІККЛ) на структурах метал-оксид-напівпровідник та метал-діелектрик-напівпровідник призвело до загострення проблем виявлення і локалізації несправностей, характерних для цього класу об’єктів діагностування (ОД) і високочастотних

режимів їх роботи.

Переведення ДІККЛ на високі робочі частоти зумовило збільшення питомої ваги несправностей динамічного типу[1]. Аналіз передумов виникнення і характерних особливостей прояву зазначених несправностей свідчить, що одним із основних факторів є значно більший вплив паразитної ємності ДІККЛ[2], ніж у елементів на біполярних транзисторах, що і зумовлювало протягом багатьох років обмеження швидкодії елементів на уніполярних транзисторах. Хоча робочі частоти ДІККЛ вдалося багатократно підвищити, від паразитної ємності уніполярних транзисторів і її впливу на роботу цифрових схем позбавитися не вдалося. По мірі старіння або при тимчасових переходах ДІККЛ в нестандартні режими роботи вплив паразитної ємності може ставати вирішальним і призводити до збоїв в їх роботі[3,4]. Окрім впливу паразитної ємності збої можуть бути зумовлені проявом інших несправностей динамічного типу (затримками, гонками тощо).

Складність виявлення несправностей динамічного типу визначається нестабільністю їх прояву і виникнення зумовлених цим збоїв в роботі пристроїв і систем з ДІККЛ. Для збільшення ймовірності виявлення несправностей динамічного типу пристроїв і систем з ДІККЛ повинні бути виконані умови ефективної реалізації діагностичних випробувань [1,5]:

- тестові випробування ОД мають проводитися на максимальних робочих частотах;
- наявні математичні моделі повинні адекватно відображувати справний і несправні стани ОД, а також особливості прояву несправностей динамічного типу в ході проведення тестових випробувань;
- використовувані технічні засоби діагностування повинні відповідати вимогам реалізовуваних методів і алгоритмів діагностування.

Першочерговою задачею для ефективної реалізації діагностичних випробувань пристроїв і систем з ДІККЛ є визначення класів і моделей можливих несправностей досліджуваного типу ОД.

Основна частина. Для опису цифрових пристроїв з ДІККЛ запропоновано різноманітні моделі, а саме [1, 6-9]: вентильні, транзисторні, струмові, нейронні, мережі Петрі, перемикальні.

Наявність згаданої сукупності моделей свідчить як про наявні проблеми моделювання цих пристроїв як ОД, так і про актуальність вибору адекватної поставленим задачам математичної моделі і відсутність єдиного універсального варіанту.

Першочергово відзначимо, що модель має бути орієнтована на діагностування цифрових пристроїв ДІККЛ з локалізацією несправностей динамічного типу, що є некласичними для інших технологій виготовлення мікросхем. Некласичні несправності цифрових пристроїв з ДІККЛ можуть бути адекватно відображені тільки на транзисторному рівні [6]. В [1, 6] доводиться, що найбільш адекватними для відображення несправностей динамічного типу ДІККЛ є перемикальні моделі.

Будь-яка модель цифрового пристрою як ОД першочергово базується на визначенні різновидів сигналів, що мають враховуватись. Традиційні варіанти з урахуванням лише двох булевих значень контрольованого сигналу 0 та 1 не можуть бути достатніми хоча б через неможливість ідентифікації стану високого імпедансу (Z-стану). Крім того, слід враховувати, що несправності динамічного типу частіше проявляються не зміною булевих значень контрольованих сигналів, а затягуванням та спотворенням процесів зміни чи утримання вказаних значень. Через це для відображення ознак прояву несправностей динамічного типу важливо мати засоби опису перехідних процесів затягування та спотворення зміни та утримання значень контрольованих сигналів. Для запобігання надмірної деталізації опису перехідних процесів, що зумовлює ускладнення моделі і інструментарію для роботи з нею, а також призводить до значного підвищення вимог до використовуваних засобів діагностування, введемо поняття невизначеного стану контрольованого сигналу, рівень напруги якого не відповідає жодному з характерних значень для ДІККЛ відповідного класу.

Виходячи з цього, опис сигналів ДІККЛ як ОД задамо у вигляді мінімальної множини значень сигналів V:

$$V = \{\ 0,\ 1,\ Z,\ U\ \}, \qquad (1)$$

де 0 - логічний нуль, який описує сигнали, що належать області низьких значень напруги; 1 - логічна одиниця, яка описує сигнали, що належать області високих значень напруги; Z - значення, яке відповідає стану виходу ДІККЛ, в якому він має високий вихідний опір; U - невизначене значення, яке належить розподільчій області між областями низьких і високих значень напруги та відображує перехідні процеси при зміні рівнів напруги булевих значень контрольованого сигналу.

Оберемо за прототип математичні моделі КМДН-схем [1, 6] як ОД та уточнимо їх з урахуванням обраної системи кодування можливих значень контрольованих сигналів. При цьому будемо спиратись на класифікацію несправностей динамічного типу ДІККЛ (рис. 1).

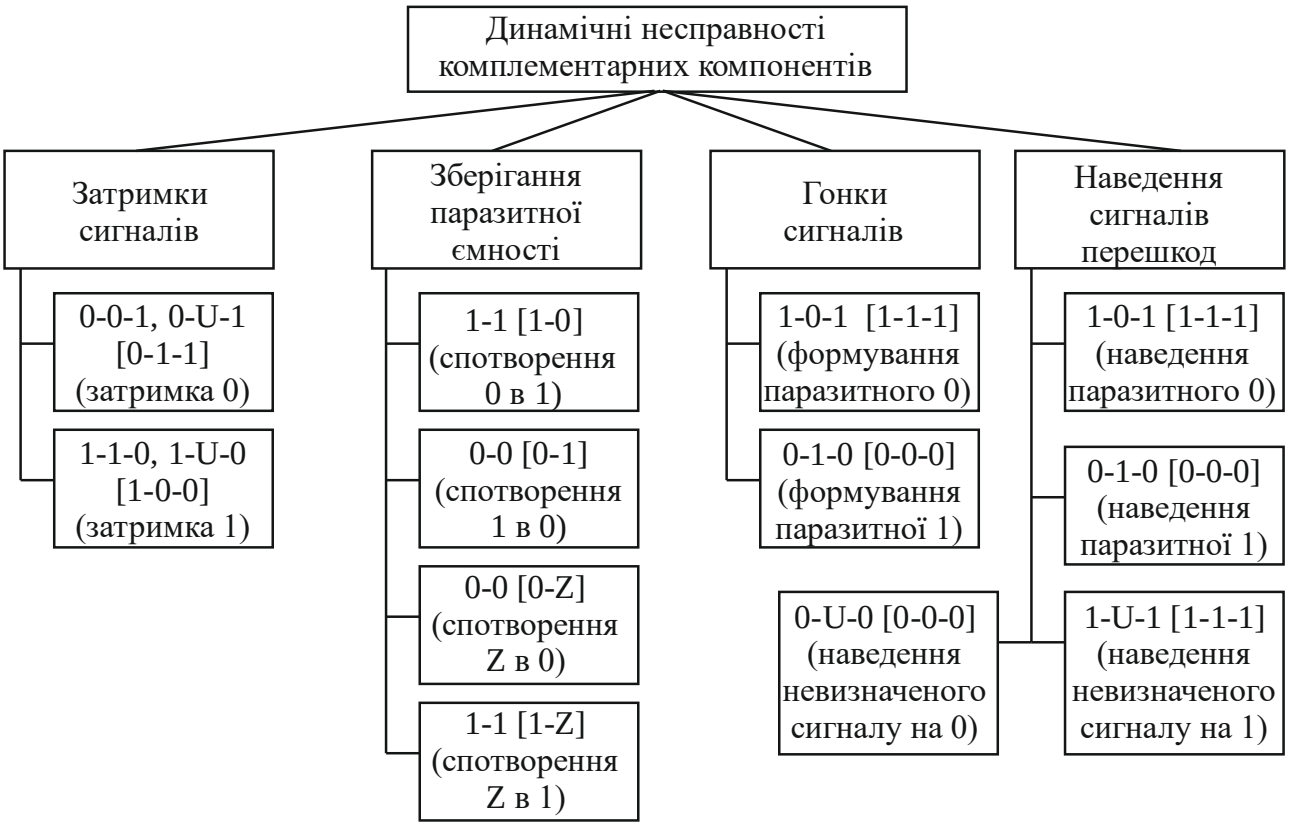


Рис. 1. Узагальнена класифікація несправностей динамічного типу ДІККЛ

У наведеній класифікації наведені чотири класи несправностей: зберігання паразитної ємності, затримки сигналів, гонки сигналів та наведення сигналів перешкод. Для кожного класу несправностей визначено типові варіанти їх прояву, надано характер спотворення сигналу в часі для кожного варіанту (спотворений варіант надано без дужок, правильний – в квадратних дужках) та короткий опис характеру спотворення.

Для усунення неоднозначності дамо визначення класів динамічних несправностей, що розглядаються, на основі яких сформуємо математичні описи моделей несправностей.

Розглянемо динамічну несправність, яка пов’язана із зберіганням паразитної ємності. Через паразитну ємність вихідний сигнал зберігає свій попередній стан *s* на протязі невизначеного часу. При спробі зміни значення виходу вентиля вхід наступного вентиля приймає не правильне значення, а значення заряду паразитної ємності.

Отже, зберігання паразитної ємності - динамічна несправність, яка полягає у «запам’ятовуванні» значення виходу вентиля внаслідок дії паразитної ємності, що призводить до утримання невірних значень на виході схеми.

Класичними переходами, при яких може проявлятися негативний вплив паразитної ємності (наявного її заряду) є перехід зі стану 0 в 1 або Z стан, а також зі стану 1 в 0 або Z стан. Ємнісна властивість в схемі відображується накопичувачем.

Відобразимо динамічну несправність, пов'язану із зберіганням паразитної ємності накопичувачем.

Нехай $x \in X$ – вхідна змінна накопичувача; $y \in Y$ – внутрішня змінна накопичувача, що відображує поточний стан вихідного сигналу. Тоді прояв динамічної несправності, пов'язаної із зберіганням паразитної ємності, буде відображатись значенням вихідної змінної q накопичувача, які визначаються за функцією (в квадратних дужка вказані зафіксоване значення вихідного сигналу і час його реєстрації, в круглих - умови):

$$\begin{aligned} q_C(t) = f_C(x,y) = [0][t=\tau_{01}](x=1 \wedge y=0) \vee [1][t=\tau_{10}](x=0 \wedge y=1) \vee \\ \vee [0][t=\tau_{0Z}](x=Z \wedge y=0) \vee [1][t=\tau_{1Z}](x=Z \wedge y=1), \end{aligned} \quad (2)$$

де τ_{01} – номінальний час переключення виходу ДІККЛ зі стану 0 в стан 1; τ_{10} – номінальний час переключення виходу ДІККЛ зі стану 1 в стан 0; τ_{0Z} – номінальний час переключення виходу ДІККЛ зі стану 0 в стан Z; τ_{1Z} – номінальний час переключення виходу ДІККЛ зі стану 1 в стан Z.

Розглянемо динамічну несправність, яка пов'язана із затримкою сигналу.

Затримка - динамічна несправність, яка полягає у збільшенні часу перетворення сигналів і проявляється при створенні умов зміни логічного рівня вихідного сигналу збереженням його початкового значення або встановленням невизначеного рівня на надлишковий період часу, що може призводити до сприйняття наступними елементами невірних значень.

Відобразимо динамічну несправність, яка пов'язана із затримкою сигналу, математичним описом моделі несправності.

Нехай $X_З \in X$ – послідовність значень вхідної змінної, яка повинна забезпечити певну зміну $\{q_1\text{-}q_2\}$ вихідного сигналу q відповідно до функції $f_З(X_З)$ перетворення вхідних сигналів на протязі часового інтервалу від t_1 до t_2, $T_З=\{t_1, t_2\}$. Відповідне призначення послідовності значень вхідної змінної будемо позначати як $X_З=\{q_1\text{-}q_2\}$. Тоді прояв динамічної несправності класу «затримки» буде відображатись динамікою зміни значень вихідних змінних $q_З$ в часі:

$$\begin{aligned} q_З(t) = f_З(X_З) = [\{0-0\}][T_З=\{t_1, t_1+\tau_{01}\}](X_З=\{0-1\}) \vee \\ \vee [\{0-U\}][T_З=\{t_1, t_1+\tau_{01}\}](X_З=\{0-1\}) \vee [\{1-1\}][T_З=\{t_1, t_1+\tau_{10}\}](X_З=\{1-0\}) \vee . \\ \vee [\{1-U\}][T_З=\{t_1, t_1+\tau_{10}\}](X_З=\{1-0\}) \end{aligned} \quad (3)$$

Розглянемо динамічну несправність, яка пов'язана із взаємовпливом сигналів у сусідніх провідниках, наслідком яких є виникнення перешкод.

Перешкода - динамічна несправність, яка полягає в індукуванні непередбаченого імпульсу в провідниках компонентів або друкованої плати пристрою за рахунок індуктивних взаємодій між сусідніми провідниками.

Індукування перехресних наводок небезпечне у двох випадках:

1) коли в провіднику, який перебуває в стані 0, формується хибна зміна значень сигналів, яка може сприйматися як послідовність сигналів 0-1-0;

2) коли в провіднику, який перебуває в стані 1, формується хибна зміна значень сигналів, яка може сприйматися як послідовність сигналів 1-0-1.

Перешкоди можуть призводити до формування хибних рівнів логічних сигналів (чіткі перешкоди) і невизначеного рівня, що не відповідає вимогам до 0 та 1 і реакцію на який інших вузлів передбачити важко (нечіткі перешкоди).

При цьому можливі два варіанти чітких перешкод:

- «0-перешкода» - динамічна несправність типу «перешкода», яка полягає в індукуванні послідовності значень сигналів 1-0-1 у провіднику, що перебуває в стані 1;

- «1-перешкода» - динамічна несправність типу «перешкода», яка полягає в індукуванні послідовності значень сигналів 0-1-0 у провіднику, що перебуває в стані 0.

Крім того, можливі два варіанти нечітких перешкод:

- «U_0-перешкода» - динамічна несправність типу «перешкода», яка полягає в індукуванні послідовності значень сигналів 1-U-1 у провіднику, який перебуває в стані 1, що може призвести до сприйняття зазначеної зміни сигналу іншими вузлами як послідовності 1-0-1;

- «U_1-перешкода» - динамічна несправність типу «перешкода», яка полягає в індукуванні послідовності значень сигналів 0-U-0 у провіднику, який перебуває в стані 0, що може призвести до сприйняття зазначеної зміни сигналу іншими вузлами як послідовності 0-1-0.

Як видно з опису, перешкода відображується трьома моментами часу $T_П=\{t_1, t_2, t_3\}$ для фіксації її наявності (t_1 – початково-стабільний стан сигналу; t_2 – час фіксації спотворення сигналу під дією перешкоди; t_3 - час повернення сигналу до початкового стану) і впливом на сигнал процесу зміни значень сигналу $X_П = x_1\text{-}x_2$ в сусідньому провіднику.

Нехай $x \in X$ – вхідна змінна (стан) сигналу лінії, яка діагностується, $X_П \in X$ – множина значень змінюваних сигналів сусідньої лінії, яка наводить перешкоду, $X_П=\{x_1, x_2\}$, $x_1 \neq x_2$. Тоді прояв «перешкоди» буде відображатись наступною функцією:

$$\begin{aligned} q_П(t) = f_П(x, X_П) = &\left[\{0-1-0\}\right]\left[T_П = \{t_1, t_2, t_3\}\right]\left(x = 0 \wedge X_П = \{0-1\}\right) \vee \\ &\vee \left[\{0-U-0\}\right]\left[T_П = \{t_1, t_2, t_3\}\right]\left(x = 0 \wedge X_П = \{0-1\}\right) \vee \\ &\vee \left[\{1-0-1\}\right]\left[T_П = \{t_1, t_2, t_3\}\right]\left(x = 1 \wedge X_П = \{1-0\}\right) \vee \\ &\vee \left[\{1-U-1\}\right]\left[T_П = \{t_1, t_2, t_3\}\right]\left(x = 1 \wedge X_П = \{1-0\}\right), \end{aligned} \tag{4}$$

де $T=\{t_1, t_2, t_3\}$ - множина часових параметрів послідовності $q_П$ вихідного сигналу, який контролюється на прояв «перешкоди»; $Q_П=\{q_1, q_2, q_3\}$ - послідовність значень вихідного сигналу лінії, який контролюється на прояв «перешкоди»; $X_П=\{x_1, x_2\}$, $x_1 \neq x_2$ - множина значень сигналу сусідньої лінії, яка наводить перешкоду.

Розглянемо динамічну несправність, яка пов’язана із гонками сигналів.

Під гонками будемо розуміти динамічну несправність, яка полягає у виникненні на виході вузла непередбаченого імпульсу за рахунок розбіжності в тривалості обробки сигналів в ланках з різним часом спрацьовування.

Зовні прояв гонок схожий на прояв перешкод, але виникнення хибних значень сигналів зумовлюється не індукуванням перехресних наводок між провідниками, а неузгодженістю спрацьовування елементів ОД в часі. Наслідком може бути два варіанти прояву гонок:

- коли на контрольованому виході, який за логікою роботи при зміні вхідних сигналів повинен перебувати в стані 0, в ході обробки зазначених вхідних сигналів тимчасово формується хибне значення вихідного сигналу 1, тобто, виникає послідовність сигналів 0-1-0;

- коли на контрольованому виході, який за логікою роботи при зміні вхідних сигналів повинен перебувати в стані 1, в ході обробки зазначених вхідних сигналів тимчасово формується хибне значення вихідного сигналу 0, тобто, виникає послідовність сигналів 1-0-1.

Таким чином, в залежності від полярності невірного імпульсу будемо розрізняти «0-гонки» і «1-гонки»:

- «0-гонки» - «гонки», які полягають у виникненні вихідного сигналу у вигляді послідовності значень 1-0-1;

- «1-гонками» - «гонки», які полягають у виникненні вихідного сигналу у вигляді послідовності значень 0-1-0.

Нехай відносно початку такту правильний стан сигналу зберігається на протязі часу t_1. Час наявності неправильного значення - t_2. Наступне правильне значення сигналу на лінії до

кінця такту наявне з часу t_3. Нехай X_{Γ}^{1} - множина з n значень вхідних сигналів для фрагменту схеми, який діагностується, що встановлює умови прояву контрольованої несправності, $X_{\Gamma}^{1}=\{x_1^1, x_2^1, \ldots, x_n^1\}$; X_{Γ}^{2} - множина з n значень вхідних сигналів для цього ж фрагменту схеми, що забезпечує умови прояву вказаної несправності після X_{Γ}^{1}, $X_{\Gamma}^{2}=\{x_1^2, x_2^2, \ldots, x_n^2\}$. Тоді прояв динамічної несправності класу «гонок» буде відображатись значеннями вихідних змінних q, які знімаються з виходу фрагмента, що діагностується, і визначаються за функцією:

$$\begin{aligned} q_{\Gamma}(t) &= f_{\Gamma}\left(X_{\Gamma}^{1}, X_{\Gamma}^{2}\right)= \\ &= [\{0-1-0\}][T_{\Gamma}=\{t_1,t_2,t_3\}]\left(X_{\Gamma}^{1}=\{x_1^1, x_2^1, \ldots, x_n^1\} \wedge X_{\Gamma}^{2}=\{x_1^2, x_2^2, \ldots, x_n^2\}\right) \vee \\ &\vee [\{1-0-1\}][T_{\Gamma}=\{t_1,t_2,t_3\}]\left(X_{\Gamma}^{1}=\{x_1^1, x_2^1, \ldots, x_n^1\} \wedge X_{\Gamma}^{2}=\{x_1^2, x_2^2, \ldots, x_n^2\}\right) \end{aligned} \quad (5)$$

де $T_{\Gamma}=\{t_1, t_2, t_3\}$ - множина значень часових параметрів «гонок»; $Q_{\Gamma}=\{q_1, q_2, q_3\}$ - послідовність вихідних значень ОД, яка змінена за рахунок прояву динамічної несправності класу «гонок».

Висновки. Запропоновані моделі несправностей несправностей динамічного типу враховують характерні особливості цифрових пристроїв з комплементарними інтегральними компонентами як об'єктів діагностування, дозволяють враховувати часові параметри зміни контрольованих сигналів та можливість набуття ними традиційних і невизначеного станів, можуть бути застосовані для формування множин і описів несправних технічних станів зазначеного класу об'єктів діагностування, розробки методів і алгоритмів діагностування, визначення вимог щодо функціональних можливостей застосовуваних технічних засобів діагностування, організації діагностичних експериментів.

ЛІТЕРАТУРА:

1. Глущак С.В. Метод і засоби тестового діагностування цифрових та мікропроцесорних пристроїв з компонентами, побудованими за КМДН-технологією: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.05 "Елементи та пристрої обчислювальної техніки та систем керування" /С.В. Глущак. – Вінниця, 2002. – 19 с.

2. Жердєв М.К. Концептуальні засади методу діагностування сучасних цифрових типових елементів заміни по форматним перехідного процесу в шині живлення / М.К. Жердєв, В.О. Савран //Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. №52. – С. 20-31.

3. Гаврилов С.В. Статический временной анализ КМОП-схем с учетом дестабилизирующих факторов / С.В. Гаврилов, Г.А. Пирютина, А.Н. Щелоков // Известия ЮФУ. Технические науки, 2013. – №7 – С.65-70.

4. Гаврилов С.В. Методы логико-временного анализа цифровых СБИС с учетом эффектов деградации транзисторов / С.В. Гаврилов, О. Гудкова, Э.Р. Каграманян // Известия ВУЗов. Электроника, 2008. – № 6. – С. 30-40.

5. Глухов С.І. Аналіз існуючих методів діагностування типових елементів заміни радіоелектронних засобів озброєння та обґрунтування необхідності використання інформаційних технологій при їх застосуванні // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. №52. – С. 12-19.

6. Андрюхин А.И. Метод параллельной генерации тестов на переключательном уровне для МОП-схем / А.И. Андрюхин // Электронное моделирование, 2011. – Т. 33. – № 1. – С. 91-98.

7. Чорненький В.І. Динамічна зміна вагових коефіцієнтів як спосіб підвищення функціональних можливостей засобів діагностування, побудованих на базі теорії штучних нейронних мереж /В.І. Чорненький // Вісник ТУП, Хмельницький, 2002. – Том1. –№3. – С.103-108.

8. Діагностичні моделі трансляторів n-МОН та КМОН структур виготовлення / М.К. Жердєв, В.В. Вишнівський, Г.Б. Жиров, С.І. Глухов //Збірник наукових праць ВІТІ НТУУ "КПІ". – К., 2006. – №3. – С.9-12.

9. Жиров Г.Б. Узагальнена діагностична модель цифрової ВІС для енергостатичного методу діагностування /Г.Б. Жиров //Вісник КНУ ім. Т. Шевченка. – К.: Київ. ун-т, 2005. – Сер. Військово-спеціальні науки, Вип. 11. – С. 54-60.

REFERENCES:

1. Hlushchak S.V. Metod i zasoby testovoho diahnostuvannia tsyfrovykh ta mikroprotsesornykh prystroiv z komponentamy, pobudovanymy za KMDN-tekhnolohiieiu: avtoref. dys. na zdobuttia nauk. stupenia kand. tekhn. nauk: spets. 05.13.05 "Elementy ta prystroi obchysliuvalnoi tekhniky ta system keruvannia" /S.V. Hlushchak – Vinnytsia, 2002. – 19s.

2. Zherdiev M.K. Kontseptualni zasady metodu diahnostuvannia suchasnykh tsyfrovykh typovykh elementiv zaminy po formatnym perekhidnoho protsesu v shyni zhyvlennia / M.K. Zherdiev, V.O. Savran //Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2016. – Vyp. №52. – S. 20-31.

3. Gavrilov S.V. Staticheskiy vremennoy analiz KMOP-shem s uchetom destabiliziruyuschih faktorov / S.V. Gavrilov, G.A. Piryutina, A.N. Schelokov // Izvestiya YuFU. Tehnicheskie nauki. – 2013. – №7 – S.65-70

4. Gavrilov S.V. Metodyi logiko-vremennogo analiza tsifrovyih SBIS s uchetom effektov degradatsii tranzistorov / S.V. Gavrilov, O. Gudkova, E.R. Kagramanyan // Izvestiya VUZov. Elektronika. – 2008. – №6. – S. 30-40.

5. Hlukhov S.I. Analiz isnuiuchykh metodiv diahnostuvannia typovykh elementiv zaminy radioelektronnykh zasobiv ozbroiennia ta obgruntuvannia neobkhidnosti vykorystannia informatsiinykh tekhnolohii pry yikh zastosuvanni //Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2016. – Vyp. №52. – S. 12-19.

6. Andryuhin A.I. Metod parallelnoy generatsii testov na pereklyuchatelnom urovne dlya MOP-shem / A.I. Andryuhin // Elektronnoe modelirovanie. – 2011 – T. 33, № 1. – S. 91-98.

7. Chornenkyi V.I. Dynamichna zmina vahovykh koefitsiientiv yak sposib pidvyshchennia funktsionalnykh mozhlyvostei zasobiv diahnostuvannia, pobudovanykh na bazi teorii shtuchnykh neironnykh merezh /V.I. Chornenkyi // Visnyk TUP, Khmelnytskyi. – 2002. – tom1, №3. – S.103-108.

8. Diahnostychni modeli transliatoriv n-MON ta KMON struktur vyhotovlennia / M.K. Zherdiev, V.V. Vyshnivskyi, H.B. Zhyrov, S.I. Hlukhov //Zbirnyk naukovykh prats VITI NTUU "KPI". – K., 2006. – №3 – S.9-12.

9. Zhyrov H.B. Uzahalnena diahnostychna model tsyfrovoi VIS dlia enerhostatychnoho metodu diahnostuvannia /H.B. Zhyrov //Visnyk KNU im. T. Shevchenka. – K.: Kyiv. un-t, 2005. – Ser. Viiskovo-spetsialni nauky, Vyp. 11. – S. 54-60.

Рецензент: д.т.н., проф. Мясіщев О.А., завідувач кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету

к.т.н. Чешун В.Н., д.т.н., проф. Ленков С.В., Прокопчук С.О.,
к.т.н., с.н.с. Охрамович М.Н., Шевченко В.В.

МОДЕЛИ ДИНАМИЧЕСКИХ НЕИСПРАВНОСТЕЙ ДИСКРЕТНЫХ ИНТЕГРАЛЬНЫХ КОМПОНЕНТОВ КОМПЛЕМЕНТАРНОЙ ЛОГИКИ

Проведенный анализ тенденций развития цифровых интегральных компонентов и средств их диагностики показывает, что длительное время основное внимание уделялось технологиям на биполярных транзисторах и наиболее актуальной считалась транзисторно-транзисторная логика с диодами Шоттки, а элементы комплементарной логики были на второстепенных позициях. В работе рассмотрены условия актуализации комплементарной технологии изготовления дискретных интегральных компонентов и последствия изменения тенденций для диагностики цифровых устройств и систем, указаны причины увеличения удельного веса неисправностей динамического типа, предоставлено классификацию указанных неисправностей компонентов комплементарной логики и описание характерных признаков их проявления, предложены математические модели типовых неисправностей динамического типа. Математические модели базируются на учете четырех возможных состояний контролируемых сигналов (логический 0 и 1, Z-состояние и неопределенное состояние) и

временных параметров их изменения, предназначенны для применения при формировании множества и моделей неисправных состояний комплементарных компонентов и построенных с их использованием цифровых объектов диагностирования, разработки методов и алгоритмов диагностирования, определения требований к техническим средствам диагностики.

Ключевые слова: тестовая диагностика, цифровые устройства, комплементарная логика, математическая модель.

Ph.D. Cheshun V.M., Ph.D. Lyenkov S.V., Prokopchuk S.O.,
Ph.D. Ohramovych M.M., Shevchenko V.V.

DISCRETE MODEL OF DYNAMIC FAULT INTEGRAL COMPONENT COMPLEMENTARY LOGIC

The analysis of trends in digital integrated components development and means of diagnostics shows, that for a long time the focus has been given to technologies based on bipolar transistors and the transistor-transistor logic with Schottky diodes was most actual, elements with complementary logic were in secondary positions. The article contains analysis of conditions of popularization complementary technology in manufacturing of discrete integrated components and effects of changes in trends for diagnostics of digital devices and systems, describes the reasons for increasing the share of dynamic type faults, includes classification of these faults for components with complementary logic and description of the characteristic features of their display, mathematical models of typical dynamic type faults. The mathematical models are based on considering four possible states of controlled signals (logic 0 and 1, Z-state and the uncertain state) and their change time parameters, proposed for use in the formation of sets and models for states of complementary components and digital objects of diagnostics with faults, for development of diagnostics methods and algorithms, for determine the technical requirements to diagnostic systems.

Keywords: test diagnostics, digital devices, complementary logic, mathematical model.

УДК 629.7.083

к.т.н., проф. **Шишанов М.О.** (ЦНДІ О ВТ)
к.т.н. **Любарець А.А.** (ДП «ДККБ «Луч»)
к.т.н., с.н.с. **Шатров А.М.** (ДНДІА)
Горбачевський С.А. (ЦНДІ О ВТ)

ВИЗНАЧЕННЯ ТЕРМІНУ ТЕХНІЧНОЇ ПРИДАТНОСТІ ЗАСОБІВ УРАЖЕННЯ НА ОСНОВІ МОДЕЛІ НАДІЙНОСТІ З АРГУМЕНТОМ, ЩО ЗАПІЗНЮЄТЬСЯ

Можливості продовження призначених показників засобів ураження встановлюються за результатами виконання сукупності робіт, зокрема оцінювання і прогнозування на продовжуваний період показників надійності.

Надійність є інтегральною властивістю, яка, в залежності від призначення зразка і умов його використання, містить сукупність властивостей: безвідмовність, довговічність і ремонтопридатність. При цьому вирішальним фактором обрання надійності для рішення задач оцінювання деградації технічного стану ЗУ є її властивість змінюватися у часі в залежності від початкових властивостей зразка та умов експлуатації. При рішенні задачі було використано апріорну гіпотезу щодо сталості потоку відмов на етапі нормальної (ефективної) експлуатації системи.

У статті викладено результати досліджень щодо можливості визначення терміну технічної придатності до використання засобів ураження із заданою достовірністю на основі моделі надійності з аргументом, що запізнюється.

Ключові слова: граничний стан, засоби ураження, інтенсивність відмов, модель надійності з аргументом, що запізнюється

Постановка проблеми. На сьогодні, одним з ключових проблемних питань підтримання боєздатності Збройних Сил України є забезпечення справності засобів ураження (ЗУ) – одних з основних складових військової техніки, які фактично визначають її бойовий потенціал та спроможність виконувати свої завдання за призначенням.

Аналіз світового досвіду підтримання справності ЗУ засвідчує, що на озброєнні провідних країн продовжують знаходитися ЗУ, виготовлені ще до початку 90-х років минулого сторіччя. Такий підхід, направлений на зменшення витрат військових відомств, притаманний багатьом країнам світу.

У загальному випадку, продовження встановлених строків придатності ЗУ до використання за призначенням – це комплекс досліджень і робіт, які виконуються для максимально повного використання фактичних залишків ресурсу (строку служби, строку зберігання) та визначення можливості їх подальшої експлуатації. Зниження вартості цих робіт може бути досягнуто за рахунок збільшення долі аналітичних та теоретичних досліджень шляхом:

- впровадження математичних моделей зміни у часі технічного стану ЗУ та їх складових частин;
- максимального використання статистичної інформації про реальний технічний стан та рівень безпеки;
- використання інформації про результати виконання таких робіт на ЗУ – аналогах.

Надійність є інтегральною властивістю, яка, в залежності від призначення зразка і умов його використання, містить сукупність властивостей: безвідмовність, довговічність і ремонтопридатність. При цьому вирішальним фактором обрання надійності для рішення задач оцінювання деградації технічного стану ЗУ є її властивість змінюватися у часі в залежності від початкових властивостей зразка та умов експлуатації. Таким чином, за результатами аналізу сукупності експлуатаційно-технічних властивостей ЗУ та їх складових частин з позицій дослідження складних технічних систем, можна зробити висновок, що в якості основного показника при розв’язанні задачі оцінювання та прогнозування зміни

технічного стану систем у часі доцільно розглядати надійність, як найбільш інформаційну властивість зразка [1].

Метою статті є розробка методики оцінки та прогнозування можливості визначення терміну технічної придатності до використання засобів ураження із заданою достовірністю на основі моделі надійності з аргументом, що запізнюється.

Основний матеріал. Сучасні ЗУ є специфічним видом військової техніки, основними особливостями яких є відносна самостійність та можливість лише одноразового використання за призначенням. Отримання інформації про показники надійності їх здійснюється шляхом вибіркового контролю відносно невеликої кількості ЗУ, які підлягають повному розбиранню з подальшим поглибленим дослідженням всіх систем, агрегатів, деталей тощо, у тому числі із застосуванням методів руйнівного контролю. Обсяг вибірки обмежується також міркуваннями економічного характеру. При цьому момент виникнення відмови можна встановити лише з точністю, яка визначається інтервалами перевірок [2].

Таким чином, для ефективного прогнозування характеристик надійності будь-яких систем, необхідно як найбільш точно встановити закон зміни інтенсивності потоку відмов $\lambda(t)$, а принциповою особливістю рішення цієї задачі – неможливість безпосередньої оцінки значень $\lambda(t)$ [1, 3].

Сучасні ЗУ складаються з великої кількості різноманітних елементів, кожен з яких виконує свої функції, побудований на використанні певних фізичних принципів та має зв'язки з іншими елементами, а структура – визначається бойовим призначенням. Разом з цим, всі вони мають спільні риси по організації побудови та складу обладнання, тобто є типовими представниками складних систем та можуть бути розглянуті з позицій теорії складних систем в організаційному і функціональному аспектах [4]. При цьому найбільш поширений підхід щодо здійснення поточних та прогнозних оцінок стану складних технічних систем базується на визначенні рівня показників їх експлуатаційних властивостей.

У зв'язку з цим, в основу розв'язання задачі щодо прогнозування термінів технічної придатності до використання ЗУ із заданою достовірністю пропонується покласти загальні положення методології дослідження складних технічних систем [4], які зокрема включають проведення декомпозиції ЗУ на складові та проведення їх ранжирування за впливом на безпеку експлуатації, вибір моделі надійності для прогнозування у часі кількісних показників критеріїв якості та врахувати випадковий характер вектора параметрів технічного стану ЗУ, який обумовлений недосконалістю технології виробництва і впливом експлуатаційних факторів, та формування довірчих інтервалів на основі правила Клопера-Пірсона [3].

Для рішення поставленої задачі в умовах обмеженої вибірки параметрів ЗУ, що визначають їх технічний стан пропонується використовувати модель надійності з аргументом, що запізнюється, яка у загальному вигляді може бути записана у вигляді [1]:

$$\lambda(\underline{A}, \underline{B}, t_з) = \varphi_1(\underline{A}, t) + \varphi_2(\underline{B}, t) \cdot 1(t - t_з), \qquad (1)$$

де $\varphi_1(\underline{A}, t)$ – функція, що апроксимує закон зміни інтенсивності відмов ЗУ у період нормальної експлуатації виробів (як правило це лінійна функція); $\varphi_2(\underline{B}, t)$ – функція, що апроксимує закон зміни інтенсивності відмов у період масових відмов ЗУ; $1(t - t_ç)$ – одинична функція, яка може приймати значення:

$$l(x) = \begin{cases} 1, x \geq 0; \\ 0, x, < 0. \end{cases}$$

де $t_ç$ – час запізнення аргументу, який визначає час переходу системи у стан технічної несправності.

При рішенні задачі використовуємо апріорну гіпотезу щодо сталості потоку відмов $\lambda(t)$ на етапі нормальної (ефективної) експлуатації системи.

Очевидно, що для визначення моменту початку масових відмов системи необхідно оцінити $t_ç$ с максимальною точністю.

Відомо декілька підходів щодо оцінки $t_ç$. Так, враховуючи модель (1) лінійна по параметрах $(a_0', a_1'; b_0', b_1') = (\underline{A}', \underline{B}')$, то фіксуючи $t_ç$ та обчислюючи відомими методами, наприклад методом найменших квадратів (МНК), отримуємо значення функціоналу, який відповідає вибраному $t_ç$. Далі задача зводиться до мінімізації функції (2)

$$\min_{\underline{A}', \underline{B}'} J(\underline{A}', \underline{B}', t_з) = j(t_з), \tag{2}$$

яка може бути розв'язана стандартними методами пошуку мінімуму функції однієї змінної.

Більш точну оцінку $t_ç$ можна отримати при використанні інтегрального МНК [5]. Вибір $t_Ç$ можна здійснювати також на основі методів індивідуальних або колективних експертних оцінок, тобто з використанням інтуїтивних методів прогнозування [1].

Разом з цим, наведені та інші методики визначення $t_ç$ не враховують імовірність досягнення граничних значень параметрами, що визначають технічний стан ЗУ або його складових частин. У зв'язку з цим пропонується наступна методика його визначення.

У загальному випадку, за результатами вибірки параметру x_i при різних строках служби АЗУ методами регресійного аналізу можливо визначити тенденцію його зміни та визначити строк служби при якому розрахункове значення параметру x_{i+n} досягне граничного значення $X_{гр}$. Остаточний вибір апроксимації та прогнозування пропонується здійснювати за рекомендаціями ДСТУ 3004-95 [5]: експоненціальний розподіл, характерний для агрегатів та технічних систем, які мало підлягають старінню та спрацюванню, а розподіл Вейбулла-Гнеденко – для систем, яким притаманні процеси механічного руйнування, стомлення, корозії, раптових змін їх властивостей. Враховуючи, що основним видом експлуатації ЗУ є зберігання, при цьому вони мало підлягають старінню і спрацюванню, доцільно використовувати експонентний розподіл

$$F(t) = 1 - e^{-\lambda t}, \tag{3}$$

Для прогнозування тривалості експлуатації ЗУ із заданою імовірністю P, необхідно розрахувати та побудувати довірчі інтервали таким чином, щоб дійсні значення параметру X не виходили за межі інтервалу ε. Тобто повинна виконуватись нерівність [5]

$$\alpha = P\left[\left|(\hat{X}_i + \sigma) - (\hat{X}_i - \sigma)\right|\right] \le \varepsilon, \tag{4}$$

де α – функція двох аргументів t_a та n, яка виз начається як $\alpha = 2\int_0^{t_a} Sn(t)dt$; σ – середньоквадратичне відхилення значення параметру; $\varepsilon = t_a S$ – довірчий інтервал.

Величина t_a визначається відповідно до заданої імовірності та кількості наявних статистичних даних (n) по таблиці, наведеній в [6], а при визначенні σ необхідно використовувати незміщені оцінки математичного очікування m_x та дисперсії σ_x^2 [3]

$$m_x = \frac{1}{n}\sum_{i=1}^{n} x_i \text{ та } \sigma_x = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\left(x_i - m_x^*\right)^2},$$

де $x_i(t)$ – значення параметра x у кожному з n незалежних вимірів.

Тоді довірчі інтервали розраховуються як

$$\varepsilon \geq \hat{X}_i \pm t_a\sigma. \tag{5}$$

Виконавши обчислення за (5) у всьому діапазоні значень x_i, отримаємо довірчі інтервали обмежені кривими $\hat{X}_i + t_a\sigma$ та $\hat{X}_i - t_a\sigma$.

Прогнозування виконується по одному або групі визначальних параметрів на визначений термін із заданою імовірністю, яка може бути визначена на основі відомих чи заданих значень потрібного рівня ефективності та безпеки функціонування ЗУ. Граничні значення параметрів визначені у відповідній нормативно-технічній документації. Результати прогнозування по деякому параметру X із заданою імовірністю 0,85 наведено на рисунку 1, на якому використано такі позначення: $X_{ãð}$ – граничне значення параметра X; ε – довірчий інтервал, розрахований за (5); $t_ç$ та $t_{ïðîã}$ – час запізнення та прогнозу відповідно.

За результатами прогнозування по визначеним параметрам та їх граничним значенням, можна визначити величину $t_з$. При цьому можливі два варіанти:

довірчий інтервал не перетинає граничні значення допуску параметру в межах заданого терміну прогнозу;

довірчий інтервал перетинає граничні значення допуску параметру в межах терміну прогнозу.

У першому випадку $t_з$ може бути обчислено шляхом розв'язання рівняння (2) або будь-яким відомим методом, але у будь якому випадку не може перевищувати термін прогнозу. Зазначимо, що досвід виконання досліджень підприємствами промисловості та науково-дослідними установами України доводить, що недоцільно продовжувати терміни технічної придатності ЗУ більш, ніж на 5 років, тобто $t_{ïðîã} \leq 5$ років. Це обумовлено тим, що процеси фізичного старіння складових частин, особливо таких, що містять матеріали спеціальної хімії, у ряді випадків є нелінійними та мають нестаціонарний характер зміни параметрів у часі [2].

У другому випадку значення $t_з$ пропонується визначати, як інтервал від моменту останнього визначення параметру до перетину одним з довірчих інтервалів граничного значення цього параметру ($X_{ãð}$), тобто $t_{ïðîã} = t_ç$ (рис. 1).

Термін технічної придатності ЗУ ($t_{прод}$) пропонується визначати як

$$\begin{cases} t_{прод} \leq t_з, & \text{при } t_{прог} = t_з; \\ t_{прод} = 5 \text{ років}, & \text{при } t_{прог} > t_з. \end{cases} \tag{6}$$

Таким чином, для визначення моменту початку масових відмов із заданою імовірністю, запропоновано підхід до обґрунтування терміни технічної придатності ЗУ та їх складових частин на основі моделі із аргументом, що запізнюється.

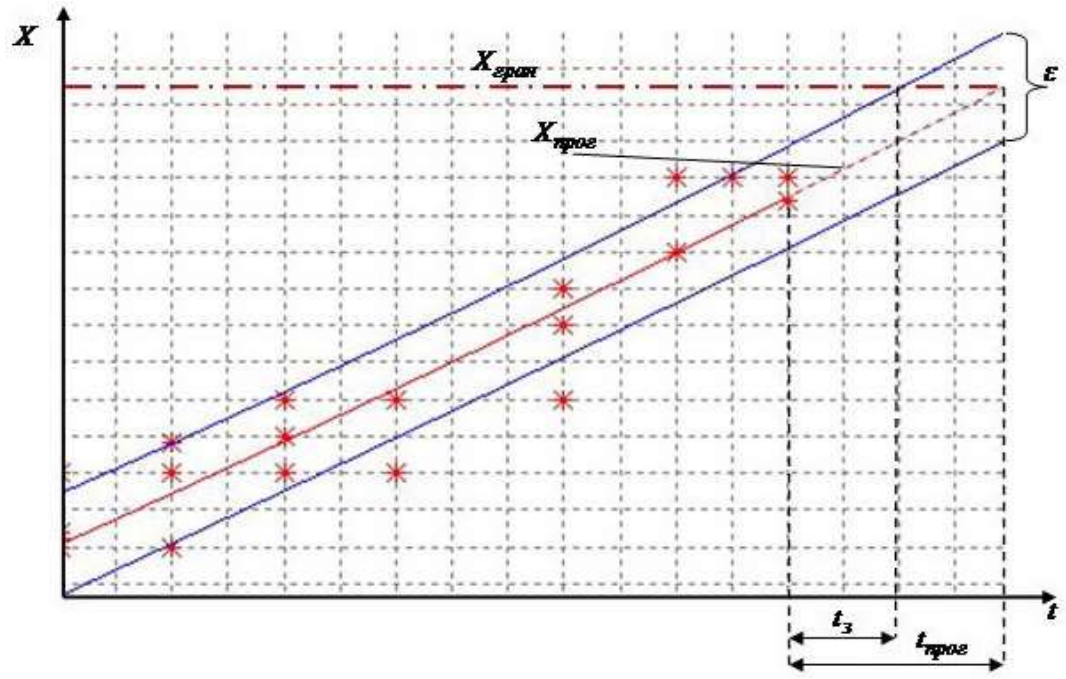


Рис. 1. Прогнозування технічного стану засобу ураження по параметру X із заданою імовірністю 0,85 та визначення для нього $t_з$

Висновки. Методика, що запропонована в статті дозволяє з заданою достовірністю враховувати технічний стан і надійність засобів ураження, на основі отриманих даних за результатами контрольних перевірок в період експлуатації.

З результатів досліджень отриманих в даній статті можна зробити наступні виводи:

довірчий інтервал не перетинає граничні значення допуску параметру в межах заданого терміну прогнозу;

довірчий інтервал перетинає граничні значення допуску параметру в межах терміну прогнозу.

Однак досвід виконання досліджень підприємствами промисловості та науково-дослідними установами України доводить, що недоцільно продовжувати терміни технічної придатності ЗУ більш, ніж на 5 років, тобто $t_{прог} \le 5$ років.

ЛІТЕРАТУРА:

1. Зубарев В. В., Ковтуненко А. П., Раскин Л. Г. Математические методы оценки и прогнозирования технических показателей эксплуатационных показателей радиоэлектронных систем: Монография. – К.: Книжное издательство НАУ, 2005. – 184 с.

2. Прогноз долговечности управляемых авиационных средств поражения в Украине / Коростелев О. П., Любарец А. А., Мамонтов В. К. // Технологические системы, №4(53), 2010. – С. 10-15.

3. Гнеденко Б. В., Беляев Ю. К., Соловьев А. Д. Математические методы в теории надежности. – М.: Наука, 1965. – 524с.

4. Ковтуненко А. П. Основы анализа сложных технических систем. Теория и приложения: Монография / А. П. Ковтуненко, В. В. Зубарев. – К.: НАУ, 2009. – 483 с.

5. ДСТУ 3004-95 “Надійність техніки. Методи оцінки показників надійності за експериментальними даними” – К.: Держстандарт України, 1995.

REFERENCES:

1. Zubarev V.V., Kovtunenko A. P., Raskin L.G. (2005). Mathematical methods for assessing and forecasting the technical performance indicators electronic systems. [Monograph], Kyiv, Book publishing house NAU, 184 p. (In Russian).

2. Korostelev O.P., Ljubarec A. A., Mamontov V.K. (2010). Forecast the longevity of managed aviation means of destruction in Ukraine. [Technological systems no.4(53)], Kyiv, VAT“Ukrainian Scientific Research Institute of aviation technology”, ZAT “Company “Industrial technologies”, pp. 10-15 (In Russian).

3. Gnedenko B.V., Belyaev Y.K., Soloviev A.D. (1965) Mathematical methods in reliability theory. [Nauka], Moscow, Akademizdatcenter “Nauka” RAN, 524 p. (In Russian).

4. Kovtunenko A.P. Zubarev V.V. (2009) Framework for the analysis of complex technical systems. Theory and applications. [Monograph], Kyiv, Book publishing house NAU, 483 p. (In Russian).

5. DSTU 3004-95 “The reliability of the technology. Methods of evaluation of reliability for the experimental data” (1995) [Government standard of Ukraine], Kyiv, DSTU, (In Ukrainian).

Рецензент: д.т.н., проф. Зубарєв В.В., головний науковий співробітник Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України

д.т.н., проф. Шишанов М.О., к.т.н. Любарец А.А., к.т.н. Шатров А.М., Горбачевский С.А.

ОПРЕДЕЛЕНИЕ СТРОКА ТЕХНИЧЕСКОЙ ПРИГОДНОСТИ СРЕДСТВ УНИЧТОЖЕНИЯ, НА ОСНОВЕ МОДЕЛИ НАДЕЖНОСТИ С ЗАПАЗДЫВАЮЩИМ АРГУМЕНТОМ

Возможности продления определенных показателей средств уничтожения устанавливаются по результатам выполнения всей работы, в частности оценки и прогнозирования на продолжительный период надежности.

Надежность является неотъемлемой чертой, которая, в зависимости от назначения образца и условий его использования, содержит набор свойств: время безотказной работы, долговечность и ремонтопригодность.

При этом решающим фактором выбора надежности для решения проблем оценки ухудшения технического состояния средств уничтожения является ее свойство различаться во времени в зависимости от первоначальных свойств образца и условий эксплуатации. Для решения проблемы было использовано априорную гипотезу относительно устойчивости потока сбоев во время нормальной (эффективной) эксплуатации системы.

В статье изложены результаты исследований о возможности определения строка технической пригодности к использования средств уничтожения с заданной точностью на основе модели надежности с запаздывающим аргументом.

Ключевые слова: граничные условия, средства уничтожения, интенсивность отказов, модель надежности с запаздывающим аргументом.

Prof. Shishanov M.O., Ph.D. Ljubarec A.A., Ph.D. Shatrov A.M., Horbachevskii S.A.

THE DEFINITION OF THE LINE TECHNICAL FEASIBILITY MEANS DESTRUCTION, ON THE BASIS OF RELIABILITY MODELS WITH RETARDED ARGUMENT

Possible extension of certain indicators means of destruction are set according to the results of the entire work, in particular the assessment and prediction of reliability for a long period.

Reliability is an integral feature of which, depending on the destination-pattern and the conditions for its use, contains a set of properties: uptime, durability and maintainability.

When you do this, the decisive factor in choosing to tackle the problems of reliability evaluation of deterioration of means of destruction is its property vary in time depending on the initial properties of the sample, and operating conditions. To solve the problem was used a priori hypothesis regarding the stability of the stream of failures during normal (effective) operating system.

The article describes the results of studies on the possibility of defining a string of technical suitability for use of means of destruction with precision on the basis of reliability models with retarded argument.

Keywords: boundary conditions, means of destruction, AFR, model reliability with retarded argument.

UDK 681.3(07)

Procenko Ya.M.
(military institute of the national university, Kiev)

MODEL OF ADAPTIVE CONDITION BASED TECHNICAL MAINTENANCE OF RADIOELECTRONIC TECHNOLOGY OBJECTS

The article proposed adaptive strategy for condition based maintenance (ACTM) of complex objects of radioelectronic technology (RET), in which the frequency of the technical condition (TC) of the object is changed (corrected) during the operation, taking into account the current dynamics of the degradation processes in the apparatus. The basic idea of the ACTM strategy is that during each next control of the TC of the object (besides the maintenance) the forecast of reliability indices of its elements is adjusted, and according to the results of an adjusted forecast the time of the next control is calculated. The article reviews the algorithm of these calculations.

The ACTM model is implemented in the framework of the simulation statistical model of the maintenance process and the RET objects repair. Through the application of the ACTM strategy, the obtained gain of the operation cost of the object is the greater (compared with the simple, not adaptive strategy), the greater is the value of the control TC of the object. The article gives an example of the strategy ACTM modelling.

Keywords: objects of radioelectronic technology, reliability indices, operation cost, simulation statistical modelling, condition based technical maintenance.

Considered objects of radioelectronic technology (RET) belong to a class of objects long repeated use, so we assume that at each time the object is able to perform the task in accordance with its purpose or in a state of readiness to perform this task. In view of the limited reliability of objects at random times there are hardware failures that lead to the disruption of the assignment and related to these losses. It is also assumed that the performance monitoring (PM) of the object is perfect, that is, any hardware failure is detected immediately at work or when the object is activated.

When a failure is detected immediately begins the repair work which requires certain costs (financial and as well as time input). In order to improve reliability of the object (and, consequently, to reduce the losses associated with the failure) the performance of technical maintenance (TM) is provided during the operation, which in most cases is reduced to preventive replacement (renewal) of the individual elements of the reliable units. If during the TM before the preventive replacement of the unit, the measurement of a parameter characterizing the technical condition (TC) of this unit is performed, such an approach to the TM it called *strategy for condition based technical maintenance (CTM)*.

In [1] was examined and investigated the model of CTM strategy with a constant frequency control, which formally is described by the following parameters

$$\mathrm{P}_{\mathrm{CTM}} = \left\langle E_{\mathrm{TM}}, U_{\mathrm{TM}}, T_{\mathrm{c}} \right\rangle, \tag{1}$$

where $\mathrm{P}_{\mathrm{CTM}}$ is a notation of generalized parameter strategy CTM; E_{TM} is a bunch of maintained units; $U_{\mathrm{TM}} = \{u_{i\,TM}; i = \overline{1, |E_{\mathrm{TM}}|}\}$ is a vector of normalized values defining parameters of maintained units in achieving that requires TM (replacement) of the unit; T_{c} is frequency of monitoring the TC of the object.

The *governing parameter* (GP) refers to the physical or functional parameter whose value is determinate by the performance capacity of the unit [2]. The limit value of GP leads to unit failure.

The set of E_{TM} is a subset of the set of all units of the object E_{o} that are taken into account in the calculation of reliability indexes (RI) of RET object. In accordance with the strategy of the CTM (1) for each maintained unit $e_i \in E$ shall be known the GP, which characterizes the actual

TC of the unit. The normalized value of the unit GP e_i denoted by $u_i(t)$ ($u_i(t) \in [0,1]$). When $u_i(t) = 1$ unit e_i considered inoperable. $U(t) = \{u_i(t); i = \overline{1, |E_{\text{TM}}|}\}$ is a vector of GP values measured at time moment *t*.

According to the strategy (1) the control of the TC (CTC) of the object RET is carried out periodically at the times $t_c = k \cdot T_c$, where $k = 1, 2, \ldots$. During the CTC, the first shall be performed the unit performance monitoring (PM) (if the object is inoperable, the control process is interrupted and then the object recovery shall be made), after that the CTC is performed for all maintained units $e_i \in E_{\text{TM}}$

CTC of the unit involves the measuring value $u_i(t)$ and check the fulfillment of condition $u_i(t) \geq u_{i\,\text{TM}}$, where $u_{i\,\text{TM}}$ is the *level* of TM, that is, a value of normalized GP, which requires preventive replacement (upgrade) the unit e_i. The level values of TM $u_{i\,\text{TM}} \in U_{\text{TM}}$ are set by parameters CTM (1).

The obvious disadvantage of CTM strategy (1) is that the frequency control T_c it remained constant throughout the period of operation of the object, although in reality the TC of the object may change. Once selected value of T_c, even if it's the optimal one, in further operation of the strategy (1) even if it is valid, it becomes insensitive to the possible changes in the actual TC of the object. In addition it is likely that the original data of the reliability indexes of object units, which were involved in calculation of the optimal T_c, contained significant errors, resulting in actual losses from failure of the object increases as compared with the minimum loss possible. In this connection, instead of deterministic strategy (1) it is proposed an adaptive strategy CTM, the essence of which is summarized in the following.

After each CTC of the object at time t_c the time of the next control time is calculated basing on t_{C+1} taken into account the current TC of the object [1]. Moment of time t_{C+1} it is calculated as follows:

$$t_{C+1} = t_C + \gamma \min_i \tilde{T}_{\text{mean}\,i}(t_k), \ (k = 1, 2, \ldots) \tag{2}$$

where γ is factor, the value of which is selected empirically; $\tilde{T}_{\text{mean}\,i}(t_C)$ is mean time to failure of the *i*-th unit in view of its TC at the time t_C ($i = \overline{1, |E_{\text{o}}|}$).

The value $\tilde{T}_{\text{mean}\,i}(t_c)$ determined by the formula

$$\tilde{T}_{\text{mean}\,i}(t_c) = 1/\tilde{a}_i(t_c), \tag{3}$$

where $\tilde{a}_i(t_c)$ is forecasted at time t_c average speed degradation GP of *i*-th unit, which is determined by the exponential smoothing method [3] in accordance with the equation:

$$\tilde{a}_i(t_c) = \beta \tilde{a}_i(t_{c-1}) + (1 - \beta) a_i(t_c), \tag{4}$$

where β is smoothing constant ($\beta \in [0,1]$);

$a_i(t_c)$ is value of GP measured at time t_c, which is determined by the formula

$$a_i(t_c) = \left(u_i(t_c) - u_i(t_{c-1})\right) / (t_c - t_{c-1}). \tag{5}$$

According to expression (4) value $\tilde{a}_i(t_c)$ it is defined as a weighted average wherein a weight β is recorded for the whole prehistory of *i*-th unit failure. Thereby the forecast $\tilde{a}_i(t_c)$ is updated each time, taking into account the current TC of the unit.

[1] In simple (non-adaptive) strategy CTM $t_{c+1} = t_c + T_c$.

It is easy to see that according to the equation (2) the time of the next control time t_{c+1} is calculated taking into account the reliability level of the object made in this current time t_c. The meaning of introduced empirical coefficient γ can be interpreted as a relative "margin of safety" (in the sense of prevention of possible failures of the object), taken as a criterion when planning regular TM. To be specific, let us call the coefficient γ anticipation index.

The analyzed model of CTM process described by the equation (2) - (5), let us agree to call an *adaptive strategy condition based TM* (ACTM). Generalized parameter of *ACTM* strategy is denoted by $\mathrm{P}_{\mathrm{ACTM}}$ and defined as follows:

$$\mathrm{P}_{\mathrm{ACTM}} = \langle E_{\mathrm{TM}}, U_{\mathrm{TM}}, \gamma, \beta \rangle. \quad (6)$$

The strategy model of *ACTM* (6) is implemented in software (ISMPN program) in the framework of the previously developed simulation statistical model (SSM) [4].

Consider the example of modeling strategy ACTM using ISMPN program. For example, we define a simple object RET consisting of 10 serially connected (in terms of reliability) of identical units. As the law of distribution of time to failure units in ISMPN program uses *DN*-distribution (this is the most adequate model for the failure of radioelectronic equipment items [2]).

At the initial data for ISMPN program for all units are specified the following parameters of *DN*-distribution: the expectation value of time to failure μ (scale parameter), and the coefficient of variation ν (shape parameter). In this example, we define values $\mu = 10000\ h$ and $\nu = 0{,}8$. As well as the following same data for all units is specified: the cost of unit C_{0i} = 1 c.u.; replacement operation cost $C_{\mathrm{repl}\,i}$ = 1 c.u.; TM operation cost $C_{\mathrm{TM}\,i}$ = 1 c.u.; the probability of unit replacement with TM $p_{\mathrm{repl}\,i}$ = 0.

The duration of object operation to be 20 years.

The following prediction estimate of indicators is obtained as a result of the simulation at the "without TM " mode:

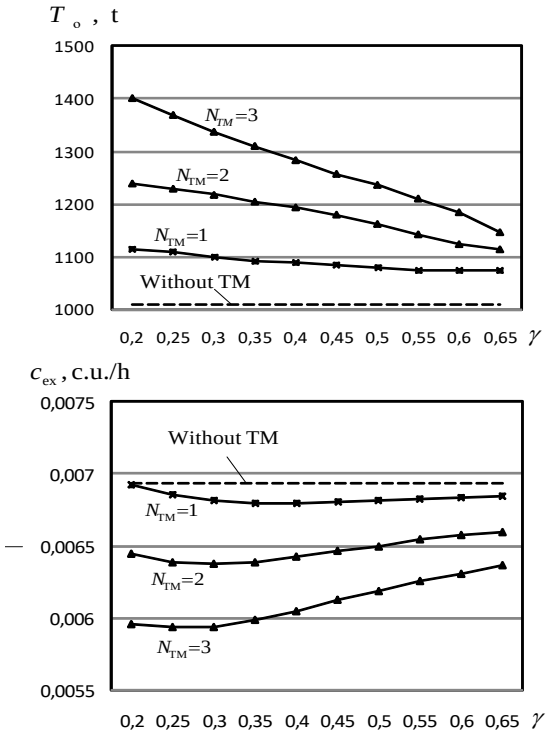


Fig. 1. The graphs of indicators T_o and c_{ex} from strategy parameters ACTM N_{TM} and γ.

$T_o = 1010\,\mathrm{h}$; $c_{ex} = 0{,}00693\,\mathrm{c.u./h}$.

Then we perform the calculations in the ACTM simulation mode with preset parameters $\mathrm{P}_{\mathrm{ACTM}}$. The goal is to determinate the nature of the parameter $\mathrm{P}_{\mathrm{ACTM}}$ influence on performance T_o and c_{ex}. The only parameters E_{ACTM} и γ of all the parameters included in $\mathrm{P}_{\mathrm{ACTM}}$ shall vary.

The calculations shall be made for three values of the parameter $E_{\mathrm{TM}}: E_{\mathrm{TM}\,1} = \{e_1\}$, $E_{\mathrm{TM}\,2} = \{e_1, e_2\}$ и $E_{\mathrm{TM}\,3} = \{e_1, e_2, e_3\}$, wherein the parameter γ will be varied within [0,2 ÷ 0,65]. Since all of the elements are the same, in the notation instead of the set $E_{\mathrm{TM}\,i}$ we will use a number of maintained units $N_{\mathrm{TM}\,i} = \left|E_{\mathrm{TM}\,i}\right|$ ($i = 1, 2, 3$).

Fig. 1 shows the graphs obtained from the results of these calculations. The obtained graph clearly shows these patterns:

1) The most significant impact on performance T_o and c_{ex} has a number of maintained units N_{TM}. With increasing N_{TM} increases the

mean time to failure of the object T_o is reduced, the specific cost of operation c_{ex}. This is consistent with the physical sense of the researched process.

2) With increasing coefficient γ of mean time to failure T_f decreases monotonically, striving asymptotically to the value of T_f without TM. This also corresponds to the physics of the processes, as it grows γ, and the average frequency of TM with an increase. The indicator c_{ex} has an extremum (minimum) at a certain value γ. It is also easy to explain: the average loss due to losses in a failed condition, with an increase in frequency of TM are beginning to prevail over the corresponding losses in the condition of TM.

In general, these following conclusions may be drawn based on the article content:

1. The proposed strategy ACTM is quite suitable for its possible implementation in practice in the design of RET objects. Obviously, the ACTM strategy will be even more effective than are the more significant costs of monitoring the TC of the object.

2. The comparing of the effectiveness of CTM strategies and ACTM has meaning only when the values of their parameters are optimal. The issue of optimization parameters CTM and ATCM strategies are not considered in the article.

3. The example ACTM strategy modeling using ISMPN program confirms the overall adequacy of the developed model and the correctness of its software implementation.

LITERATURE:

1. Lenkov S.V., Cicarev V.M., Zaycev D.V., ProcenkoY.M. Modelling of the maintenance process as objects of electronic appliances with redundant elements. *System of information processing,* no. 7 (144), pp. 61-65 (in Russian).

2. GOST 27.005-97. (1999) Reliability in technique. Model failures. The main provisions. – Introduced. – 45 p. (in Russian).

3. Sarkisian S.A. (1977) The theory of forecasting and decision-making. M.: High school. – 351 p. (in Russian).

4. Lenkov S.V., K.F. Boryak, G.V. Banzak, V.O. Braun (2014) Forecasting the reliability of complex objects electronic equipment and optimization of parameters of their technical operation, simulation of statistical models. Monography / [etc.] :– Odessa : Publisher «BMB»,. – 256 p. (in Russian).

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

Проценко Я.М.

МОДЕЛЬ АДАПТИВНОГО ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ЗА СТАНОМ ОБ'ЄКТІВ РАДІОЕЛЕКТРОННОЇ ТЕХНІКИ

У статті запропонована адаптивна стратегія технічного обслуговування за станом (АТОС) складних об'єктів радіоелектронної техніки (РЕТ), в якій періодичність контролю технічного стану (ТС) об'єкта змінюється (коригується) в процесі експлуатації з урахуванням поточної динаміки деградаційних процесів в апаратурі. Основна ідея стратегії АТОС полягає в тому, що при черговому контролі ТС об'єкта (крім самих робіт з технічного обслуговування) проводиться уточнення прогнозу показників надійності його елементів і з урахуванням отриманого уточненого прогнозу розраховується час наступного контролю. У статті розглядається алгоритм цих розрахунків.

Модель АТОС реалізована в рамках імітаційної статистичної моделі процесу технічного обслуговування і ремонту об'єктів РЕТ. За рахунок застосування стратегії АТОС виграш у вартості експлуатації об'єкта виходить тим більшим (в порівнянні з простою, що не адаптований стратегією), чим більше величина вартості контролю ТС об'єкта. У статті наводиться приклад моделювання стратегії АТОС.

Ключові слова: об'єкт радіоелектронної техніки, показники надійності і вартості експлуатації, імітаційне статистичне моделювання, технічне обслуговування за станом.

Проценко Я.Н.

МОДЕЛЬ АДАПТИВНОГО ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ПО СОСТОЯНИЮ ОБЪЕКТОВ РАДИОЭЛЕКТРОННОЙ ТЕХНИКИ

В статье предложена адаптивная стратегия технического обслуживания по состоянию (АТОС) сложных объектов радиоэлектронной техники (РЭТ), в которой периодичность контроля технического состояния (ТС) объекта изменяется (корректируется) в процессе эксплуатации с учетом текущей динамики деградационных процессов в аппаратуре. Основная идея стратегии АТОС состоит в том, что при очередном контроле ТС объекта (помимо самих работ по техническому обслуживанию) производится уточнение прогноза показателей надежности его элементов и с учетом полученного уточненного прогноза рассчитывается время следующего контроля. В статье рассматривается алгоритм этих расчетов.

Модель АТОС реализована в рамках имитационной статистической модели процесса технического обслуживания и ремонта объектов РЭТ. За счет применения стратегии АТОС выигрыш в стоимости эксплуатации объекта получается тем большим (по сравнению с простой, не адаптивной стратегией), чем больше величина стоимости контроля ТС объекта. В статье приводится пример моделирования стратегии АТОС.

Ключевые слова: объект радиоэлектронной техники, показатели надежности и стоимости эксплуатации, имитационное статистическое моделирование, техническое обслуживание по состоянию.

УДК 004.891

д.т.н., доц. **Гунченко Ю.О.** (ОНУ)
к.т.н., доц. **Бойчук В.О.** (ХмНУ)
Юмашов В.С. (ХмНУ)

МЕТОД ВИЯВЛЕННЯ ЗАГРОЗИ ПОШИРЕННЯ ЗАБОРОНЕНОЇ ДО РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

У статті розглядаються комп'ютерні мережі (КМ), що знаходяться під впливом загрози поширення забороненої інформації. Досліджуються моделі загрози поширення цієї інформації і особливості комп'ютерних мереж. Наведено основні проблеми інформаційної безпеки, які актуальні для даного дослідження. Розробляється і досліджується імітаційна модель, що враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. і аналітична модель загрози поширення забороненої до розповсюдження інформації в КМ з урахуванням топологічної вразливості мережі. Релевантність результатів аналітичного рішення підтверджена серією експериментів на топології реальної мережі з використанням імітаційного моделювання. Також розробляється методика формування топології великомасштабної КМ з проведенням досліджень, яка враховує основні топологічні характеристики доступної частини мережі і працює в умовах недостатньої репрезентативності вибірки вихідних даних. Запропоновано систему протидії загрозі поширення забороненої до розповсюдження інформації.

Ключові слова: безпека комп'ютерних мереж, заборонена інформація, моделювання, формування топології.

Вступ. Комп'ютерні мережі (КМ) забезпечують практично повний спектр можливостей для обміну інформацією між користувачами - мережевими абонентами. Комп'ютерна мережа надає різні сервіси для організації соціальних взаємовідносин між користувачами (абонентами). На сьогоднішній день найбільш популярним з них є соціальні мережі. У світі існує величезна кількість різних соціальних мереж, але практично в кожній країні або регіоні існують кілька найбільш популярних представників. У США це «Facebook», «MySpace», «Twitter» і «LinkedIn»; «Nexopia» - в Канаді, «Bebo» - в Великобританії, «Facebook», «dol2day» - в Німеччині. В Україні на сьогоднішній день найпопулярними є «ВКонтакте» і «Одноклассники». Сучасною проблемою таких систем є їх низький рівень інформаційної безпеки. Для забезпечення захисту інформації в телекомунікаційних мережах, включаючи Інтернет, розроблено безліч методів і засобів, запропонованих в працях П.Д. Зегжди, С.П. Расторгуєва, Р. Бретта, В.І. Завгороднього, В.А. Герасименко, А.А. Малюка, В. Столінгса, К. Касперски, С. Норкатта, В.В. Домарева. Тим не менш, ефективного захисту абонентів від загроз поширення забороненої інформації, зокрема в умовах широкого використання індивідуально-орієнтованих сервісів і пов'язаних з ними протоколів і технологій (SOAP, CORBA, REST і ін.), не існує. Серед безлічі функцій захисту принциповою відносно цих систем є функція попередження прояву забороненої інформації. Вона реалізується за рахунок механізмів прогнозування загрози поширення і розсилки повідомлень з попередженнями про наслідки дій із забороненим контентом. Використання інших функцій (попередження, виявлення, локалізації та ліквідації загрози) припускає наявність повного контролю над системою, що в справжніх умовах неможливо.

Постановка задачі. Одним з підходів до прогнозування загрози поширення забороненої інформації (ЗгЗІ) є моделювання, наприклад, з використанням моделей впливу, моделей просочування і зараження (Д.А. Новиков, Д.А. Губанов і А.Г. Чхартішвілі, J. Leveille, D . Watts і S. Strogatz, R. Albert та A. Barabasi, J. Leskovec, M. Gjoka, SN Dorogovtsev, MEJ Newman і RM Ziff, JO Kephart і SR White і ін.). Дані моделі, як правило, не враховують топологічні особливості мережі (розподіл ступенів зв'язності, кластерний коефіцієнт, середня

довжина шляху). Взаємодія між абонентами в рамках цих математичних моделей описується переважно гомогенним графом, що при моделюванні великомасштабних мереж (більше 10 млн. вузлів) може дати похибку прогнозування ЗгЗІ більше 30%. Крім того, дані підходи носять в основному теоретичний характер, практика їх використання не виходить за рамки експериментів. Таким чином, дослідження, спрямовані на створення моделей та алгоритмів ЗгЗІ, актуальні і мають теоретичне і практичне значення у вирішенні проблеми забезпечення інформаційної безпеки в системах і мережах телекомунікацій.

Мета роботи полягає в підвищенні точності прогнозування загрози поширення забороненої інформації в комп'ютерних мережах.

Для досягнення мети роботи необхідно вирішити наступні завдання:

1. Провести інформаційний огляд і експерименти для виявлення істотних характеристик об'єкта і зовнішніх факторів, що впливають на процес реалізації ЗгЗІ. Виконати аналіз основних підходів до моделювання ЗгЗІ.

2. Розробити імітаційну модель ЗгЗІ в КМ.

3. Синтезувати і показати адекватність аналітичної моделі ЗгЗІ в КМ.

4. Розробити методику формування топології КМ.

5. Змоделювати процес реалізації ЗгЗІ на топології реальної великомасштабної КМ. Провести експериментальне дослідження з отриманими результатами.

Виклад основного матеріалу досліджень. За результатами огляду предметної області було поставлено завдання створення імітаційної і аналітичної моделей поширення загрози забороненої інформації в КМ. Імітаційна модель необхідна для отримання експериментальних результатів для синтезування аналітичної моделі. Необхідність створення аналітичної моделі обґрунтовується тим, що для імітаційного моделювання на топології існуючих комп'ютерних мереж (десятки мільйонів вузлів) необхідні великі витрати часу. Не враховуючи час на збір інформації про топологію мережі, який може становити близько тижня, безпосередньо моделювання загрози поширення забороненої інформації займає кілька годин навіть при використанні розподілених обчислювальних ресурсів. Аналітична модель може дати прогноз ЗгЗІ майже миттєво. З її допомогою можна отримати актуальні дані (до того моменту, коли кількість атакуючих абонентів буде максимальним) по динаміці ЗгЗІ.

Процес ЗгЗІ характеризується наступними особливостями. У мережі існують вузли трьох типів. Перший тип - атакуючі вузли, це вузли, які розповсюджують заборонену до поширення інформацію. Другий тип - захищені вузли, які характеризуються тим, що не беруть участі в поширенні забороненої інформації і ніколи не будуть цим займатися. Третій тип - потенційно вразливі. Вузли такого типу не беруть участі в процесі поширення загрози, але можуть бути схильні до негативного впливу з боку атакуючих вузлів і можуть почати поширювати заборонену інформацію.

Імітаційне моделювання:

Наведемо алгоритм реалізації ЗгЗІ, грунтуючись на описі процесів, що протікають в реальних КМ. Схема реалізації загрози представлена на рис. 1.

Крок 1. Поширення інформації забороненої до поширення (ЗІ) (далі процес «атаки») ініціює будь-який абонент-зловмисник (на рисунку - вузол 1), поширюючи повідомлення з ЗІ (реалізує загрозу) по його списку контактів. Атаку може починати один зловмисник або група.

Крок 2. Абоненти-одержувачі (вузли 2,3,4), прийнявши повідомлення з ЗІ, читають його і включаються в процес атаки, поширюючи його далі по своїх контактах (вузол 3), або ігнорують або взагалі видаляють повідомлення (вузол 2), тобто в атаці не беруть участь. Процес атаки зазвичай йде лавиноподібно. Атакуючі абоненти не закінчують атаку, одного разу передавши повідомлення із забороненою інформацією. Вікно атаки, як правило, триває протягом досить значного проміжку часу і залежить від типу подачі ЗІ в повідомленні, зацікавленості абонента і тд.

Крок 3. Абоненти можуть перестати сприймати і, відповідно, поширювати ЗІ (вузол 5) (далі процес «захисту»), внаслідок впливу механізмів захисту (наприклад, попередження про нього), тому повідомлення з ЗІ від атакуючих абонентів будуть постійно відхилятися.

Крок 4. Процес триває поки в мережі є абоненти-зловмисники, або є потенційно вразливі вузли, якщо відсутній процес захисту.

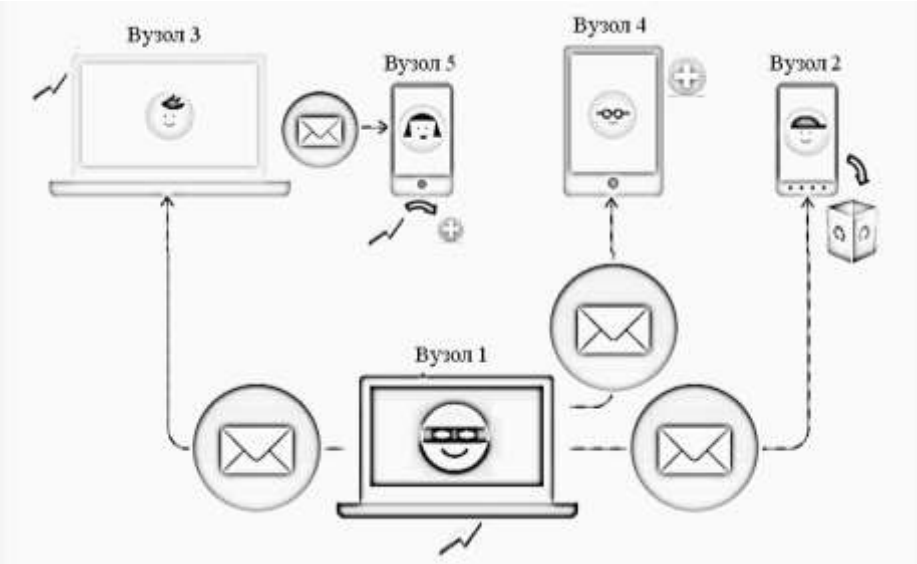


Рис. 1. Схема реалізації ЗгЗІ

Таким чином, ЗгЗІ в КМ являє собою складний динамічний процес, що складається з двох протидіючих підпроцесів атаки і захисту вузлів мережі. Для моделювання таких явищ часто застосовують епідеміологічні моделі, зокрема нашому опису точно відповідає SIR-модель Кермака-Маккендріка. Характер графіків, отриманих в результаті імітаційного моделювання (рис. 2 і 3), схожий з результатами, які дає дана модель. За наведеними вище причинами дана модель була взята за основу в цьому дослідженні. При використанні системи диференціальних рівнянь SIR-моделі для аналізу ЗгЗІ в КМ отримали результати у вигляді графіків, які хоча і правильно описують характер процесу, але не дають потрібної точності прогнозу.

На основі описаного алгоритму була побудована імітаційна модель ЗгЗІ в КМ.

Імітаційна модель ЗгЗІ:

Вхідні дані: N - кількість вузлів, що дорівнює кількості абонентів мережі, k - середній ступінь зв'язності вузлів, α - параметр, що відображає середню довжину шляху і рівень мережевої кластеризації, β - параметр, що відображає силу загрози, ймовірність здійснення атаки, γ - параметр відображає ступінь протидії загрозі, ймовірність захисту абонента (в моделі вважається, що β і γ однакові для кожного абонента), I_0 (абоненти-зловмисники - початкові джерела загрози) R_0 (абоненти, початково-несприйнятливі до атакуючих дій). Вихідні дані: $I(t)$, $R(t)$, $S(t)$ - чисельні масиви даних, що описують динамічний процес реалізації ЗгЗІ (кількості атакуючих, захищених і потенційно вразливих вузлів в кожну умовну одиницю часу відповідно).

Крок 1. Створення топології КМ – графа $G_{sw} =< V, E >$, де G_{sw} - граф small-world мережі (на основі моделі Watts-Strogatz), $V = \{v_i\}$ - множина вершин, $E = \{e_{ij}\}$ - множина ребер, $i = 1..N$, $j = 1..N$. Даний крок здійснюється з використанням вільно розповсюджуваної програми Pajek, адаптованої під це завдання, за рахунок заданих топологічних параметрів N, k, α .

Крок 2. Сформувати множину $V = \{V^I, V^S, V^R\}$, де $V^I = \{v_i^I\}$ – множина атакуючих вузлів $(|V^I| = I_0)$, $V^R = \{v_i^R\}$ - множина захищених вузлів $(|V^R| = R_0)$, $V^S = \{v_i^S\}$ - множина потенційно вразливих вузлів $(|V^S| = N - I_0 - R_0)$.

Крок 3. $\forall v_i^I$ якщо $\exists e_{ij}$ і $v_j \in V^S$ $j = 1..N$, то з ймовірністю β виконати: $V^S \backslash v_j$ і $V^I \cup v_j$; з ймовірністю γ виконати: $V^I \backslash v_i$, $V^R \cup v_i$.

Крок 4. Якщо $V^I = \varnothing$ або $\gamma = 0$ і $V^S = \varnothing$, то кінець алгоритму, інакше перейти до кроку 3.

Після вибору типу мережі та введення параметрів відбувається імітаційне моделювання за алгоритмом реалізації ЗгЗІ. Потім результати відправляються в функцію побудови графіків для виведення результатів в графічному вигляді. На рис. 2 і 3 наведені результати імітаційного моделювання ЗгЗІ на мережі з параметрами $(N = 10000, \beta = 0{,}2, \gamma = 0{,}1, I_0 = 1, R_0 = 2000)$.

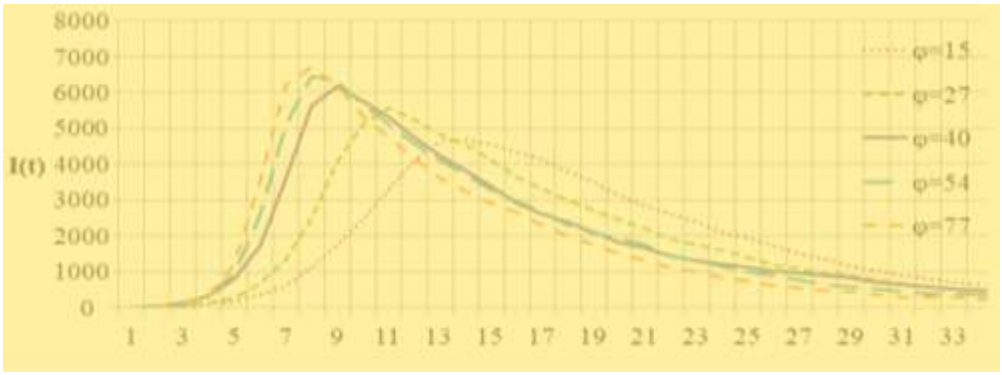


Рис. 2. Результати імітаційного моделювання ЗгЗІ

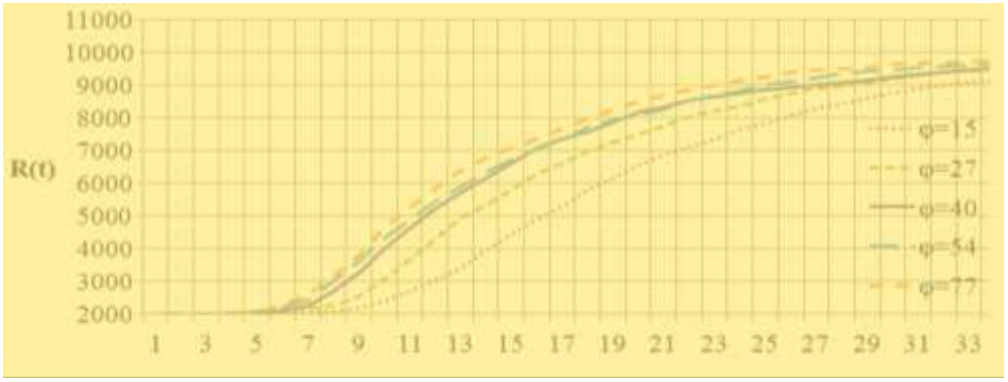


Рис. 3. Результати імітаційного моделювання ЗгЗІ

SIR (від англ. Susceptibles - Infectives - Removed with immunity) - епідеміологічна модель, спрощено описує поширення захворювання, що передається від одного індивіда до іншого, яка розглядає суб'єктів з точки зору трьох можливих станів: сприйнятливий, інфікований, імунізований.

Система диференціальних рівнянь, що описують SIR-модель, має вигляд [6,7]:

$$\begin{cases} \dfrac{dI}{dt} = \beta \cdot \dfrac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \dfrac{dR}{dt} = \gamma \cdot I(t) \\ \dfrac{dS}{dt} = -\beta \cdot \dfrac{S(t) \cdot I(t)}{N} \end{cases},$$

де $I(t)$ - кількість заражених (інфікованих) особин, $S(t)$ – кількість сприйнятливих особин, $R(t)$ - кількість «виключених з імунізацією» (removed with immunity) особин, $N = I(t) + S(t) + R(t)$ - кількість особин в популяції, γ - коефіцієнт відновлення / смерті, β - швидкість зараження (інфікування), t - час. Дана система є надлишковою – будь-яке рівняння з трьох рівнянь можна виключити.

Була висунута гіпотеза про те, що система не дає потрібної точності в зв'язку з тим, що в моделі, яку вона описує, не враховуються топологічні особливості мережі. У зв'язку з цією гіпотезою було поставлено завдання адаптування системи шляхом інтегрування в неї параметра топологічної вразливості мережі φ.

В результаті отримали аналітичну модель, яка описується системою диференційних рівнянь:

$$\begin{cases} \dfrac{dI}{dt} = 2 \cdot \ln \varphi \cdot \beta \cdot \dfrac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \dfrac{dR}{dt} = \gamma \cdot I(t) \\ \dfrac{dS}{dt} = -2 \cdot \ln \varphi \cdot \beta \cdot \dfrac{S(t) \cdot I(t)}{N} \end{cases},$$

де φ - коефіцієнт топологічної вразливості мережі - показник, який обчислюється за формулою:

$$\varphi = \frac{k \cdot (C+1)}{L},$$

k - середній ступінь зв'язності вузлів мережі, C - коефіцієнт кластеризації мережі, L - середня довжина шляху мережі.

Релевантність результатів аналітичного рішення підтверджена серією експериментів на топологіях реальних мереж з використанням імітаційного моделювання. При цьому похибка для процесу захисту склала не більше 10%, для процесу атаки - не більше 15%.

Для моделювання ЗгЗІ необхідно мати топологію реального об'єкта. Пряме отримання цієї інформації утруднено у зв'язку з тим, що для підвищення точності результатів моделювання необхідно мати топологію всієї мережі. Отримати таку інформацію без прав адміністратора не представляється можливим. При зборі даних з правами абонента КМ маємо справу з двома типами вузлів: відкритими і закритими. Якщо в ході збору даних ми отримуємо ідентифікатори (id) вузла і суміжних з ним вузлів, то такий вузол називаємо відкритим. Якщо ж отримуємо тільки id вузла (абонент за допомогою налаштувань приховав інформацію про свої контакти), то такий вузол називаємо закритим. Також в мережі можуть існувати вузли, які з'єднані тільки з закритими вузлами. В такому випадку неможливо отримати навіть ідентифікатор вузла. Таких вузлів в мережі незначна частина. Емпірично показано, що закритих вузлів на порядок більше, ніж відкритих, тому при зборі даних втрачається значна частина інформації.

При наявності адміністративного ресурсу можна реалізувати автоматизовану систему протидії загрозі поширення забороненої інформації. Узагальнений алгоритм роботи такої

системи представлений на рис. 4. Розглянуті функції реалізуються за допомогою типових засобів.

Крок 1. Введення даних - типове повідомлення, що містить інформацію, заборонену до поширення. База даних таких повідомлень формується зі списку екстремістських матеріалів і реєстру доменних імен, покажчиків сторінок сайтів в мережі «Інтернет» і мережевих адрес, що дозволяють ідентифікувати сайти в мережі «Інтернет», що містять інформацію, поширення якої в Україні заборонено.

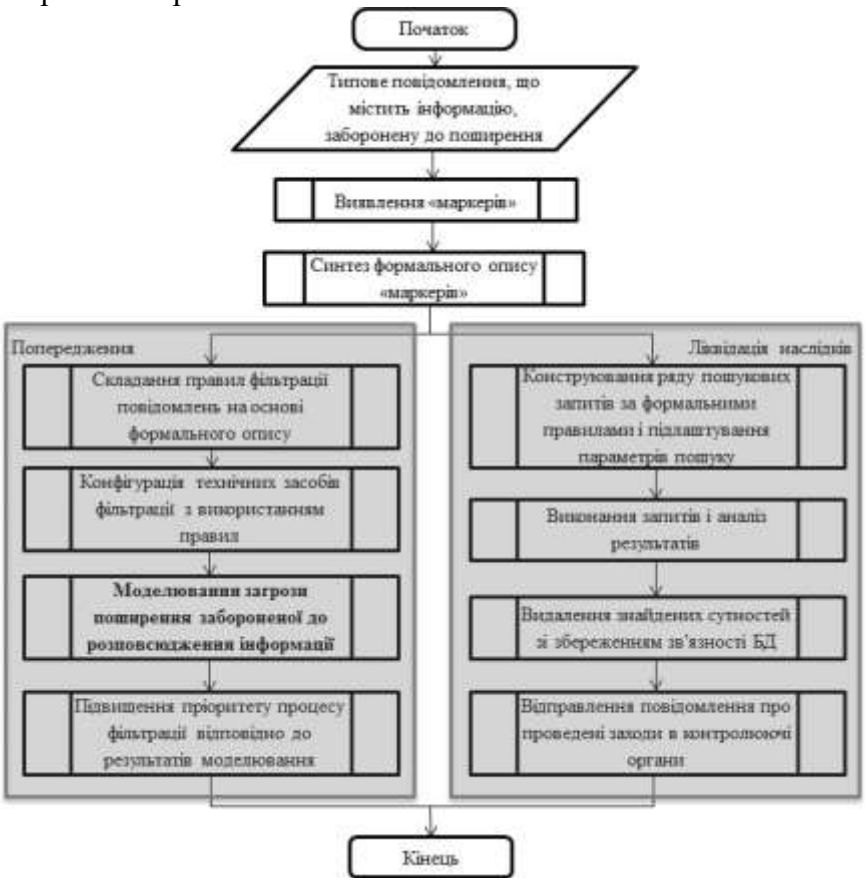


Рис. 4. Узагальнений алгоритм протидії поширенню загрози забороненої до розповсюдження інформації

Крок 2. Виявлення «маркерів», тобто слів і словосполучень, які мінімально змінюються в ході переформулювання.

Крок 3. Синтез формального опису «маркерів» з використанням регулярних виразів або контекстно-вільної граматики.

Далі робота алгоритму розбивається на дві частини, паралельно виконуються процедури попередження і усунення наслідків загрози.

Попередження

Крок 4а. Складання правил фільтрації повідомлень на основі формального опису. Здійснюється шляхом компіляції регулярних виразів за допомогою засобів, призначених для фільтрації (див. Крок 5а).

Крок 5а. Конфігурація технічних засобів фільтрації з використанням правил. Як правило, це антиспам системи такі як FASTBL, Apache Spamassassin, Kaspersky Antispam, Yandex Spamooborona, dnsbl і ін.

Крок 6а. Моделювання загрози поширення забороненої до розповсюдження інформації.

Крок 7а. Підвищення пріоритету процесу фільтрації відповідно до результатів моделювання загрози поширення забороненої інформації.

Ліквідація наслідків

Крок 4б. Конструювання ряду пошукових запитів за формальними правилами і підлаштування параметрів пошуку (пріоритет, глибина і тд.)

Крок 5б. Виконання запитів і аналіз результатів. На даному етапі можливе уточнення запитів.

Крок 6б. Видалення знайдених сутностей зі збереженням зв'язності БД.

Крок 7б. Відправлення повідомлення про проведені заходи в контролюючі органи.

Висновки. В результаті інформаційного огляду і проведених експериментів було виявлено, що на ЗгЗІ в комп'ютерних мережах істотно впливає топологія інформаційних зв'язків між абонентами і модель інформаційної взаємодії між ними. Виконаний аналіз основних підходів до моделювання ЗгЗІ показав, що найбільш адекватними моделями для цього завдання є моделі впливу, просочування і зараження. Створена імітаційна модель ЗгЗІ в КМ. З її допомогою проведені експерименти, результати яких показали залежність реалізації ЗгЗІ від топологічної вразливості мережі. Розроблено аналітичну модель. Похибка для процесу захисту склала не більше 10%, для процесу атаки - не більше 15%. Розроблено методику формування топології КМ. Створено алгоритм формування вихідних даних про топологію мережі (велика кількість вершин і зв'язків між ними доступної частини мережі), який враховує обмеження по збору даних. Розроблено алгоритм формування повного графа мережі з урахуванням додавання недоступної частини на основі обчислених прогнозованих топологічних характеристик. В ході експериментальних досліджень були отримані результати, що стосуються топології розглянутих КМ. Отримане значення середньої довжини шляху сходиться з результатами незалежних досліджень та дає можливість використовувати його в аналітичній моделі як фіксований параметр. В якості рекомендацій запропонований алгоритм роботи системи протидії поширенню загрози забороненої до розповсюдження інформації.

Приклади ефективного застосування механізмів прогнозування ЗгЗІ в КМ дають підставу констатувати адекватність і функціональність основних теоретичних побудов і розроблених на їх основі алгоритмічних і інструментальних засобів.

ЛІТЕРАТУРА:

1. Ferrara E. Topological features of Online Social Networks. Communications on Applied and Industrial Mathematics / E. Ferrara, G. Fiumara, 2011.

2. Easley D. Networks, Crowds and Markets Reasoning About a Highly Connected World / D. Easley, J. Kleinberg, 2010.

3. Albert R. Statistical mechanics of complex networks / R. Albert, A. Barabasi; Rewiews of Modern Physics, 2002.

4. Губанов Д.А. Соціальні мережі: моделі інформаційного впливу, керування і протистояння / Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили; под. ред. чл..-корр. РАН Д.А. Новикова – М.: Видав. Фізико-математичної літератури, 2010. – 228 с.

5. Закон України про захист суспільної моралі [Електронний ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1296-15

6. Frauenthal, J.C. Mathematical Models in Epidemiology / J.C. Frauenthal; New York: Springer-Verlag, 1980. – 335 s.

7. Hethcote, H.W. The Mathematics of Infectious Diseases / H.W. Hethcote; - 2000.

8. Roberts, M.G., Heesterbeek, JAPMathematical models in epidemiology / M.G. Roberts, Heesterbeek JAP; In JA. Filar (Ed.) Mathematical Models.Oxford: EOLSS Publishers Ltd, 2004.

REFERENCES:

1. Ferrara E. Topological features of Online Social Networks. Communications on Applied and Industrial Mathematics / E. Ferrara, G. Fiumara, 2011.

2. Easley D. Networks, Crowds and Markets Reasoning About a Highly Connected World / D. Easley, J. Kleinberg, 2010.

3. Albert R. Statistical mechanics of complex networks / R. Albert, A. Barabasi; Rewiews of Modern Physics, 2002.
4. Hubanov D.A. Sotsialni merezhi: modeli informatsiinoho vplyvu, keruvannia i protystoiannia / D.A. Hubanov, D.A. Novykov, A.H. Chkhartyshvyly; pod. red. chl..-korr. RAN D.A. Novykova – M.: Vydav. Fizyko-matematychnoi literatury, 2010. – 228 s.
5. Zakon Ukrainy pro zakhyst suspilnoi morali [Elektronnyi resurs] – Rezhym dostupu: http://zakon2.rada.gov.ua/laws/show/1296-15
6. Frauenthal, J.C. Mathematical Models in Epidemiology / J.C. Frauenthal; New York: Springer-Verlag, 1980. – 335 s.
7. Hethcote, H.W. The Mathematics of Infectious Diseases / H.W. Hethcote; - 2000.
8. Roberts, M.G., Heesterbeek, JAPMathematical models in epidemiology / M.G.Roberts, Heesterbeek JAP;In JA. Filar (Ed.) Mathematical Models.Oxford: EOLSS Publishers Ltd, 2004.

Рецензент: д.т.н., проф. Мясіщев О.А., завідувач кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету

д.т.н., доц. Гунченко Ю.А., к.т.н. Бойчук В.О., Юмашов В.С.

МЕТОД ВИЯВЛЕННЯ ЗАГРОЗИ ПОШИРЕННЯ ЗАБОРОНЕНОЇ ДО РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

В статье рассматриваются компьютерные сети (КС), которые находяться под влиянием угрозы распространения запрещенной информации. Исследуются модели угрозы распространения этой информации и особенности компьютерных сетей. Приведены основные проблемы информационной безопасности, которые актуальны для даного исследования.
Разрабатывается и исследуется имитационная модель, учитывающая топологические характеристики сети, а также особенности информационного взаимодействия абонентов как человеко-машинных систем. и аналитическая модель угрозы распространения запрещенной к распространению информации в КС с учетом топологической уязвимости сети. Релевантность результатов аналитического решения подтверждена серией экспериментов на топологии реальной сети с использованием имитационного моделирования. Также разрабатывается методика формирования топологии крупномасштабной КС с проведением исследований, которая учитывает основные топологические характеристики доступной части сети и работает в условиях недостаточной репрезентативности выборки исходных данных. Предложена система противодействия угрозе распространения запрещенной к распространению информации.

Ключевые слова: безопасность компютерных сетей, запрещенная информация, моделирования, формирование топологии.

Ph.D. Gynchenko Y.A., Ph.D. Boychuk V.O., Yumashov V.S.

METHOD FOR DETECTION OF THREATS DISTRIBUTE ILLEGAL TO SPREAD INFORMATION IN COMPUTER NETWORKS

The article deals with computer networks (CN), which are influenced by the threat of banned information. Investigate the threat model disseminate this information and especially computer networks. The basic problem of information security, which are relevant to our study.
Developed and researched simulation model that takes into account the topological characteristics of the network, and also features information interaction subscribers of human-machine systems. and the threat of analytical model forbidden to disseminate information to the CM based topological network vulnerability. The relevance of the results of analytical decision confirmed a series of experiments on real network topology using simulation. Also, the technique of forming a large-scale topology of KM research, which takes into account the basic topological characteristics of the available network up and running in low representativeness of the sample source data. The system to counter the threat propagation prohibited to disseminate information.

Keywords: security computer networks, prohibited information, modeling, forming topology.

УДК 004.891 **Козак І.В.** (ХмНУ)
к.т.н., доц. **Огнєвий О.В.** (ХмНУ)

МЕТОД ПРОТИДІЇ ПРИХОВАНИМ ЗАГРОЗАМ В СЕРЕДОВИЩІ ХМАРНИХ ОБЧИСЛЕНЬ

У результаті проведеного аналізу в статті доводиться актуальність розробки технології протидії спробам змінити стан захищеності інформаційних ресурсів у середовищі хмарних обчислень. В результаті досліджень, проведених авторами, зроблено висновок про те, що перспективним напрямком вдосконалення технологій кіберзахисту в середовищі хмарних обчислень є розробка методів протидії загрозам, які реалізуються з допомогою процесів, в яких суб'єкти і об'єкти інформаційної взаємодії можуть використовувати різні канали передачі даних, у тому числі і приховані. Показано, як реалізація прихованих загроз дозволяє шкідливому коду маскуватися під системний процес, завдаючи шкоди безпеці середовища хмарних обчислень за допомогою блокування, розкрадання, знищення або несанкціонованої передачі інформації.

Для боротьби з такими загрозами актуальною є розробка нових засобів захисту інформації, заснованих на методах оперативної ідентифікації потенційних вразливостей, що виникають як на рівні процесів контролю доступу до ресурсів гостьових ОС, так і на рівні системних викликів гіпервізора, які за певних умов самі можуть ставати джерелами різних видів руйнівних впливів.

Відповідно, виникає необхідність в розробці математичної моделі прихованих загроз інформаційної безпеки, в якій враховується поведінковий характер об'єктів інформаційної взаємодії. Також розроблено модель інформаційного забезпечення для хмарних обчисленнях, що дозволяє представити формалізований опис інформаційних процесів у середовищі хмарних обчислень у вигляді мультиграфа транзакцій. На основі цих моделей розроблено метод протидії прихованим загрозам, заснований на контролі транзакцій, що відповідають вимогам політики безпеки.

Ключові слова: кібербезпека, хмарні обчислення, приховані загрози, захист інформації.

Вступ. Доктрина інформаційної безпеки України визначає поняття інформаційної сфери як сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, розповсюдження і користування інформації, а також системи регулювання суспільних відносин, що виникають при цьому. Інформаційна безпека в широкому сенсі є таким станом об'єкту захисту, яке, виключає можливість нанесення шкоди властивостям об'єкту, обумовленою його взаємодією з інформаційною сферою [1]. Згідно стандартів загроза безпеці визначається як сукупність умов і чинників, що створюють потенційну або таку, що реально існує небезпеку, пов'язану з просочуванням інформації і/або несанкціонованими і/або ненавмисними діями на неї.

Стрімкий розвиток технологій віртуалізації і створення середовищ хмарних обчислень формує нові джерела загроз, які необхідно враховувати при забезпеченні кібербезпеки сучасних комп'ютерних систем і сервісів. При цьому динамічний характер процесів інформаційної взаємодії істотно ускладнює можливості оперативної оцінки ризиків порушення конфіденційності, цілісності і доступності програмних та інфраструктурних ресурсів, що надаються в режимі віддаленого доступу.

Традиційні засоби забезпечення інформаційної безпеки такі, як засоби розмежування доступу, міжмережеві екрани, системи виявлення вторгнень, контролюють тільки ті інформаційні потоки, які проходять по каналах, призначеним для їх передачі, тому загрози, які реалізуються за допомогою прихованих каналів передачі інформації, з їх допомогою не можуть бути блоковані. В цих умовах важливого значення набувають технології захисту від загроз, які формуються з використанням прихованих каналів інформаційного впливу або всередині периметра безпеки корпоративної комп'ютерної мережі. Захист від таких деструктивних впливів повинна здійснюватися на рівні процесів управління системними викликами або контролю недекларованих можливостей прикладного програмного забезпечення, що вимагає створення нових моделей і методів протидії спробам як зовнішніх,

так і внутрішніх користувачів змінити стан захищеності інформаційних ресурсів середовища хмарних обчислень.

Хмарні технології стануть основою для формування нового простору, що створюється в рамках ініціативи, що отримала назву Intelligence Community Information Technology Enterprise.

У роботі по розгортанню хмарної платформи беруть участь фахівці всього розвідувального співтовариства США, яких припадає на частку основна частина бюджету американської розвідки [2].

Наприклад, ЦРУ розробляє захищену хмарну обчислювальне середовище для всього розвідувального співтовариства.

Ідея, що лежить в основі розвитку і впровадження розподілених інформаційних технологій хмарних обчислень в розвідувальну діяльність, давно стала стійким трендом для багатьох федеральних відомств і комерційного сектора США і привела до істотного скорочення їх трудовитрат. При цьому користувачі будуть усунені від технічних деталей, таких як операційна система, інфраструктура і програмне забезпечення. Все це користувачам надається за допомогою хмарного сервісу. Міністерство оборони США вийшло з ініціативою підключити до нього не тільки свої відомства, але і промисловість, а також інші урядові установи. Вже до 2016–2020 років у формований простір повинні інтегруватися численні розрізнені хмарні платформи Міністерства оборони США, розвідувального співтовариства, військово-промислового комплексу, уряди і інші організації.

Постановка задачі. Важливим напрямком вдосконалення технологій захисту та систем інформаційної безпеки є протидія білатеральним загрозам, у яких суб'єкт та об'єкт процесів інформаційної взаємодії є потенційним носієм небезпечних впливів. У таких випадках необхідно використовувати моделі загроз, які ідентифікують потенційні уразливості як на рівні процесів контролю доступу до ресурсів гостьових операційних систем (ОС) або додатків, так і на рівні системних викликів гіпервізора, який сам може стати джерелом руйнівних впливів, 6 реалізуються шляхом порушення функціонування планувальника завдань або диспетчера обладнання. Виникаючі при цьому загрози необхідно не тільки оперативно виявляти, але і блокувати використовуються неавторизовані канали інформаційних впливів, які у середовищі хмарних обчислень зазвичай реалізуються в прихованому для гостьових ОС режимах [3.

Хмарні системи класу «інфраструктура як сервіс» можуть стати джерелом загроз порушення безпеки програмного забезпечення, що пов'язано з активним характером взаємодії суб'єктів і об'єктів доступу до інформаційних ресурсів і призводить до ризиків порушення цілісності та доступності програмних сервісів, що надаються в режимі віддаленого доступу. Особливу небезпеку надають загрози, які реалізуються всередині периметра безпеки комп'ютерної мережі, так як їх локалізація із застосуванням сучасних засобів захисту інформації [3].

Для боротьби з такими загрозами актуальною є розробка нових засобів захисту інформації, заснованих на методах оперативної ідентифікації потенційних вразливостей, що виникають як на рівні процесів контролю доступу до ресурсів гостьових ОС, так і на рівні системних викликів гіпервізора, які за певних умов самі можуть ставати джерелами різних видів руйнівних впливів.

Відповідно, виникає необхідність в розробці математичної моделі прихованих загроз інформаційної безпеки, в якій враховується поведінковий характер об'єктів інформаційної взаємодії.

Виклад основного матеріалу. На основі попереднього аналізу та оцінки впливу нових загроз на стан захищеності ресурсів середовищ хмарних обчислень випливає, що використання традиційних підходів не дозволяє вирішити проблему підвищення рівня захищеності середовища хмарних обчислень з урахуванням гнучкості, масштабованості (підтримки апаратних платформ різного класу) пропонованих програмно-технічних рішень

мінімізації витрат. Тому для створення ефективних механізмів захисту ПЗ в середовищі хмарних обчислень потрібна розробка нових моделей загроз і створення методів відображення комп'ютерних атак, які дозволяють оперативно ідентифікувати приховані і потенційно небезпечні процеси інформаційної взаємодії.

Для середовища хмарних обчислень однією з головних проблем управління є нерівномірність запиту ресурсів з боку клієнтів. Для згладжування нерівномірності надання сервісів, т.д. розподілу ресурсів між реальним апаратним забезпеченням і хмарним програмним забезпеченням, використовують проміжний шар серверної віртуалізації.

Захист самих віртуальних машин. На відміну від фізичної машини, коли віртуальна машина вимкнена, залишається можливість її компрометації або «зараження». Тим же, хто використовує сервіси хмарних обчислень, слід переконатися в тому, що провайдер має системи захисту інформації, які встановлені на серверах віртуалізації.

Одночасно проводиться оцінка небезпеки реалізації загрози, що визначається трьома параметрами:

- низька небезпека – якщо реалізація може призвести до загрози незначним негативних наслідків для суб'єктів персональних даних;
- середня небезпека – якщо реалізація може призвести до загрози негативних наслідків для суб'єктів персональних даних;
- висока небезпека – якщо реалізація може призвести до загрози значних негативних наслідків для суб'єктів персональних даних.

У середовищі хмарних обчислень головною умовою виступає повнофункціональна підтримка програмного забезпечення сторонніх виробників і можливість швидкого (гнучкого) налаштування окремих компонентів. Інформаційні системи даного класу на відміну від комунікаційних мереж спеціального призначення не можуть «існувати» в ізоляції з боку апаратно-програмних засобів контролю, забезпечення достовірності і захисту ПО. Слід зазначити важливу роль мереж в умовах глобалізації процесів навчань, розвитку Internet, технологій проведення відеоконференцій в режимі реального часу, розвитку партнерських науково-дослідних програм в рамках проектів ЮНЕСКО і ООН, співпраці комерційних і державних установ освітнього призначення.

Використання традиційних підходів не дозволяє вирішити проблему підвищення рівня захищеності середовища хмарних обчислень з урахуванням гнучкості, масштабованості (підтримка апаратних платформ різного класу) пропонованих програмно-технічних рішень і мінімізації витрат .

Розглянемо компоненти гіпервізора як джерело загрози при проведенні атак зловмисником з подальшим розповсюдженням шкідливого програмного забезпечення на серверах віртуалізації.

Користувачі можуть атакувати компоненти гіпервізора, посилаючи некоректні запити на обробку модулям програмного забезпечення гіпервізора і використовуючи недокументовані можливості системного і прикладного програмного забезепечення, встановленого на серверах віртуалізації Логіка виконання програм повинна контролюватися з точки зору відмови в обслуговуванні. Це підвищує ризики від реалізації прихованих погроз. не тільки функціональних можливостей, але і безпеки, яка оцінюється величиною ризику їх не документованої роботи. Для цього необхідно добре уявляти, що і як може загрожувати нормальному функціонуванню системи, що захищається. При цьому шкідливе прогамне забезпечення не здійснює блокування і знищення інформації, циркулюючої в системі, не перехоплює системні виклики гостьових ОС, а «вбудовується» безпосередньо на рівні планувальника завдань і диспетчера роботи з устаткуванням гіпервізора і може ушкоджувати програмному забезпеченні гіпервізора. Приховані погрози, що приводять до порушення роботи середовищі хмарних обчислень, реалізуються за допомогою дій з боку шкідливого програмного забезпечення, від яких немає захисту на рівні гостьової ОС.

Під реалізацією прихованих погроз маються на увазі використання механізмів створення і зміни контексту виконання потоків, за допомогою яких можуть передаватися дані від сутностей з високим рівнем безпеки до сутностей з низьким рівнем безпеки в обхід правил і може порушуватися стан захищеності самого гіпервізора.

Гіпервізор забезпечує ізоляцію різних ОС одна від одної, розділення і управління ресурсами. Гостьові ОС – це операційні системи віртуальних машин, що запускаються під управлінням гіпервізора.

У гіпервізорі, як і в будь-якій операційній системі, створюється множина сутностей (об'єктів і суб'єктів доступу) з різним рівнем безпеки. Операція породження суб'єктів $Create\left(Subi, Om\right) \to Subj$ називається породженням з контролем незмінності об'єкту, якщо для будь-якого моменту часу $t > t0$, в який активізована операція породження об'єкту $Create$, породження об'єкту $Subj$ можливо тільки при тотожності об'єкту-джерела щодо моменту $t0 : Om[t] = Om[t0]$, де Sub – суб'єкт, O – об'єкт доступу. У разі середовища хмарних обчислень суб'єкти і об'єкти доступу можуть мінятися ролями.

Тому для протидії прихованим погрозам в середовищі хмарних обчислень, в якому діє породження суб'єктів з контролем незмінності об'єкту, необхідно, щоб у момент часу $t0$ через будь-який суб'єкт до будь-якого об'єкту існували тільки потоки, що не суперечать умові коректності: монітор безпеки повинен реалізувати спеціальні механізми ідентифікації контексту контрольованих потоків даних як для суб'єктів, так і для об'єктів доступу, а будь-який суб'єкт доступу (ініціатор доступу) повинен використовувати тільки дозволені механізми доступу. З цією метою вводиться набір який підходить для створення об'єктів доступу, так і при породженні об'єктів у вигляді кортежу $(s, Ord, Context\_type)$, тобто формалізація операцій породження суб'єктів або об'єктів доступу представляється в наступному вигляді:

$$Create\left(Subi, Om, s, Ord, Context\_type\right) \to Subj, Create\left(Om, s, Ord, Context\_type\right) \to Oj.$$

При цьому породження нового суб'єкта доступу з номером j Sub_j можливо тільки за умови, що $Om[t] = O_m[to]$, де Sub - суб'єкт доступу, O_m - об'єкт доступу, j, m - номера об'єктів в запропонованій специфікації даного хмарного середовища.

Таблиці дозволених зв'язків об'єктів і суб'єктів доступу, за допомогою яких здійснюється контроль транзакцій операцій породження нових об'єктів, необхідно розширити на випадок прихованих погроз.

Предикативна функція ідентифікації прихованих погроз - це відображення 8-рівневої моделі операцій на множину його можливих станів - небезпечні, безпечні і невизначені. В цьому випадку модель прихованих погроз описується у вигляді розширеного кортежу :

$$\langle\ Source, Services, Measuring, \{proc\}, Actions, \{hv\}, \{vm\}, Security\ Roles\ \rangle,$$

де $Source$ - суб'єкт доступу або процес, джерело загрози;

$Services$ - набір шаблонів правил безпеки, використовуваних традиційними СЗІ (наприклад, правила фільтрації для МСЕ тощо);

$Measuring$ - пристрої, що встановлені на серверах віртуалізації і використовувані гостьовими операційними системами ВМ (диск, мережний контролер тощо), як об'єкт доступу;

$\{\ proc\ \}$ - множина суб'єктів впливу (шкідливий код гіпервізора, несертифіковані засоби віртуалізації і. т. п.);

$Actions$ $(дії)$ - множина суб'єктів впливу (шкідливий код гіпервізора, несертифіковані засоби віртуалізації і. т. п.); множина суб'єктів впливу (шкідливий код гіпервізора, несертифіковані засоби віртуалізації і. т. п.);

$\{hv\}$ - середовище ВМ у гіпервізорі, що представляє собою безліч компонентів $\mathrm{mod}\, i$;

$\{vm\}$ - об'єкти впливу (множина ВМ).

• *Security - Roles* - процедури багаторівневої рольової ПБ для протидії прихованим загрозам, які реалізуються у вигляді набору міток безпеки. Набір міток являють собою значення кортежу $(s, Ord, Context\_type)$..

В рамках пропонованої моделі погроз середовище хмарних обчислень розглядається як система взаємодії гіпервізорів, встановлених на серверах віртуалізації. В рамках направленої схеми «суб'єкт-дія-об'єкт» активний характер суб'єктів і об'єктів інформаційної взаємодії має на увазі та обставина, що вони можуть мінятися місцями. Розглянемо ситуацію, в якій зловмисник(суб'єкт) атакує сервер віртуалізації(об'єкт), модифікує компоненти гіпервізора шляхом реалізації нових погроз, приведених в таблиці 1

Таблиця 1

Перелік нових загроз, які виникають в середовищі хмарних обчислень

Перелік загроз	Наслідки
Загроза нестандартного виконання команд в гіпервізорі	Можливість отримання несанкціонованого доступу до ресурсів гіпервізору
Загроза порушення однозначності переходів станів при обміні інформацією між віртуальною машиною та гіпервізором	Можливість отримання несанкціонованого доступу до данних користувача іншої віртуальної машиши
Загроза модифікації програмного забезпечення гіпервізорі	Поширення шкідливого програмного забезпечення в середовищі хмарних обчислень

При цьому «заражені» гіпервізори, що знаходяться в одній або різних підмережах, стають учасниками атаки, тобто суб'єктами доступу, а запущеними під їх управлінням віртуальні машини користувачів - об'єктами.

Середовище хмарних обчислень може бути представлене у вигляді 8 - рівневої ієрархічної моделі.

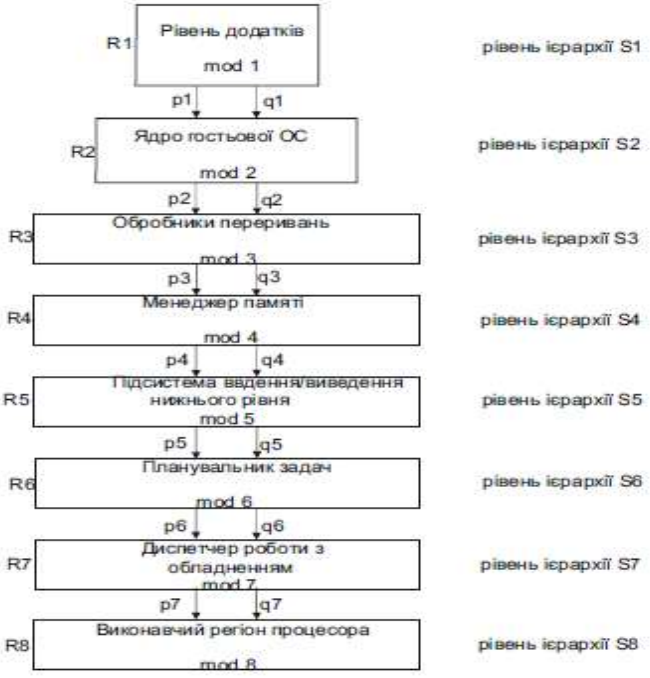


Рис. 1. Ієрархічна модель середовища хмарних обчислень

На рис. 1 використовуються такі позначення:

$R..R8$ – стан процесів; $S1$ – рівень додатків; $S2$ – рівень ядра гостьової ОС; $S3$ – рівень обробників переривань; $S4$ – рівень менеджера пам'яті гіпервізора; $S5$ – рівень підсистеми-введення виведення гіпервізора; $S6$ – рівень планувальника завдань гіпервізора; $S7$ – диспетчер роботи з обладнанням гіпервізора; $S8$ – рівень виконавчого процесора. На рівнях $S1-S5$ функціонують традиційні системи захисту інформації, які використовують набори правил контролю доступу, що відповідають вимогам політики безпеки. На рівнях $S6-S7$ реалізуються приховані для гостьових ОС загрози, а на рівні $S8$ здійснюється контроль виконання операцій. Лівими стрілками $p1-p7$ позначені переходи в мультиграфі транзакцій без зміни контексту виконання операцій. Правими $q1-q7$ позначені переходи зі зміною контексту виконання операцій, коли компонент $\mathrm{mod}\,i$ модифікований шкідливим програмним забезпеченням.

На основі запропонованої декомпозиції модель операцій можна конструктивно представити за допомогою мультиграфа транзакцій, який описує дозволені механізми ініціалізації процесів доступу до прикладних і системних інформаційних ресурсів. В результаті запропонованої формалізації опис прихованих загроз зводиться до введення контекстно-залежних переходів в мультиграфе транзакцій, тому для їх виявлення потрібно розробка ефективних алгоритмів ідентифікації стану як прикладних, так і системних процесів.

Висновки. Розроблена модель прихованих загроз, в якій враховується активний характер суб'єктів та об'єктів інформаційної взаємодії. Для формалізації опису даних процесів запропоновано модель операцій, виконуваних на різних рівнях функціонування середовища хмарних обчислень. В запропонованій моделі операцій різні компоненти гіпервізора розглядаються в якості потенційного джерела загроз інформаційній безпеці, які реалізується шляхом поширення шкідливого програмного забезпечення або ініціалізації процесів, що руйнують стан захищеності ресурсів середовища хмарних обчислень. За допомогою розробленої моделі запропоновано формалізований опис загроз, які формують послідовності запитів до некоректних програмним модулям гіпервізора або використовують недекларовані можливості системного і прикладного програмного забез.

Запропонований підхід до опису операцій заснований на класифікації ризиків порушення інформаційної безпеки та аналізі контексту виконання потоків команд, за допомогою яких можуть передаватися дані в обхід вимог прийнятої політики безпеки, що призводить до порушення захищеності ресурсів гіпервізора. В розробленій моделі носіями аналізованих операцій є множини об'єктів і суб'єктів доступу, яким присвоєно різні рівні безпеки.

ЛІТЕРАТУРА:

1. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №555/2015. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України" [Електронний ресурс] / П.О. Порошенко.
- Режим доступу http://www.president.gov.ua/documents/5552015-19443.

2. Муляр І.В. Аналіз проблем забезпечення функціональної безпеки інформаційних систем обробки даних /І.В. Муляр, А.В. Джулій, М.В. Костюк // Вимірювальна та обчислювальна техніка в технологічних процесах: Міжнародний науково-технічний журнал.-Хмельницький, 2013. - №1 -С. 133-138.

3. Козак І.В. Аналіз проблем захисту інформації в середовищі хмарних обчислень / І.В. Козак, С.О. Пашков, О.В. Огнєвий // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 51. – С.164-171

4. Моляков, А.С. KPROCESSOR_CID_TABLE факторинг – новый метод в теории компьютерного анализа вирусного кода и поиска программных закладок/ А.С. Моляков // Проблемы

информационной безопасности. Компьютерные системы. - СПб.: Изд-во Политех. Ун-та, 2009. - №1. - с. 17-19.

REFERENCES:

1. UKAZ PREZYDENTA UKRAYiNY #555/2015Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 2 veresnya 2015 roku "Pro novu redaktsiyu Voyennoyi doktryny Ukrayiny" [Elektronnyy resurs] / P.O. Poroshenko // Rezhym ostupu http://www.president.gov.ua/documents/5552015-19443

2. Kozak I.V. Analiz problem zakhystu informatsiyi v seredovyshchi khmarnykh obchyslen' / I.V. Kozak, S.O. Pashkov, O.V. Ohnyevyy // Zbirnyk naukovykh prats' Viys'kovoho instytutu Kyyivs'koho natsional'noho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2016. – Vyp. # 51. – C.164-171

3 . Mulyar I.V. Analiz problem zabezpechennya funktsional'noyi bezpeky informatsiynykh system obrobky danykh /I.V. Mulyar, A.V. Dzhuliy, M.V. Kostyuk // // Vymiryuval'na ta obchyslyuval'na tekhnika v tekhnolohichnykh protsesakh: Mizhnarodnyy naukovo-tekhnichnyy zhurnal. -Khmel'nyts'kyy, 2013.-#1 -S. 133-138.

4. Molyakov, A.S. KPROCESSOR_CID_TABLE faktoring – novyiy metod v teorii kompyuternogo analiza virusnogo koda i poiska programmnyih zakladok/ A.S. Molyakov // Problemyi informatsionnoy bezopasnosti. Kompyuternyie sistemyi. - SPb.: Izd-vo Politeh. Un-ta, 2009. - #1. - c. 17-19.

Рецензент: д.т.н., проф. Сбітнєв А.І.

Козак І.В., к.т.н., доц., Огнєвий О.В.

МЕТОД ПРОТИВОДЕЙСТВИЯ СКРЫТЫМ УГРОЗАМ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

По результатам проведеного анализа в статье доказывается актуальность разработки технологии противодействия попыткам изменить состояние защищенности информационных ресурсов в среде облачных вычислений. В результате проведенных авторами исследований сделан вывод о том, что перспективным перспективным направлением совершенствования технологий киберзащиты в среде облачных вычислений является разработка методов противодействия угрозам, реализуемым с помощью процессов, в которых субъекты и объекты информационного взаимодействия могут использовать различные каналы передачи данных, в том числе и скрытые. Показано, как реализация скрытых угроз позволяет вредоносному коду маскироваться под системный процесс в ущерб безопасности среды облачных вычислений с помощью блокировки, хищения, уничтожения или несанкционированной передачи информации.

Для борьбы с такими угрозами актуальна разработка новых средств защиты информации, основанных на методах оперативной идентификации потенциальных уязвимостей, возникающих как на уровне процессов контроля доступа к ресурсам гостевых ОС, так и на уровне системных вызовов гипервизора, которые при определенных условиях сами могут становиться источниками различных видов разрушительных воздействий.

Соответственно, возникает необходимость в разработке математической модели скрытых угроз информационной безопасности, в которой учитывается поведенческий характер объектов информационного взаимодействия. Также разработано модель информационного обеспечения для облачных вычислений, что позволяет представить формализованное описание информационных процессов в среде облачных вычислений в виде мультиграфа транзакций. На основе этих моделей разработан метод противодействия скрытым угрозам, основанный на контроле транзакций, соответствующих требованиям политики безопасности.

Ключевые слова: кибербезопасность, облачные вычисления, скрытые угрозы, защита информации.

Kozak I.V., Ph.D. Ohnevyj A.V.

METHOD OF THE COUNTERACTING THE HIDDEN THREATS IN THE CLOUD COMPUTING ENVIRONMENT

As a result of the analysis, the authors of this article prove the relevance of developing the counteracting technology to the attempts of changing the condition of protecting the information resources in the cloud computing environment. At the end of the research, authors made a conclusion that the promising direction of improving the cyberprotecting technology is to develop methods of counteracting the threats, which are realized through the processes in which subjects and objects of the information exchange may use different data transmission channels, including the hidden ones. Authors showed how the realization of hidden threats allows the harmful code to disguise as a systemic process, harming the security of the cloud computing environment with the help of blocking, theft, destruction or unauthorized transfer of information.

To fight such threats it is relevant to develop the new information security based on the methods of rapid identification of potential vulnerabilities arising at the level of processes of controlling the access to the resources of the guest OS and at the level of system hypervisor's calls, which under certain conditions can become sources of different types of destructive influence.

Consequently, there is a necessity to elaborate a mathematical model of hidden threats of the information security, which takes into account the behavioral nature of the information interaction of objects. Also the authors created the model of information support for cloud computing, which allows to introduce a formalized description of information processes in the cloud computing environment as a multigraph of transactions. On the basis of these models the researchers developed a method of counteracting the hidden threats, based on the control of transactions that meet the requirements of security policy.

Keywords: cybersecurity, cloud computing, hidden threats, protection of the information.

УДК 004.65

к.т.н. **Кольцов Р.Ю.** (ВІКНУ)

ІДЕНТИФІКАЦІЯ НЕВІДОМИХ СИСТЕМ КООРДИНАТ ЗА ДОПОМОГОЮ ДОДАТКУ ARCGIS - ARCMAP 10.2.

На основі аналізу впровадження сучасних інформаційних технологій у практику підготовки спеціалістів з географічних інформаційних систем і технологій встановлено, що не всі джерела геопросторової інформації (цифрова картографічна інформація) про місцевість та об'єкти на ній мають "правильну" прив'язку в системам координат, що може спричинити подальше хибне визначення та прив'язку координат, та їх використанням за призначенням. Розглянуто рішення по визначенню потрібної систем координат та прив'язку геопросторової інформації за допомогою основного додатку програми ArcGis - ArcMap.

Ключові слова: система координат, географічна інформаційна система.

Вступ. При виконанні робіт в програмному забезпеченні ArcGis завжди вказується система координат в якій повинні бути отримані представлені результати. Автоматизація обробки вимірювань потребує чіткого розуміння щодо систем координат, які використовуються при роботі на тій чи іншій території. Це дозволяє оптимально підбирати та використовувати відповідні модулі програмного забезпечення, задавати необхідні для перерахунку координат дані. Крім того, необґрунтоване застосування деяких систем координат призводить до суттєвих викривлень отриманої в них інформації. Інформація про

системи координат зазвичай присутня в джерелах даних, але не завжди. Наведене технічне описання програми допоможе правильно визначити систему координат, але якщо система координат невідома, при спробі додати шар в ArcMap буде отримано попередження: "У перерахованих нижче джерел даних відсутня інформація про просторову прив'язку". Дані можуть бути відображені в ArcMap, але не можуть бути спроектовані.

Мета статті. Метою статті є аналіз процесу знаходження потрібної системи координат для подальшого “правильного” використання геопросторової інформації та її прив’язка в програмному продукті ArcMap. Термін "система координат" може посилатися на дані, представлені у десятих долях градусів, або проекцію системи координат, виражену в метрах або футах. Термін "проекція" або PRJ є застаріли, але також використовується, хоча не є точним. Якщо у джерелі даних система координат визначена, то ArcMap може "миттєво" спроектувати дані в різні системи координат, але якщо система координат даних не визначена, то програма не зможе їх спроектувати, вона просто відобразить їх.

Основна частина. Для визначення системи координат в джерелі даних розглянемо наступний алгоритм на базі програмного продукту американської фірми ESRI – ArcGis, а саме його додатку ArcMap. Роботу розпочнемо з нової карти і завантажимо дані з невідомою системою координат. Дані не повинні мати певної системи координат, шейп-файли не повинні мати файлу проекції PRJ. Натиснемо правою кнопкою назву шару в таблиці змісту, виберемо Властивості (Properties), щоб відкрити діалогове вікно Властивості шару (Layer Properties), виберемо вкладку Джерело (Source), потім перевіремо экстент даних.

Якщо координати, які показані у вікні Экстент (Extent), виражені у десяткових градусах і довгота знаходиться в діапазоні від -180 до +180 градусів, а широта від -90 до +90 градусів, то ми маємо справу з географічною системою координат (датумом), який використовується для даних (наприклад, North American Datum (NAD) 1927 або NAD 1983).

Якщо система координат наших даних визначається як 'GCS_Assumed_Geographic_1', це неправильна система координат. Ця система координат була створена для того, щоб додаток ArcMap "думав", що дані зберігаються в десяткових градусах. Ми повинні визначити правильну систему координат для даних.

Якщо дані відносяться до території США, і показують экстент, координати в яких ліворуч від десяткової коми (крапки) мають 6, 7 або 8 цифр, можливо, що дані відносяться до системи координат State Plane або UTM, які є системами координат проекції. Якщо невідомі дані лежать у межах США, додамо в ArcMap дані для прив'язки. Ми можемо знайти відповідні дані в папці Reference Systems додатку ArcGIS. Її розміщення, як правило, знаходиться по наступній директорії: C:\Program Files\ArcGIS\Desktop10.2.

Увійдемо в папку Reference Systems і додамо файл usstpln83.shp. У таблиці змісту зайдемо до Шари (Layers) > Властивості (Properties), а потім вкладку Система координат (Coordinate System). В цьому розділі виберемо систему координат (Select a coordinate system) Зумовлені (Predefined) > Системи координат проекції (Projected Coordinate Systems) > State Plane. Знайдемо в папках відповідну проекцію State Plane і натиснемо кнопку Застосувати. Може з'явитися вікно "*Увага! Географічна система координат*", попереджаючи нас про те, що географічна система координат шару не збігається з географічною системою координат фрейму даних. Це може стати причиною неспівпадання від декількох метрів до декількох сотень метрів. Географічне (датум) перетворення може зменшити відхилення. Ми можемо виконати перетворення, запропоноване в діалоговому вікні або також перевірити інформацію про перетворення наступним чином:

- Натиснемо кнопку Перетворення (Transformations) на закладці Система координат (Coordinate System);

- Переконаймося, що відповідний метод трансформації доданий в спадаюче меню Використовуючи (Using). Наприклад, використовуючи NAD_1927 To NAD_1983_NADCON для переходу між NAD 1927 і NAD 1983 48 континентальних штатах, візьміть відповідний файл штату або регіону для перетворення в High Accuracy Reference Network (HARN).

Переберемо різні зони State Plane, поки файл usstpln83.shp не стане на місце і дані з невідомою системою координат не з'являться в правильному місці в межах відповідного штату.

Можна додати для деяких штатів файли PRJ, які є в папках State Systems, County National Systems і Grids. Якщо ваші дані знаходяться у одному з цих регіонів, занесених в ці папки, ви можете також використовувати їх файли PRJ.

Натиснемо кнопку OK у діалоговому вікні Властивості даних (Data Frame Properties). Перевіремо наскільки добре дані "сіли" на свої місця, збільшуючи до экстента шару і натискаючи інструментом Ідентифікувати (Identify) у місцях, де відображені дані. Якщо дані не "потрапили" на свої місця після застосування проекцій State Plane, спробуємо зробити те ж саме з допомогою проекцій UTM PRJ. Розгорнемо папку UTM. Відкриємо там по черзі всі папки, вибираючи файли проекцій UTM і натискаючи Застосувати (Apply) як було описано в попередніх кроках для проекції State Plane. Це буде корисно для нашого первинного визначення, в якій зоні UTM знаходяться наші дані. Для карти зон UTM, пошукаємо карту зон Web for UTM. Одне з посилань — UTM Grid Zones of the World compiled by Alan Morton. Координати UTM в метрах датума NAD 1983 і координати деяких точок датума WGS 1984 в континентальній частині США знаходяться в межах півметра один від одного. Дані в системі координат UTM в датумі NAD 1983 зміщені приблизно на 200 метрів на північ у деяких даних щодо датума NAD 1927. Там також може бути незначний зсув на схід чи захід між даними в цих двох датумах, але приблизно 200-метрову зміщення на північ або південь набагато більш відчутно. Різниця в 200 метрів є порівняно невелика; тим не менш, має значення, що ми використовуємо більш точні дані для визначення, який з датум NAD 1927 або NAD 1983 більш коректний для даних в проекції UTM. Коли коректна система координат знайдена, запам'ятаємо її ім'я та місце розташування, щоб ми змогли її застосувати, коли будемо використовувати інструмент *Визначити проекцію*.

Провівши процес визначення потрібної нам системи координат ми з легкістю зможемо орієнтуватися в геопросторовій інформації і виконувати поставлені завдання. Але виникає питання – визначити координати можна, але якщо в нас є відсканований аркуш карти і його потрібно прив’язати до однієї із систем координат, щоб по ній знаходити потрібну нам інформацію, то як це правильно зробити? Відповідь є.

Координатна (географічна) прив'язка в ArcMap здійснюється в кілька етапів, послідовність яких залежить від типу прив’язуваного матеріалу. Даний приклад ми і проілюструємо як один із найпростіших випадків, прив'язку тематичної карти, з нанесенням додаткової сітки координат, в даному випадку ми прив'язку здійснемо в географічну систему координат.

Даний приклад можна використовувати в якості уроку з координатної прив'язки карти в ArcGIS/ArcMap. Загальний вигляд панелей інструментів відповідає ArcGIS 10.2, дану методику прив'язки можна застосовувати і в інших версіях ArcGIS, при цьому зовнішній вигляд інструментів може відрізнятися від наведених у статті. В нашому випадку ми проведемо процес прив’язки на основі топографічної карти.

Підготовка растру. Ми відсканували карту з роздільною здатністю, достатньою для вирішення поставлених завдань. В технічній літературі рекомендовано повністю зберегти координатну сітку, якщо вона є і залишити позарамкове оформлення, якщо воно не дуже велике.

Координатна сітка. Якщо на карті не нанесена координатна сітка (наприклад присутні тільки на рамці), можна самостійно це зробити в графічному редакторі. Якщо карта дуже дрібного масштабу (країни, континенти), то це не завжди можливо, так як меридіани і паралелі в деяких проекціях не є прямими лініями, але так само вірно, що для карт часто точність так само не велика.

Завантаження даних. Завантажуємо відсканована карту по команді: File/add data. Запускаємо панель просторової прив’язки (View\Toolbars\Georeferencing). Натискаємо на

кнопку Таблиця (остання в панелі інструментів прив'язки). При цьому з'явиться порожня таблиця. Приберіть галочку у вікні "Автонастройка". Відключення автоналаштування означає, що в даному випадку, карта не буде автоматично трансформуватися після кожної нової точки прив'язки. За допомогою інструменту прив'язки (передостання кнопка), натискаючи на перетин координатних ліній (або будь-якій іншій точці з відомими координатами) на карті і вдруге натискаючи в будь-якому місці карти правою кнопкою миші, вибравши "Ввести координати", ввести правильні координати точки. Координати повинні вводитися у форматі DD.DDDDD (десяткові градуси), якщо ваші координати в іншому форматі, наприклад DD MM SS, необхідно перевести їх у потрібний формат.

Вибір моделі трансформації. Після розміщення всіх точок, в таблиці необхідно включити функцію "Автонастройка" (Рис.1). При цьому карта змінить розміри і положення орієнтуючись до прив'язки координат. При цьому точки прив'язки наблизяться до точок з відомими координатами. Якщо розставлено більше 6 точок, можна спробувати вибрати поліноміальну модель трансформації 2-го порядку враховуючи можливу кривизну ліній. Якщо перехід у цей режим призводить до очевидних сильних викривлень, рекомендується переглянути точки на предмет великої середньої квадратичної похибки і видалити їх, поки результат не стане задовільним. Повторіть цей крок для всіх або більшості точок з відомими координатами на карті, чим більше точок прив'язки, тим більш точно буде прив'язана наша карта. В таблиці зв'язків, з кожним новим натисканням, будуть з'являтися нові рядки, які при необхідності можна корегувати, або видаляти.

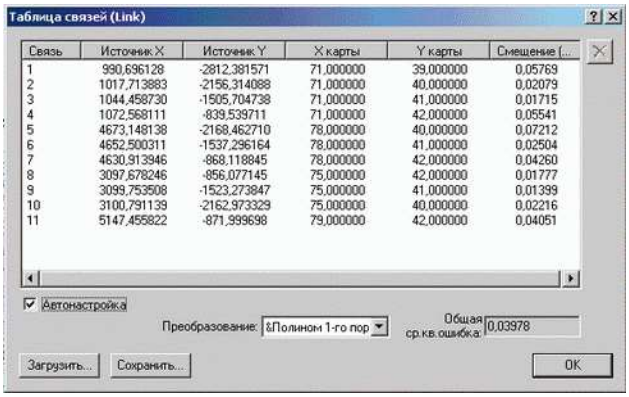


Рис. 1. Таблиця зв’язків

Перевірка. Для перевірки прив'язки можна завантажити існуючий шар або шейп-файл, про який відомо, що він правильно прив'язаний географічно і має ту ж систему координат (в даному випадку це межа країни в географічній системі координат). Звверніть увагу на розбіжність синьої лінії - кордони з векторного шару і червоної лінії - тієї ж кордону з самої карти (рис. 2).



Рис. 2. Розбіжність кольорів

Додаткова корекція. Для додаткового коректування прив'язаної карти, можна, використовуючи навігаційні інструменти (збільшити, зменшити і т. д.) додати додаткові точки прив'язки між прив’язуваного картою і відомими границями. Для спостереження за змінами розташування карти можна залишити опцію "Автонастройка" включеною. Невелика розбіжність карти і шару може бути присутня постійно. Для подальшого поліпшення прив'язки, можна також знайти зв'язку опорних точок, які розташовані на великій відстані і видалити їх, залишивши таким чином всі "хороші" зв'язки. Видалення проводиться в таблиці точок зв'язків.

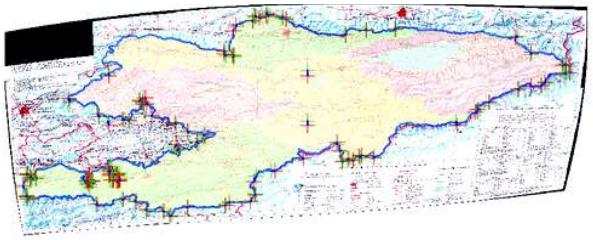


Рис. 3. Поліном 2-го порядку

Використання полінома 2-го порядку. Для більш тонкої корекції, якщо ми не досягли

ще збігу кордонів шару і прив’язуваного карти можна зробити наступне: вибрати в таблиці зв'язків в опції "Перетворення" значення "Поліном 2-го порядку". При цьому карта повинна ще більше спотворитися, "підійшовши" під лінії шейп-файлу. Далі потрібно ще раз переглянути зв'язку точок, можна додати нові і відкоректувати вже існуючі. У нас повинна вийти приблизно наступна ситуація як на рисунку 3.

При цьому потрібно пам'ятати, що повного збігу прив’язуваної карти і джерела координат (іншої карти, координатної сітки і т.д.) як правило досягти неможливо, через похибки сканування, невідповідності масштабів та інших джерел помилок.

Прив'язка вихідного растру. Після отримання остаточного варіанту прив'язки потрібно ще раз зберегти всі опорні точки в таблиці зв'язків. Після цього, потрібно видалити шар з яким ми працювали і завантажити шар без координат (якщо нам потрібна карта без намальованих осей). У новий файл ArcMap завантажуємо спочатку копію оригінальної карти, далі запускаємо модуль геоприв’язки, таблицю, завантажимо точки з збереженого нами файлу. Для перевірки можна також завантажити шейп-файл.

Збереження результатів. Після того, як ми переконаємося, що максимально наблизилися до результату - потрібно зберегти отримані результати. Для цього необхідно в модулі прив'язки вибрати кнопку - "Просторова прив'язка"/Трансформувати: де потрібно вказати кінцевий шлях та назву файлу. Так само в опції "розмір осередку" можна округлити число (наприклад до 0,001) у бік зменшення. Після натискання ОК ми отримаємо файл карти прив'язаний до системи координат, який можна буде використовувати з будь-якою іншою прив'язаною картою.

Висновки. Якщо ми підібрали і застосували відповідну систему координат, то всі дані, що додаються при подальшій роботі в ArcMap, будуть коректно сідати на свої місця. Якщо попередні кроки не привели до того, що дані в ArcMap "сіли" на свої місця, значить, ці дані були створені в “нестандартній” системі координат. Потрібно продовжити перебирати інші файли проекцій, використовуючи цю технологію. В кінці проведених робіт ще раз уважно вивчимо дані, щоб зрозуміти, в якій саме системі координат вони були створені. Використання вищезазначених рекомендацій дозволяє користувачу програмного забезпечення ArcGis провести процес визначення (індетифікації) “невідомої” системи координат та зробити подальшу прив’язку для роботи з даними.

ЛІТЕРАТУРА:

1. Зейлер М. Моделирование нашего мира: Руководство ESRI по проектированию базы геоданных / М.Зейлер; пер. с англ. – М.:СП ООО Дата+, 2004.

2. Степанов М.М., Уварова Т.В. Аналіз систем координат, що використовуються в Україні - Системи управління, навігації та зв'язку, 2011, випуск 4(20).

3. [Електронний ресурс] – http://resources.arcgis.com

4. [Електронний ресурс] Геоинформационные системы военного назначения. – marshal-group/geoinformacionniesistemi.html

5. [Електронний ресурс] http://gis-lab.info/qa/georef-ag.html

REFERENCES:

1. Zejler M. (2004) Modelirovanie nashego mira: Rukovodstvo ESRI po proektirovaniju bazy geodannyh / M.Zejler. – M.:SP OOO Data+. (*abstract in English*).

2. Stepanov M.M., Uvarova T.V. (2011) Analiz system koordynat, shho vykorystovujut'sja v Ukrai'ni. *Systemy upravlinnja, navigacii' ta zv'jazku*. 4. 20.

3. Sistema ArcGIS: http://resources.arcgis.com

4. Geoinformacionnye sistemy voennogo naznachenija: htth:// marshal-group/geoinformacionniesistemi.

5. Geograficheskie informacionnye sistemy i distancionnoe zondirovanie: http://gis-lab.info/qa/georef-ag.html.

Рецензент: д.т.н., проф. Сбітнєв А.І.

к.т.н. Кольцов Р.Ю.

ИДЕНТИФИКАЦИЯ НЕИЗВЕСТНЫХ СИСТЕМ КООРДИНАТ С ПОМОЩЬЮ ПРИЛОЖЕНИЯ ARCGIS - ARCMAP 10.2.

На основе анализа внедрения современных информационных технологий в практику подготовки специалистов географических информационных систем и технологий установлено, что не все источники геопространственной информации (цифровая картографическая информация) о местность и объектов на ней имеют "правильную" привязку в системе координат, что может повлечь за собой дальнейшее неверное определение и привязку координат, а также их использование по назначению. Рассмотрены решения по определению нужной систем координат для привязки геопространственной информации с помощью основного приложения программы ArcGis - ArcMap.

Ключевые слова: система координат, геоинформационные системы.

Ph.D. Koltsov R.Yu.

IDENTIFY UNKNOWN COORDINATE SYSTEMS THROUGH THE APPLICATION ARCGIS - ARCMAP 10.2.

The analysis of the implementation of modern information technology in the practice of training specialists in geographic information systems and technology found that not all sources of geospatial information (digital mapping information) of terrain and objects in it have a "right" to bind coordinate system may cause subsequent false and binding determination of coordinates and their intended use. Considered decisions needed to determine the coordinate system for linking geospatial information via the main application program ArcGis - ArcMap.

Keywords: coordinate system, geographic information system.

УДК 004.891

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц. **Джулій В.М.** (ХмНУ)
Романовська І.А. (ХмНУ)

МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИДАЧІ РЕЗУЛЬТАТУ ПОШУКУ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

У статті проведено аналіз ранжування сторінок у сучасних інформаційних пошукових системах. Розглянуто одну з основних складових ранжування – критерій PageRank. За останні роки розвитку інформаційних технологій він істотно вплинув на створення списку авторитетності сторінок. Завдання цього критерію полягає у визначенні так званої «ваги» сторінки, яка вираховується за відповідною формулою: пріоритетним є врахування зв'язків між сторінками – їхніх посилань. Чим більше посилань є на сторінку, тим більша її «вага» і вище вона стоїть у видачі результатів пошукової системи. Саме ці зв'язки є головною складовою формули обрахунку, вони поділяються на внутрішні та зовнішні. Проблема виникає з внутрішніми зв'язками, тому що вони дають посилання одне на одного, створюючи при цьому цикл посилань, що штучно збільшує «вагу» сайту з кожним кроком перевірки. Для вирішення проблем циклічності та штучного збільшення авторитетності пропонується визначення альтернативного показника TruePageRank, який відрізняється такими особливостями: посилання, які виходять з певної сторінки, не враховуються; в процесі обчислення TruePageRank вихідна структура зв'язків між сторінками перетворюється в антициклічний граф, в якому посилання, що утворюють циклічні зв'язки, не враховуються і увага приділяється прямим посиланням. При цьому об'єктивне значення авторитетності не втрачається, тому що знімається лише штучне збільшення значення. Для нового критерію потрібні ті самі значення, тобто не потрібно шукати нову інформацію.

TruePageRank – ще один з методів обробки вихідних даних, що дозволяє отримати альтернативний показник авторитетності сторінки, який досить об'єктивно відображає її інформаційну цінність.

Ключові слова: пошук, ранжування, PageRank, посилання, сайт, інформація.

Вступ. Кількість інформації в мережі Інтернет зростає з кожним днем все швидше, але, на жаль, цього не можна сказати про її якість. Користувач у пошуках потрібної інформації може провести все життя, якщо тільки випадково не знайде шуканий матеріал, єдиний вихід для нього – скористатися пошуковими системами, які зберігають інформацію про адреси і зміст веб-сторінок. Пошукові машини намагаються вирішити проблему – серед сотень однотипних документів вибрати кращий, за цим усім стоїть багато алгоритмів та функцій, які наявні у кожній пошуковій системі, і в кожній вони відрізняються. Але у всі вони характеризуються критерієм ранжування. У наш час використовуються текстові та довідкові критерії ранжування сторінок при пошуку. Перші визначають доречність («релевантність») документа виходячи з наявності слів запиту в тексті і заголовках сторінки. Однак наявність великої кількості документів може знецінити витончені механізми розрахунку релевантності, що базуються тільки на вмісті сторінки. Це і відбулося, коли власники сайтів зрозуміли, яку вигоду вони отримують від цільових відвідувачів, яких безкоштовно надають пошукові системи. Якість пошуку зіпсувалася, кількість документів зросла – «релевантний» документ стало дуже легко створити.

Постановка завдання. З метою поліпшення якості пошуку частину роботи з визначення «хороших», «важливих» документів побічно поклали на веб-майстрів Мережі. Розміщуючи посилання на зовнішній сайт, розробник ніби рекомендує його відвідувачам – саме цю особливість Інтернету вирішили використовувати для поліпшення якості пошуку. Підвищена вагомість документа визначається, таким чином, з урахуванням посилань ззовні на сайт, що містить цей документ.

Однак при врахуванні цитованості ресурсу виникають деякі труднощі. Кількість зовнішніх посилань на сайт не підходить для подання цитованості – з появою безкоштовних

хостингів кількість посилань дуже легко збільшити. Але важливість таких посилань нікчемна порівняно з посиланнями з відомих ресурсів. PageRank і є таким параметром важливості, він показує цитованість сторінки. Щодо цього критерію свого часу було висловлено багато різних і часто суперечливих думок, які заперечують вагомість PageRank. Розробники і промоутери сайтів прагнуть максимізувати його значення для створюваних інформаційних ресурсів.

Досить поширеним явищем в Інтернеті є ситуації, коли в структурі посилань сайту зустрічаються циклічні зв'язки, в тому числі і зворотні циклічні зв'язки. Наявність таких зв'язків не тільки ускладнює процес розрахунку показника авторитетності, а й істотно знижує його роль як індикатора семантичної значущості певної сторінки. При розрахунку значення показника PageRank частина ваги, переданої сторінкою A сторінці B під час однієї ітерації, повертається назад сторінці A під час наступної ітерації. Так виникає проблема циклічності. Під проблемою циклічності мається на увазі наявність у структурі посилань так званих штучних циклічних зв'язків. Крім них існують також об'єктивні (природні) циклічні зв'язки, але вони меншою мірою впливають на проблему обчислення авторитетності за допомогою PageRank. Штучні циклічні зв'язки передбачають навмисне, тобто штучне збільшення значення показника авторитетності PageRank з метою його підвищення. Якщо брати до уваги ступінь важливості вхідних посилань на сторінки сайту, то при розрахунку авторитетності більшу роль мають відігравати прямі зв'язки, ніж циклічні.

Виклад основного матеріалу дослідження. Сучасні пошукові системи Інтернету в процесі обробки запитів користувачів застосовують досить складні алгоритми ранжування документів (точніше, посилань на ці документи), які видаються як результати пошуку. Деякі фахівці говорять про кілька десятків і навіть про сотні критеріїв упорядкування, використовуваних у різних поєднаннях [1].

Для початку розглянемо сам процес ранжування документів. Ранжування – послідовне розміщення чогось, у нашому випадку – це розміщення шуканих сторінок у видачі пошукової системи. Фактори, що впливають на ранжування, поділяються на статичні, динамічні і власні. Статичні фактори не залежать від запиту до пошукової системи. Динамічні фактори залежать від запиту і поділяються на внутрішні (організація документа) і зовнішні (ранжування посилань). Власні належать до самої системи. Зупинимося на статичних факторах. Хорошим прикладом є критерій PageRank [2]. Порядок здійснення ранжування має такий вигляд:

- Знайти всі сторінки, що відповідають ключовим словами пошуку.
- Сортувати відповідно до «сторінкових факторів», таких як ключові слова.
- Врахувати текст посилань на сторінки.
- Відкоригувати результати з даними PageRank.

PageRank – це система, що базується на алгоритмі, який дозволяє визначати цифрову «вагу» кожного елемента мережі пов'язаних документів для з'ясування важливості кожного елемента у відношенні до іншого. Значення показника PageRank враховується в процесі розрахунку підсумкової релевантності документа при формуванні видачі пошуковою системою у відповідь на запит користувача [2].

Формула розрахунку PageRank має такий вигляд:

$$PR(A) = (1 - d) + d(PR(T1)/C(T1) + ... + PR(Tn)/C(Tn)), \quad (1)$$

де $PR(A)$ – «вага» PageRank сторінки A (та «вага», яку ми хочемо визначити);

d – коефіцієнт затухання, що відображає, яку частку «ваги» може передати сторінка-донор на сторінку-акцептор. Зазвичай його приймають рівним 0,85, це означає, що сторінка може передати 85% «ваги»;

$PR(Ti)$ – PageRank сторінки, яка вказує на сторінку A ;

$C(Ti)$ – кількість посилань на сторінку;

PR(Tn)/C(T n) A – означає, що дія виконується для кожної сторінки, яка вказує на сторінку A .

У публікаціях найчастіше згадуються такі методи обчислення PageRank [2]:

- ітераційний;
- матричний;
- функціональний.

Ітераційний метод розрахунку PageRank

Цей метод найбільш часто використовується в практиці демонстраційних обчислень. Являє собою метод розв'язання системи рівнянь, що визначають PageRank сторінок:

1) вибирається геометрія сайту, розставляються посилання, формується система рівнянь шляхом запису формули (1) для кожної сторінки;

2) задаються початкові значення PageRank для кожної сторінки, вони можуть бути будь-якими;

3) розраховується новий набір значень PageRank за рівнянням виду (1), виходячи з наявного поточного набору значень;

4) розраховується середній PageRank по всьому набору сторінок, PageRank кожної сторінки ділиться на отриману величину; в результаті середній PageRank стає рівним одиниці;

5) якщо набір значень PageRank змінився порівняно з вихідним набором кроку 3, повертаємося до кроку 3; якщо цього не відбулося, то розрахунок закінчується.

Матричний метод розрахунку PageRank

Нижче подано матрицю зв'язків (рис. 1), матрицю можна помножити на вектор значень PageRank m-го кроку ітерації, отриманий вектор помножити на d, додати одиничний вектор, помножений на $(1-d)$, і отримати наступне наближення вектора PageRank з номером $m+1$, який потрібно пронумерувати (щоб сума проекцій вектора PageRank дорівнювала N). При навичках роботи з математичними програмами цей спосіб може бути більш зручним.

	1	2	3	4
1	0	1/3	1/3	1/3
2	0	0	1/2	1/2
3	0	0	0	1
4	1	0	0	0

Рис. 1. Матриця зв'язків

На рисунку 1 сторінка 1 посилається на 2, 3, 4; сторінка 2 – на 3 і 4; сторінка 3 – на 4, а 4 – на 1. Наведена матриця містить значення $Mij = 1/Cj > i$, тобто значення в кожному осередку розділене на загальну кількість посилань Cj на сторінці j.

Функціональний метод розрахунку PageRank

Суть цього методу полягає в тому, щоб розрахувати стабільні значення PageRank, не застосовуючи ітераційних методів.

Зауважимо, що у функціональному методі міститься не одна, а дві якісних відмінності від ітераційних методів:

- до розгляду залучаються кількісно невизначені значення PageRank зовнішніх (у відношенні до розглянутого сайту) сторінок.
- використовується неітераційний метод розв'язання системи лінійних алгебраїчних рівнянь, що визначає PageRank для сторінок розглянутого сайту. Залучення до розгляду «вхідного» потоку авторитетності являє собою спробу врахування впливу зовнішніх сайтів на PageRank конкретного сайту, розглянутого ізольовано від мережі. При цьому «вхідний», зовнішній, PageRank конкретної сторінки розглядається як інтегрований потік – він символізує не одне, а певну кількість зовнішніх посилань. У загальному випадку, природно,

потрібно враховувати «вхідний» PageRank для всіх сторінок розглянутого сайту, а не тільки для головної сторінки.

Деякі особливості дозволяють зробити висновок про те, що функціональний метод обчислення PageRank – це гарне теоретичне рішення, придатне для наочних ілюстрацій у простих випадках, коли розглядаються окремі сайти, але не більше. Для аналізу великих фрагментів мережі Інтернет цей метод не придатний [3].

Типовими структурами зв'язків усередині сайту є:

- ієрархічна (рис. 2);
- циклічна (рис. 3);
- «широке зв'язування» (рис. 4).

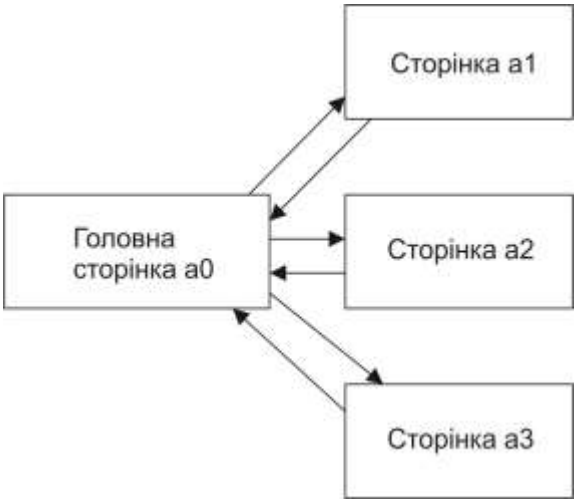


Рис. 2. Ієрархічна структура

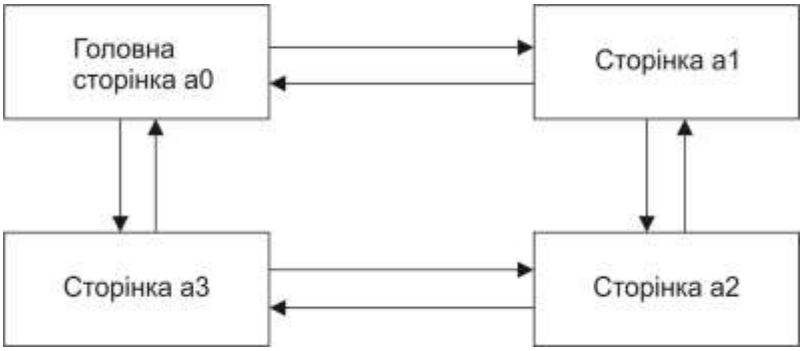


Рис. 3. Циклічна структура

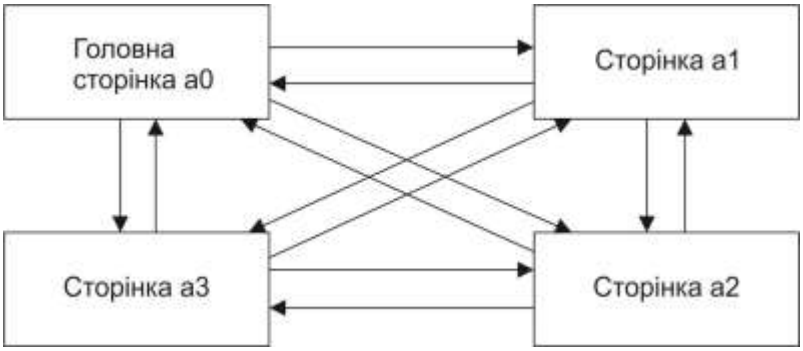


Рис. 4. Структура «широке зв'язування»

Вже досить часто стали зустрічатися проблеми циклічності, а саме так званої штучної циклічності. Цей фактор не рідко враховується при створенні сайту з метою його просування. Наявність природних циклічних зв'язків є наслідком прагнення оптимізувати структуру сайту і використовувати існуючий у мережі готовий інформаційний матеріал. Такі об'єктивні циклічні зв'язки становлять невід'ємну частину структури сайту. Якщо брати до уваги ступінь важливості вхідних посилань на сторінки сайту,то при розрахунку авторитетності більшу роль мають відігравати прямі зв'язки, ніж циклічні. Розглянемо приклад: нехай два сайти мають приблизно однакові суми значень показників авторитетності сторінок (PRA = PRB) (рис. 5, рис. 6).

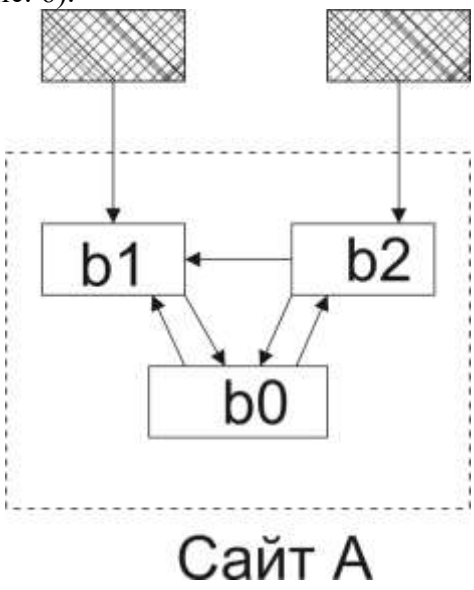


Рис. 5. Зв'язки сайту A

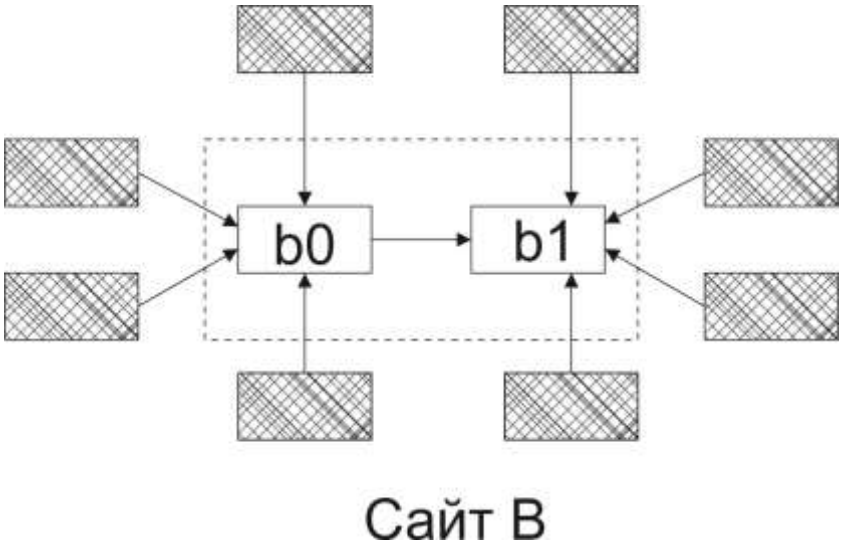


Рис. 6. Зв'язки сайту B

Величина значення авторитетності сайту A досягається завдяки циклічним зв'язкам між сторінками, з урахуванням того, що прямих зв'язків (як внутрішніх, так зовнішніх) мало. Величина значення авторитетності сайту B , навпаки, досягається завдяки прямим зв'язкам. Прямі вхідні посилання (зовнішні – з інших сайтів) семантично більшою мірою підкреслюють авторитетність сторінок, а отже, сайту в цілому. Авторитетність сайту

визначається кількістю вхідних посилань на цей сайт, а не внутрішньою структурою посилань. Отже, значення авторитетності сайту B має перевищувати значення авторитетності сайту A. Алгоритм обчислення авторитетності PageRank не має на увазі вирішення цього протиріччя ($PRA = PRB$).

Для вирішення проблем циклічності і штучного збільшення значення авторитетності можна розробити альтернативний показник TruePageRank, який відрізняється такими особливостями:

- вихідні посилання з певної сторінки не враховуються;
- у процесі обчислення TruePageRank вихідна структура зв'язків між сторінками перетворюється в ациклічний граф, у якому посилання, що утворюють циклічні зв'язки, не враховуються. Ця особливість приводить до того, що в інформаційних ресурсах Інтернету виключаються з розгляду численні внутрішні посилання, при цьому відбувається відмова як від штучних циклічних зв'язків, так і від об'єктивних, і увага приділяється прямим посиланням, при цьому об'єктивне значення авторитетності не губиться, тому що знімається лише зміна значення;
- у результаті викреслювання вихідних посилань у структурі зв'язків утворюється термінальна ситуація, яка характеризується відсутністю вихідних посилань, на конкретний сайт з безлічі сторінок і означає закінчення обчислення значення TruePageRank на певному етапі процедури.

Загальна формула для розрахунку показника авторитетності має такий вигляд:

$$NPRb = (1 - d) + d(NPRi(A[b])/Ci + ... + NPRn(A[b])/Cn), \quad (1)$$

де $NPRb$ – значення показника авторитетності сторінки;

d – коефіцієнт загасання (ймовірність того, що користувач, який прийшов на сторінку, перейде по одному з посилань на цій сторінці, а не припинить подорож по мережі, зазвичай встановлюється рівною 0,85);

$NPRi$ – значення показника авторитетності i-ї сторінки, що посилається на сторінку b;

Ci – загальна кількість посилань на i-ту сторінку;

$NPRn$ – значення показника авторитетності n сторінки, що посилається на сторінку b;

Cn – загальна кількість посилань на n сторінку;

$A[b]$ – поточна матриця зв'язків між сторінками, що відповідає певному етапу процедури.

З метою послідовного аналізу алгоритму обчислення TruePageRank розглянемо приклад розрахунку показника авторитетності однієї зі сторінок сайту, що містить таку структуру посилань (рис. 7):

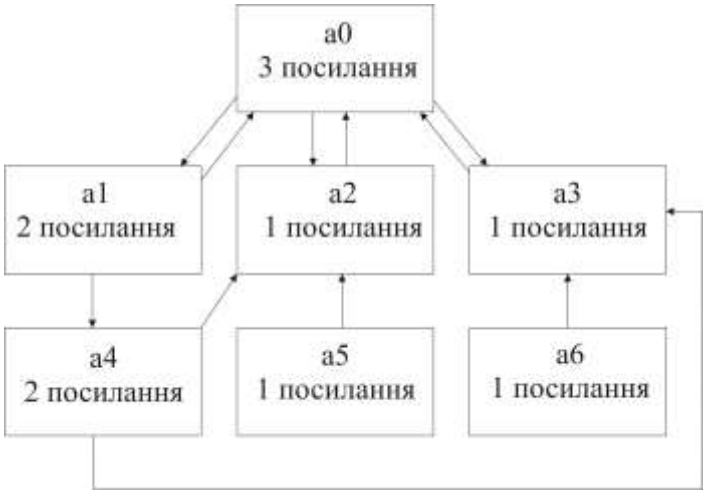


Рис. 7. Структура посилань сайту

Структура посилань, зображена на рис. 7 містить зворотні й циклічні зв'язки. Метою розрахунку авторитетності сторінки за допомогою алгоритму TruePageRank є запобігання впливу зворотних і циклічних зв'язків на шуканий результат і запобігання штучному збільшенню показника авторитетності сторінки.

Висновки.У статті розглянуто методи роботи ранжування сторінок та їхній вплив на авторитетність сторінки і результати пошуку. Також наведено формальний опис критерію PageRank, формулу його розрахунку. Виділено циклічну структуру зв'язків та недолік в роботі з циклічними посиланнями, а саме врахування з однаковим коефіцієнтом як прямих, так і циклічних зв'язків. Це призводить до неправильного визначення «ваги» сайту і дає можливість штучно збільшувати авторитетність сторінки. У зв'язку з цим запропоновано новий метод ранжування – TruePageRank та його модифіковану формулу. Подаються алгоритм роботи та рисунки у вигляді блок-схем Планується розробити вдосконалений TruePageRank, який буде відкидати циклічні зв'язки та враховувати тільки прямі посилання із сайтів, що значно змінить показники результатів авторитетності та не допустить штучного підвищення «ваги» PageRank.

ЛІТЕРАТУРА:

1. Муляр І.В. Адаптивний метод впорядкування інформаційного забезпечення з використанням пошукової функції // Зб. наук. праць Військового інституту Київського НУ ім. Тараса Шевченко. – К.: ВІКНУ, 2011. – Вип. №33. – С. 192-196.

2. Райдингс К., Садовский А. Растолкованный PageRank, или Все, что вы всегда хотели знать о PageRank [Электронный ресурс] / К. Райдингс, А. Садовский. – Режим доступа: http://digits.ru/ articles/promotion/ pagerank.html (дата звернення 10.09.2016).

3. Сбітнєв А.І., Алгоритм пошуку семантично подібних документів / А.І Сбітнєв, С.В. Лєнков, В.М Джулій., І.В Муляр., Л.В. Охрамович // Науково-практичний журнал «Сучасні інформаційні технології у сфері безпеки та оборони». – Київ, 2013. - №2(17). – С. 24 – 29.

4. Трофименко Е. PageRank: иерархия и обмен ссылками [Электронный ресурс] / Е. Трофименко. – Режим доступа: http://promosite.ru/articles/pagerank-exchange.php (дата звернення 12.09.2016).

REFERENCES:

1. Mulyar I.V. Adaptyvnyy metod vporyadkuvannya informatsiynoho zabezpechennya z vykorystannyam poshukovoyi funktsiyi // Zb. nauk. prats' Viys'kovoho instytutu Kyyivs'koho NU im. Tarasa Shevchenko. – K.: VIKNU, 2011. – Vyp. – №33. – S. 192-196

2. Raydynhs K., Sadovskyy A. Rastolkovannыy PageRank, yly Vse, chto vы vsehda khotely znat' o PageRank [Эlektronnыy resurs] / K. Raydynhs, A. Sadovskyy. – Rezhym dostupa: http://digits.ru/ articles/promotion/ pagerank.html (data zvernennya 10.09.2016).

3. Sbitnyev A.I., Alhorytm poshuku semantychno podibnykh dokumentiv / A.I Sbitnyev, S.V. Lyenkov, V.M Dzhuliy., I.V Mulyar., L.V. Okhramovych // Naukovo-praktychnyy zhurnal «Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony». – Kyyiv, 2013. – №2(17). – S. 24 – 29.

4. Trofimenko E. PageRank: ierarhija i obmen ssylkami [PageRank: hierarchy and link exchange]. Available at: http://promosite.ru/articles/pagerank-exchange.php (Accessed 12 September 2016).

Без рецензії.

д.т.н., проф Ленков С.В., к.т.н., доц. Джулий В.Н., Романовская И.А.

МЕТОД ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ВЫДАЧИ РЕЗУЛЬТАТА ПОИСКА В ИНФОРМАЦИОННОЙ СРЕДЕ

В статье проведен анализ ранжирование страниц в современных информационных поисковых системах. Рассмотрены одни из основных составляющих ранжирование - критерий PageRank. За последние годы развития информационных технологий он существенно повлиял на

создание списка авторитетности страниц. Задача этого критерия заключается в определении так называемого «веса» страницы, который рассчитывается по соответствующей формуле: приоритетным является учет связей между страницами - их ссылок. Чем больше ссылок является на страницу, тем больше её «вес» и выше она стоит в выдаче результатов поисковой системы. Именно эти связи являются главной составляющей формулы расчета, они делятся на внутренние и внешние. Проблема возникает с внутренними связями, так как они дают ссылки друг на друга, создавая при этом цикл ссылок, искусственно увеличивает «вес» сайта с каждым шагом проверки. Для решения проблем цикличности и искусственного увеличения авторитетности предлагается определение альтернативного показателя TruePageRank, который отличается следующими особенностями: ссылки, которые выходят с определенной страницы, не учитываются; в процессе вычисления TruePageRank исходная структура связей между страницами превращается в антициклических граф, в котором ссылки, образуют циклические связи, не учитываются и внимание уделяется прямой ссылке. При этом объективное значение авторитетности не теряется, потому что снимается только искусственное увеличение значения. Для нового критерия нужны те же значения, то есть не нужно искать новую информацию.

TruePageRank - еще один из методов обработки исходных данных, позволяет получить альтернативный показатель авторитетности страницы, который достаточно объективно отражает её информационную ценность.

Ключевые слова: поиск, ранжирования, PageRank, ссылки, сайт, информация.

Prof. Lenkov S.V., Ph.D. Dzhuliy V.N., Romanovska I.A.

METHOD OF INCREASING THE EFFICIENCY OF THE ISSUANCE OF A SEARCH RESULT IN THE INFORMATION ENVIRONMENT

This article provides an analysis of ranking pages in modern informative search systems. Considered one of the main components of the ranking - the criterion PageRank. In recent years, IT development was significantly influenced the creation of the list of authority pages. The purpose of this criterion is to determine the so-called "weight" of the page, which is calculated by the appropriate formula: the priority is the consideration of the links between pages - their links. The more links there are on a page, the higher its "weight" and it is higher in issuarance of search system's results. These links are the main components of the calculation formula, they are divided into internal and external. There is a problem with the internal connections, because they provide a link at each other, creating a cycle of links that artificially increases the "weight" of the site with each step of verification. To resolve the cyclical problems and artificial increase of credibility is proposed the determining of alternitive index TruePageRank, which is characterized by the following features: links, which come from a particular page do not count; in the process of calculating PageRank the original structure of links between pages is converted into an anti-cyclical graph in which the links are forming cyclic connections, is not considered and focuses on the direct link. The objective determination of credibility isn't lost because only the artificial increase in value is removed. The new criteria requires the same values, that is not necessary to search for new information.

TruePageRank - is another method of processing of output data, allowing you to get the alternative index of page's authority, which is quite objectively reflects its information value.

Keywords: search, ranking, PageRank, link, website, information.

УДК 621.396.1
к.т.н., с.н.с. **Міночкін Д.А.** (НТУУ «КПІ»)

АНАЛІЗ МЕХАНІЗМІВ КЕШУВАННЯ КОНТЕНТУ В БЕЗПРОВОДОВИХ МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ

З розвитком технологій послуги мобільного зв'язку змінюють акцент з послуг, які орієнтовані на встановлення з'єднання, на послуги, які орієнтовані на передачу контенту. Одним із можливих напрямків розвитку архітектури мобільних мереж є створення безпроводових мереж, які орієнтовані на передачу контенту. Одним із підходів для зменшення навантаження на базову мережу оператора та зменшення затримки передачі в таких мережах є кешування найбільш популярного контенту на ділянці «останньої милі» - базових станціях (БС) та кінцевих терміналах користувачів (КТ). На відміну від проводових мереж, унікальною властивістю безпроводових мереж, які орієнтовані на передачу контенту, є мобільність користувачів. Тому, в роботі розглядаються основні властивості моделі мобільності користувачів та можливість використання цієї додаткової інформації для збільшення ефективності механізмів кешування.

Ключові слова: кешування, безпроводові мережі, мобільність.

Вступ. В останні роки йде швидке зростання трафіку, що припадає на мобільну передачу даних, як наслідок збільшення кількості мобільних пристроїв, таких як смартфони та планшети. Зокрема, послуги мобільного зв'язку змінили направленість з послуг, які орієнтовані на встановлення з'єднання (наприклад, телефонні дзвінки) на послуги, які орієнтовані на передачу контенту (наприклад, передача медіа файлів або відео трансляції). Основним напрямком забезпечення зростаючих потреб пропускної здатності мережі є її ущільнення, тобто розміщення більшої кількості точок доступу чи базових станцій (БС). Не зважаючи на те, що це дозволить збільшити пропускну здатність перспективних стандартів 4G та 5G, такий підхід створить значне навантаження на опорну мережу оператора, що з'єднує точки доступу. Таким чином, оператор мобільного зв'язку буде вимушений витратити значні кошти на модернізацію опорної мережі для передачі мобільного трафіку з мультимедійним контентом. Однак, така модернізація може бути економічно не вигідною у зв'язку з тим, що цей тип трафіку характеризується імпульсністю та регіональністю. Альтернативним підходом може служити використання безпроводових мереж, що орієнтовані на передачу контенту з підтримкою кешування.

На сьогодні, пристрої що знаходяться на «останній милі», такі як БС та кінцеві термінали користувачів (КТ), мають пам'ять великих об'ємів, що може використовуватись для зберігання «популярного» контенту, що найбільш часто запитується користувачами. Зі зменшенням вартості пристроїв зберігання даних великого об'єму, з кожним роком зростає економічна ефективність використання механізмів кешування порівняно з прокладанням нових високошвидкісних каналів для опорної мережі оператора зв'язку [1]. Більш того, об'єми пам'яті пристроїв зберігання даних на мобільних КТ також зростають, що потенційно може бути використано для кешування. Такий підхід дозволить зменшити затримки передачі даних та перевантаження опорної мережі [2], так як користувачі зможуть отримати необхідні файли від БС, що їх обслуговує, або від інших користувачів, що знаходяться в зоні досяжності, без необхідності використання опорної мережі оператора зв'язку.

Створення проводових мереж, що орієнтовані на контент, вже розглянуто та реалізовано. В таких мережах частини контенту безпосередньо маршрутизуються та доставляються на пакетному рівні, а пакети з контентом автоматично кешуються на маршрутизаторах на шляху доставки. Для безпроводових мереж, широкомовна природа радіоканалу принципово вплине на механізми кешування та доставку файлів. Особливістю безпроводових мереж є мобільність користувачів. Вона ускладнює розробку механізмів кешування в мережах, що орієнтовані на передачу контенту, однак її можна використати для отримання додаткової інформації, яка може бути використана для кешування, як, наприклад, мобільність була використана для модернізації протоколів маршрутизації в епізодичних

мережах [3]. Вплив мобільності на механізми кешування розглядається лише частково [4], і більшість досліджень проводиться з фіксованою топологією мережі.

Тому, метою даної роботи є аналіз механізмів кешування в безпроводових мережах, які орієнтовані на контент, з урахуванням мобільності користувачів.

Основна частина. Розглянем безпроводову мережу з підтримкою кешування, яка зображена на рис. 1.

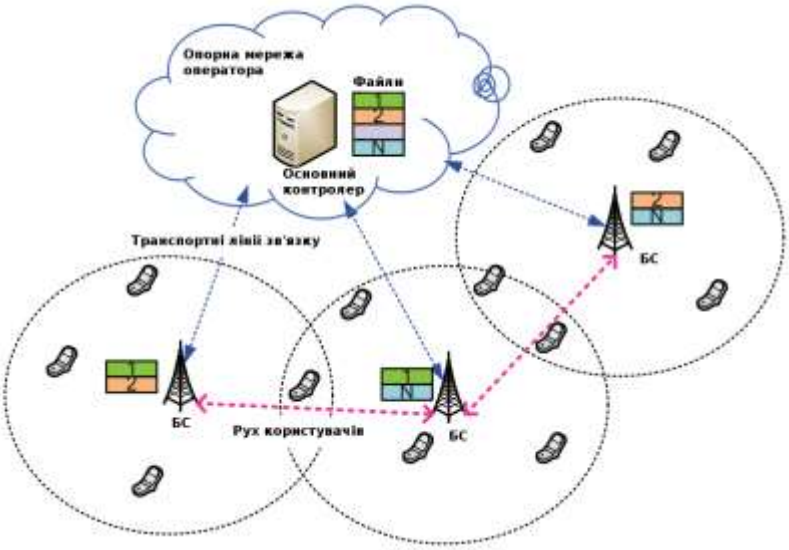


Рис. 1. Безпроводова мережа з підтримкою кешування

Основною проблемою, що необхідно вирішити при розробці механізму кешування є визначення того, яку інформацію та в якому місці кешувати. Робота механізму кешування може залежати від деякої додаткової інформації, яка може бути довгостроковою, тобто зібраною на основі спостережень впродовж тривалого відрізку часу (наприклад, статистика запитів від користувачів, середній час перебування в зоні однієї БС та середній час безпосереднього зв'язку між КТ), та короткостроковою, тобто заснованою на миттєвих змінах важливих параметрів (наприклад, поточна інформація про стан каналу зв'язку або місцезнаходження абонента в реальному часі). Збір довгострокової інформації вимагає зазвичай менше ресурсів, в той час коли короткострокова інформація більш ефективна, але потребує постійного оновлення. Проаналізуємо деякі задачі, які виникають при вирішенні проблеми розробки механізмів кешування в залежності від своєчасності наявної інформації.

Розміщення кешованого контенту зазвичай базується на довгостроковій інформації про систему, і визначає способи ефективного попереднього кешування контенту у доступному сховищі. Для зменшення службового трафіку оновлення додаткової інформації та кешування контенту може виконуватись з низькою періодичністю. Зазвичай, припускається, що довготривалий розподіл популярності деякого контенту відомий апріорі, а топологія мережі є фіксованою. В літературі розглядається механізм кешування з розміщенням кешованого контенту на БС. Зокрема, без кооперації між БС, найліпшою стратегією є зберігання найбільш популярних файлів [5-6].

Розміщення кешованого контенту на КТ доже дозволити користувачам завантажувати необхідний контент більш ефективно за допомогою безпосереднього зв'язку з іншими користувачами з технологією Device to Device (D2D). Порівняно з кешуванням на БС, перевагою кешування на КТ є менші витрати для операторів зв'язку та автоматичне збільшення ємності кешу при збільшенні щільності КТ, так як скупчення КТ утворюють сукупний кеш. Недоліком даного підходу є складність мотивації користувачів для приєднання до сукупного кешу, а також випадковість взаємодії з використанням технології D2D [7].

Однак, більшість досліджень не враховують мобільність користувачів, яку можна відслідковувати на сучасному етапі розвитку технологій. Використовуючи довгострокову статистичну інформацію щодо мобільності користувачів, як, наприклад, імовірнісний розподіл середнього часу перебування користувачів в зоні покриття базових станцій, можна збільшити ефективність більшості механізмів кешування контенту.

Довгострокова інформація потребує меншого службового трафіку, але може втратити актуальність з плином часу, і тому не може гарантувати точність. Наприклад, топологія з'єднань між БС та КТ, або між КТ та КТ може швидко змінюватись через переміщення КТ. Тому, використання не актуальної інформації може призвести до значної кількості помилок в роботі механізму кешування. У випадку, коли є короткострокова інформація, як, наприклад, інформація про запити на завантаження файлів та стан каналів зв'язку, можливо організувати своєчасне оновлення закешованого контенту.

Через обмежену ємність сховища для кешованого контенту, необхідно заміняти неактуальний контент для збільшення ефективності кешування. Для цього використовуються алгоритми адаптивного кешування, що замінюють неактуальний контент до якого більше не звертаються користувачі та імовірніть нових звернень до якого дуже мала [8]. Також, адаптивне кешування можна використати для обслуговування користувачів, що рухаються за заздалегідь відомим моделями пересування та мають передбачувані запити. Коли траєкторія руху та уподобання мобільних користувачів відомі, базові станції можуть оновлювати закешовану інформацію відповідно до оцінки майбутніх запитів. Основним завданням в цьому випадку є точне передбачення майбутнього місцезнаходження користувачів та їх запитів, а також визначення частоти з якою необхідно використовувати алгоритми адаптивного кешування.

На практиці, користувачі можуть завантажити лише частину файлу з БС, а не весь файл в цілому, тому що при пересуванні їм може не вистачити часу, на протязі якого вони знаходяться в зоні покриття даної БС. Алгоритми кешування з упередженням дозволяють виконувати безшовну передачу обслуговування та завантаження для користувачів за допомогою попереднього завантаження необхідного контенту на БС, що з найбільшою імовірністю будуть знаходитись на шляху пересування користувача. Однак, запити користувачів та їх місцезнаходження в реальних умовах не відомі, тому для ефективної роботи таких алгоритмів необхідні точні методи передбачення майбутнього місцезнаходження абонента.

Властивості мобільності користувачів можуть бути розділені на просторові властивості та часові властивості. Просторові властивості містять інформацію відносно фізичного місцезнаходження користувача, тоді як часові властивості описують зміну поведінки з часом.

Мобільність користувачів може бути описана *траєкторією руху* користувача. Важлива для кешування інформація, така як БС, що обслуговуватимуть користувача, відстань між користувачем та БС, може бути визначена за допомогою аналізу траєкторії користувача. Для аналізу можуть бути використані різноманітні моделі, як, наприклад, модель випадкових точок [9].

З іншого боку, мобільність користувача може бути оцінена за допомогою оцінки зміни обслуговуючого стільника, яка містить основні відомості про БС, що будуть обслуговувати користувача на його шляху. Порівняно з траєкторією користувачів дана модель містить менш деталізовану інформацію, так як шлях пересування в середині кожного стільника не відомий, але саме інформація про обслуговуючі БС на шляху користувача є найбільш критичною для більшості механізмів кешування. Цей процес можна описати за допомогою моделі ланцюга Маркова [10], число станів рівне числу БС. В ланцюгу Маркова кожен стан описує конкретного користувача, що обслуговується конкретною БС, а імовірність переходу описує імовірність переходу конкретного користувача з зони покриття однієї БС до зони покриття іншої.

Сучасні дослідження показують, що модель мобільності значною мірою залежить від соціальних взаємин між користувачами. Наприклад, було показано, що мобільні користувачі, які мають відносно сильні соціальні зв'язки, з великою імовірністю будуть мати схожі траєкторії [11]. Авторами було запропоновано дворівневу модель мобільності, що спочатку будує соціальний граф, де вершини описують мобільних користувачів, а зважені ребра – силу соціальних зв'язків між користувачами. На другому етапі, будуються соціальні групи і мобільні користувачі в кожній групі рухаються разом. Така інформація може бути корисна при кешуванні на КТ.

Для зображення частоти та тривалості періоду, на протязі якого два користувача з'єднані між собою, використовується часова шкала на якій відображаються випадкові пари мобільних користувачів. Випадкові пари описуються часовим інтервалом контакту та інтервалом між контактами, де інтервалом контакту є часовий інтервал на протязі якого два користувача знаходяться в зоні радіозв'язку, а інтервалом між контактами є часовий інтервал між двома послідовними контактами. Така модель мобільності використовується для вирішення задач маршрутизації в епізодичних мережах [12].

Час перебування в стільнику описує тривалість обслуговування конкретного користувача заданою БС, що може вплинути на об'єм даних, який може отримати користувач від даної БС. В [10] був запропонований алгоритм визначення розподілу часу перебування в стільнику за допомогою аналізу історії пересування мобільного користувача.

Моделі мобільності користувачів зазвичай періодичні, що може бути використано для вирішення завдання оновлення кешованого контенту. Час повернення, що визначається як час, через який випадковий користувач повернеться до місця, в якому він вже перебував. Цей час є мірою періодичності і частоти повторного відвідування користувачем однієї ділянки. В [13] був проведений аналіз розподілу часу повернення, та визначені пікові значення імовірності часу повернення припадають на 24, 48 та 72 години.

В результаті аналізу можна сформувати потенційні пропозиції щодо використання інформації про мобільність користувачів для побудови механізмів кешування (табл. 1).

Таблиця 1

Можливість використання інформації про мобільність користувачів при проектуванні механізмів кешування

	Просторові властивості			Часові властивості		
	Траєкторія користувача	Зміна обслуговуючого стільника	Соціальні групи	Інтервал контакту	Час перебування в стільнику	Час повернення
Кешування на БС	Так	Так	Ні	Ні	Так	Ні
Кешування на КТ	Ні	Ні	Так	Так	Ні	Ні
Адаптивне кешування	Ні	Ні	Так	Ні	Ні	Так
кешування з упередженням	Так	Так	Ні	Ні	Ні	Ні

В безпроводових мережах, що орієнтовані на передачу контенту, користувач при русі може завантажувати необхідні файли з усіх БС, що знаходяться на його шляху. Різні БС можуть кооперативно кешувати запитані файли для підвищення ефективності, тому необхідна додаткова інформація для передбачення всіх БС, що будуть на шляху користувача. Для цього може бути використана інформація про його траєкторію та імовірності зміни обслуговуючих стільників. Порівняно з інформацією про імовірності зміни стільника, інформація про траєкторію користувача містить додаткові дані такі як, наприклад, відстань до БС у різних стільниках, що може знадобитись для більш ефективного кооперативного кешування. В залежності від відстані до БС може змінюватись швидкість передачі, що може вплинути на об'єм інформації, що буде завантажена з різних БС. Більш того, час перебування в стільнику також є критичним для визначення об'єму інформації, що може бути завантажена, і тому також впливатиме на кешування контенту на БС.

При використанні кешування на КТ мобільні користувачі можуть отримувати необхідні файли безпосередньо від інших користувачів за допомогою технології D2D. Для реалізації такого механізму кешування необхідна інформація щодо тривалості контакту між користувачами. Також, соціальні зв'язки дозволять розкласти всю мережу на декілька невеликил соціальних груп для зменшення складності реалізації кешування. Крім того, соціальні групи можуть містити деяку інформація про контакти, наприклад мобільні користувачі з однієї соціальної групи імовірно будуть білшь часто контактувати між собою [14]. Тому, інформація про соціальні групи може бути використана при проектуванні механізмів кешування з розміщенням контенту на КТ.

Закешований контент може адаптивно оновлюватись в залежності від періодичності руху користувачів використовуючи дані про час повернення. Також, мобільні користувачі з різних соціальних груп можуть мати різні уподобання щодо контенту. Тому, модель мобільності кожної соціальної групи може використовуватись для збільшення ефективності алгоритмів адаптивного кешування. Наприклад, в кафе можуть приходити різні групи клієнтів з різними уподобаннями щодо контенту та в різні проміжки часу: студенти можуть заходити на ранкову каву, люди старшого віку можуть заходити на чай пообіді, офісні працівники можуть разом заходити на вечерю. Таким чином, БС навколо кафе можуть адаптивно оновлювати закешованний контент для різних груп.

Якщо траєкторія користувача або його зміна обслуговуючих стільників може бути визначена на основі попередніх даних, то можна передбачити які БС будуть його обслуговувати на маршруті. Таким чином, якщо мобільний користувач запитує деякий файл, БС що будуть обслуговувати його на його майбутньому шляху, можуть заздалегідь закешувати необхідний файл або деякий його фрагмент, після чого користувач зможе завантажувати цей файл рухаючись між даними БС. Хоча даний підхід може збільшити навантаження на опорну мережу оператора, але такий механізм попереднього кешування може значно збільшити ефективність системи та зменшити затримки при завантаженні.

Висновки. Таким чином, в роботі проведено аналіз можливості використання інформації щодо мобільності користувачів в безпроводових мережах, що орієнтовані на контент. Були розглянуті просторові та часові властивості мобільності, що можуть бути використані для вирішення основних завдань при розробці механізмів кешування.

У зв'язку з швидким зростанням кількості мобільних пристроїв збір інформації про мобільність користувачів означає обробку великих об'ємів даних. Тому, для повноцінного використання цієї інформації в безпроводових мережах, що орієнтовані на контент, необхідно провести додаткові дослідження щодо застосування технологій аналізу Big Data для виділення важливої інформації про мобільність користувачів.

ЛІТЕРАТУРА:

1. X. Peng, J. Zhang, S.H. Song, and K. B. Letaief, "Cache size allocation in backhaul limited wireless networks," in Proc. IEEE Int. Conf. Commun. (ICC), Kuala Lumpur, Malaysia, May 2016.

2. X. Peng, J.-C. Shen, J. Zhang, and K. B. Letaief, "Backhaul-aware caching placement for wireless networks," in Proc. IEEE Global Commun. Conf. (GLOBECOM), San Diego, CA, Dec. 2015.

3. V. Conan, J. Leguay, and T. Friedman, "Fixed point opportunistic routing in delay tolerant networks," IEEE J. Sel. Areas Commun., vol. 26, no. 5, pp. 773–782, Jun. 2008.

4. K. Poularakis and L. Tassiulas, "Exploiting user mobility for wireless content delivery," in Proc. IEEE Int. Symp. Information Theory (ISIT), Istanbul, Turkey, Jul. 2013.

5. K. Shanmugam, N. Golrezaei, A. Dimakis, A. Molisch, and G. Caire, "Femtocaching: Wireless content delivery through distributed caching helpers," IEEE Trans. Inf. Theory, vol. 59, no. 12, pp. 8402–8413, Dec. 2013.

6. M. Maddah-Ali and U. Niesen, "Fundamental limits of caching," IEEE Trans. Inf. Theory,, vol. 60, no. 5, pp. 2856–2867, May 2014.

7. N. Golrezaei, P. Mansourifard, A. Molisch, and A. Dimakis, "Base-station assisted device-to-device communications for high-throughput wireless video networks," IEEE Trans. Wireless Commun., vol. 13, no. 7, pp. 3665–3676, Jul. 2014.

8. H. Ahlehagh and S. Dey, “Video-aware scheduling and caching in the radio access network,” IEEE/ACM Trans. Netw., vol. 22, no. 5, pp. 1444–1462, Oct. 2014.

9. C. Bettstetter, H. Hartenstein, and X. Pérez-Costa, “Stochastic properties of the random waypoint mobility model,” ACM/Kluwer Wireless Netw., vol. 10, no. 5, pp. 555–567, Sept. 2004.

10. J.-K. Lee and J. C. Hou, “Modeling steady-state and transient behaviors of user mobility: formulation, analysis, and application,” in Proc. ACM Mobile Ad Hoc Netw. and Comput. (MobiHoc), Florence, Italy, Jun. 2006.

11. D. Wang, D. Pedreschi, C. Song, F. Giannotti, and A.-L. Barabasi, “Human mobility, social ties, and link prediction,” in Proc. ACM Knowledge Discovery and Data Mining (SIGKDD), San Diego, CA, Aug. 2011.

12. Сова О.Я., Міночкін Д.А., Романюк В.А., Жук П.В. Модель організації інформаційних ресурсів інтелектуальних систем управління вузлами мобільних радіомереж класу MANET. Збірник наукових праць «Наука і техніка Повітряних Сил Збройних Сил України». – Х.: ХУПС. – 2015, № 2, - с. 51-57

13. M. C. Gonzalez, C. A. Hidalgo, and A.-L. Barabasi, “Understanding individual human mobility patterns,” Nature, vol. 453, no. 7196, pp. 779–782, Jun. 2008.

14. O. Semiari, W. Saad, S. Valentin, M. Bennis, and H. V. Poor, “Context-aware small cell networks: How social metrics improve wireless resource allocation,” IEEE Trans. Wireless Commun., vol. 14, no. 11, pp. 5927–5940, Jul. 2015.

Рецензент: д.т.н., проф. Кравчук С.О., доктор технічних наук, професор кафедри, Національний технічний університет «Київський політехнічний інститут»

к.т.н. Миночкин Д.А.

АНАЛИЗ МЕХАНИЗМОВ КЭШИРОВАНИЕ КОНТЕНТА В БЕСПРОВОДНЫХ СЕТЯХ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

С развитием технологий услуги мобильной связи меняют акцент с услуг, ориентированных на установление соединения на услуги, ориентированные на передачу контента. Одним из возможных направлений развития архитектуры мобильных сетей является создание беспроводных сетей, ориентированных на передачу контента. Одним из подходов для уменьшения нагрузки на базовую сеть оператора и уменьшения задержки передачи в таких сетях является кэширование наиболее популярного контента на участке «последней мили» - базовых станциях (БС) и конечных терминалах пользователей (КТ). В отличие от проводных сетей, уникальным свойством беспроводных сетей, ориентированных на передачу контента, является мобильность пользователей. Поэтому, в работе рассматриваются основные свойства модели мобильности пользователей и возможность использования этой дополнительной информации для повышения эффективности механизмов кэширования.

Ключевые слова: кэширование, беспроводные сети, мобильность.

Ph.D. Minochkin D.A.

ANALYSIS OF CONTENT CACHING MECHANISMS IN WIRELESS NEXT GENERATION NETWORKS

With the development of technology mobile services are changing from services that focus on establishing connection, to services that focus on content delivery. One of the possible directions of mobile networks architecture development is to create wireless networks that focus on the content delivery. One of the approaches to reduce the load on the core network and reducing transmission delay in such networks is caching the most popular content on the "last mile" - base stations (BS) and end-user terminal (EUT). Unlike wired networks, wireless networks have a unique feature that can affect the content delivery and caching – user mobility. Therefore, in this paper the basic properties of user mobility are analyzed and the possibility to use this additional information to increase the effectiveness of caching mechanisms is discussed.

Keywords: caching, wireless networks, mobility.

УДК 004.891

к.т.н., доц. **Муляр І.В.** (ХмНУ)
Гусляков Г.В. (ХмНУ)
Солодєєва Л.В. (ВІКНУ)

РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ТА МЕТОДУ ЇЇ ВИРІШЕННЯ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ОБЧИСЛЮВАЛЬНИХ РЕСУРСІВ НА ОСНОВІ ТЕХНОЛОГІЇ ВІРТУАЛІЗАЦІЇ

Як правило, в кожній організації своя специфіка і свої підходи до зниження витрат на обслуговування, розвитку корпоративної мережі і отримання від неї додаткового прибутку. Завдання підвищення ефективності використання ресурсів також в кожному конкретному випадку вирішується з урахуванням особливостей і специфіки, властивих організації. Звісно, головним критерієм є ефективність, але при виборі будь-яких конкретних підходів до підвищення ефективності використання ресурсів слід також враховувати чотири важливих критерії: ізоляція несумісного програмного забезпечення, безпека корпоративної мережі, надійність обладнання, «прозорість» для користувачів. На сьогоднішній день можна виділити декілька загальновідомих підходів до підвищення ефективності використання ресурсів: використання ресурсів для внутрішніх задач; використання ресурсів для задач сторонніх організацій; застосування адекватних апаратних рішень; об'єднання сервісів і зниження числа серверних операційних систем; застосування технології віртуальних машин. У розглянутих підходах ми, так чи інакше, стикалися з серйозними проблемами інформаційної безпеки, сумісності програмного забезпечення, порушення деякої логічної структури розміщення служб і функцій серед комп'ютерів мережі, а також складності підбору адекватних апаратних конфігурацій. Але саме за допомогою технології віртуалізації можна уникнути майже всі описані проблеми, окрім надійності. Однак, на сьогоднішній день відсутня будь-яка методика з планування нового або реорганізації існуючого серверного парку з метою підвищення ефективності використання обчислювальних ресурсів при застосуванні технології віртуальних машин.Відповідно, виникає необхідність в розробці деякої математичної моделі для завдання пошуку розподілу логічних серверів по фізичним комп'ютерам з урахуванням специфіки, властивою технології віртуальних машин, і пошуку методів її вирішення.

На основі запропонованих алгоритмів, математичних моделей та методів їх вирішення розроблена програмна реалізація алгоритму пошуку оптимального розподілу логічних серверів по комп'ютерам.

Ключові слова: ефективність, технологія віртуалізації, серверний парк, реорганізація, математична модель, метод, алгоритм.

Вступ. На сьогоднішній день існує велика кількість організацій, що мають корпоративну мережу, яка складається з безлічі кінцевих робочих місць користувачів і деякого, так званого, серверного парку. Як правило, спочатку корпоративна мережа грамотно проектується фахівцями з урахуванням надійності, безпеки і багатофункціональності та керівництво організацій вкрай негативно відноситься до внесення значних або навіть невеликих змін в інфраструктуру мережі, яка вже багато років справно функціонує і задовольняє всім вимогам. Проте, керівництво завжди цікавить розширення функціональних можливостей, зниження витрат на утримання мережі і фахівців, які обслуговують її, а також отримання додаткового прибутку з використовуваного технічного обладнання. Багаторічна практика експлуатації серверних систем показала, що на сьогоднішній день більшість комп'ютерів серверного парку досить слабо завантажені по обчислювальним ресурсам [1].

Така ситуація склалася по наступній причині: ринок апаратних рішень розвивається стрімко і виробники обладнання дуже швидко відказуються підтримувати застаріле обладнання, яке можна було б використовувати для розміщення деяких серверних служб. Так, наприклад, один з найважливіших елементів добре захищеної корпоративної мережі – контролер домену, по сьогоднішнім міркам не вимагає великої кількості ресурсів: 2-3% середньодобового навантаження процесора класу Pentium, мережевий трафік – декілька

десятків або сотень мегабайт даних, які передаються не постійно, а одноразово через певний період часу (від 15 хвилин до 1 години або рідше), пам'яті необхідно не більше ніж 2 ГБ, дискового простору необхідно 100-120 ГБ. В той же час, згідно з безпекою, на контролері домену вкрай не рекомендується розміщувати будь-які інші серверні служби (файлові ресурси, WEB-сервери та ін.), тобто лише одному контролеру з такими низькими вимогами необхідний цілий комп'ютер. Тим не менш, вихід з даної ситуації є – використання технології віртуальних машин, яка дозволяє функціонувати декільком операційним системам разом зі всіма її службами – логічними серверами – на одному фізичному комп'ютері. При цьому з точки зору безпеки в корпоративних мережах, забезпечується максимальна ізоляція кожної ОС разом з її службами від інших ОС, вони постійно розділяють одні і ті ж апаратні засоби.

Постановка задачі. Таким чином, серверний парк із слабким навантаженням ресурсів може бути оптимізований, що в результаті повинно призвести до зменшення об'єму використовуваного обладнання і затрат на його підтримку. Крім того, обладнання яке звільнилось можна використовувати для отримання додаткового прибутку. Саме по собі завдання підвищення ефективності використання ресурсів є доволі застарілим і в кожній конкретній сфері діяльності людини вирішується своїми методами. Однак, технологія віртуальних машин в корпоративних мережах стала застосовуватися відносно недавно і поки не ставилось завдання підвищення ефективності використання ресурсів комп'ютерів серверного парку при умові використання цієї технології. Відповідно, необхідні нові підходи до вирішення проблеми підвищення ефективності використання обчислювальних ресурсів комп'ютерів серверного парку. Однак, для цього необхідне створення формалізованого підходу до реорганізації серверного парку з метою підвищення ефективності використання ресурсів із застосуванням сучасних інформаційних технологій.

Технологія віртуальних машин надає нові можливості для побудови нового або реорганізації існуючого серверного парку. Технологія віртуальних машин дозволяє на фізичному комп'ютері під управлінням деякої, так званої базової операційної системи, емулювати роботу віртуальних машин, на яких так як і на звичайних реальних комп'ютерах можуть функціонувати логічні сервери. Таким чином, ця технологія може забезпечити функціонування декількох ізольованих логічних серверів на одному комп'ютері і тим самим обходити проблеми безпеки, сумісності, зміни прив'язок сервісів до логічних серверів, а також позбавляє від необхідності підбору адекватних апаратних рішень, оскільки розміщення декількох логічних серверів дозволяє істотно підвищити ефективність використання ресурсів комп'ютера[2].

Таким чином, можна зробити висновок про те, що підхід, пов'язаний із застосуванням технології віртуальних машин, є найбільш прийнятним, однак, потрібна розробка нової методики реорганізації серверного парку при використанні цього підходу. Крім того, необхідно запропонувати відповідну математичну модель і метод її рішення для задачі пошуку оптимального розподілу логічних серверів по комп'ютерам

Основна частина. Запропонована методика реорганізації серверного парку із застосуванням технології віртуальних машин спирається на пошук оптимального розподілу логічних серверів на комп'ютери. Завдання пошуку оптимального розподілу вирішується один раз на першому етапі і кілька разів в залежності від результатів реорганізації серверного парку на другому етапі реорганізації.

Основна мета реорганізації – підвищення ефективності використання обчислювальних ресурсів комп'ютерів. Відповідно, з одного боку в задачі оптимізації важливе завантаження ресурсів кожного комп'ютера, з іншого боку підвищення завантаження ресурсів комп'ютерів повинно призводити до скорочення загального обсягу задіяного обладнання. Таким чином, в результаті розподілу на всіх задіяних комп'ютерах завантаження ресурсів повинно бути найкращим, а на всіх незадіяних комп'ютерах завантаження ресурсів повинно бути нульовим. Однак, очевидно, що множина задіяних комп'ютерів, що отримується внаслідок

розподілу, заздалегідь невідома і її можна отримати, лише вирішивши поставлену задачу. Якщо намагатися підвищувати завантаження ресурсів всіх комп'ютерів серверного парку, то це призведе лише до балансування завантаження ресурсів і ні один з комп'ютерів не звільниться [3].

Відповідно, виникає проблема неоднозначності в цілі оптимізації. Дану проблему можна вирішити за допомогою використання апарату динамічного програмування.

Запропонована математична модель, складається з декількох компонентів:

1. Для кожного *k*-го комп'ютера, $k = 1..NH$ повинні виконуватися обмеження по ресурсам і додаткові обмеження для виключення можливості розміщення певних логічних серверів на один комп'ютер:

$$\begin{cases} \sum_{j=1}^{NS} Q_{ij} x_{kj} \le R_{ik} - V_i, i = 1..NC \\ \sum_{j=1}^{NS} E_{dj} x_{kj} \le 1, d = 1..NX \\ \forall_j \in [1, N] : x_j \in \{0,1\} \\ k = 1..NH \end{cases}, \quad (1)$$

де, *NC* – число типів ресурсів; *NH* - число фізичних комп'ютерів; *NS* - число логічних серверів (загальне число з урахуванням додаткових логічних серверів, які були підготовлені для дублювання функцій критичних за важливістю логічних серверів); *NX* - число додаткових обмежень (підмножина дублюючих один одного логічних серверів); $R_{i,k}$ - базовий рівень *i*-го типу ресурсу *k*-го фізичного комп'ютера; $Q_{i,j}$ - вимога *j*-го логічного сервера до *i*-го ресурсу; $E_{d,j}$ - елемент булевої матриці, рівний "1", якщо *j*-й логічний сервер присутній в *d*-му обмеженні, "0" - в іншому випадку; $X_{k,j}$ - елемент булевої матриці, рівний "1", якщо *j*-й логічний сервер (віртуальна машина з логічним сервером) розміщується на *k*-му фізичному комп'ютері, "0" - в іншому випадку [4].

2. Для кожного j-го логічного сервера, $j = 1..NS$ повинні дотримуватися обмеження згідно з яким, логічний сервер може бути розміщений на один і тільки один комп'ютер:

$$\begin{cases} \sum_{k=1}^{NH} x_{kj} \le 1 \\ j = 1..NS \end{cases}, \quad (2)$$

3. Цільові функції завантаження обчислювальних ресурсів для кожного задіяного комп'ютера, причому які саме комп'ютери повинні бути задіяні - заздалегідь невідомо:

$$\begin{cases} L_y = \frac{1}{\sum_{i=1}^{NC} O_i} \left(\sum_{i=1}^{NC} \frac{O_i}{R_{iy} = Vi} \left(\sum_{j=1}^{NS} Q_{ij} x_{yj} \right) \right) \to \max \\ \forall_y \in \{k^*\} \end{cases}, \quad (3)$$

де V_i - вимога базової ОС до *i*-го ресурсу; O_i - елемент вектора маски, що приймає значення "1", якщо відповідному *i*-му типу ресурсу переважне підвищення ефективності його використання, "0" - в іншому випадку; $\{k^*\}$ - невідома множина індексів фізичних комп'ютерів, які виявляться задіяними після рішення задачі оптимального розподілу.

Після перегляду існуючих методів вирішення завдання в цілому, в силу неоднозначності в основній меті оптимізації, зроблено висновок про те, що в першому

наближенні необхідно провести розбиття початкової задачі на множину більш простих під задач. Запропоновано наступний підхід до вирішення початкової задачі в цілому:

1. Вводиться деякий, так званий "великий крок", що позначається буквою T.

2. Вводиться множина індексів $\{K(T)\}$ комп'ютерів, що залишилися незадіяними на кроці T.

3.Вводиться множина індексів $\{J(T)\}$ логічних серверів, що залишилися нерозподіленими на кроці T. Очевидно, на нульовому кроці $T = 0, \{K(0)\} = \{1, ..., NH\}$, $\{J(0)\} = \{1, ..., NS\}$. Вважаємо, що логічні сервери відокремлені від комп'ютерів, переведені на віртуальну платформу, і потрібно шукати новий розподіл по комп'ютерам.

4. Всередині кожного кроку T для кожного комп'ютера з індексом $k \in \{K(T)\}$ з числа комп'ютерів, що залишилися на етапі T, формується математична модель підзадачі, яка представляє собою задачу умовної псевдобулевої оптимізації:

$$\begin{cases} \sum\limits_{j \in \{j(T)\}} Q_{ij} x_{kj} \le R_{ik} - V_i, i = 1..NC \\ \sum\limits_{j \in \{j(T)\}} E_{dj} x_{kj} \le 1, d = 1..NX \\ L(T,k) = \dfrac{1}{\sum\limits_{i=1}^{NC} O_i} \left(\sum\limits_{i=1}^{NC} \dfrac{O_i}{R_{ik} - V_i} \left(\sum\limits_{j \in \{j(T)\}} Q_{ij} x_{kj} \right) \right) \to \max \\ \forall_j \in \{j(T)\} : x_{kj} \in \{0,1\} \end{cases}. \quad (4)$$

5. На кожному кроці T послідовно розглядаються всі комп'ютери з індексами $k \in \{K(T)\}$, ті, що залишилися до моменту кроку T, і вибирається той, для якого в результаті рішення відповідної підзадачі, досягається найвище значення цільової функції серед значень, отриманих при рішенні підзадач для комп'ютерів з індексами $k \in \{K(T)\}$. Відповідно, найкращий комп'ютер з індексом до $k*$ вибирається з наступної умови:

$$\begin{cases} L_{k*}(T) = \max\{ L_{\max}(T,k)\} \\ k \in \{K(T)\} \\ L_{k*}(T) > 0 \end{cases}, \quad (5)$$

де, $L_{\max}(T,k)$ - оптимальне значення цільової функції на кроці T при рішенні підзадачі для k-го комп'ютера; $L_{k*}(T)$ - найвище оптимальне значення цільової функції на кроці T серед значень $L_{\max}(T,k)$ для всіх $k \in \{K(T)\}$.

В умові (5) особливо важлива умова того, що $L_{k*}(T)$ не повинно бути нульовим, це гарантує, що на кроці T хоча б один логічний сервер розподілиться і хоча б один комп'ютер буде задіяний. якщо $L_{k*}(T) = 0$, то це означає, що подальший розподіл логічних серверів неможливий і рішення початкового завдання повинно бути припинено.

Якщо ж $k*$ успішно знайдений з умови (5), то виконуються наступні перетворення: з множини комп'ютерів, які залишилися виключається комп'ютер з індексом $k*$, а з множини логічних серверів – множина серверів, розподілених на цей комп'ютер:

$$\begin{aligned} \{K(T+1)\} &= \{K(T)\} / k* \\ \{K(T+1)\} &= \{K(T)\} / \{j*\} \end{aligned}, \quad (6)$$

де, $\{j*\}$ - множина індексів логічних серверів, які були розподілені на $k*$-й фізичний комп'ютер.

Якщо в результаті перетворення (6), множина $K(T+1)$ або $J(T+1)$ виявиться порожньою, то рішення задачі завершується, в іншому випадку перехід до кроку $(T+1)$.

На рис. 1 представлена схема алгоритму розв'язання задачі в цілому.

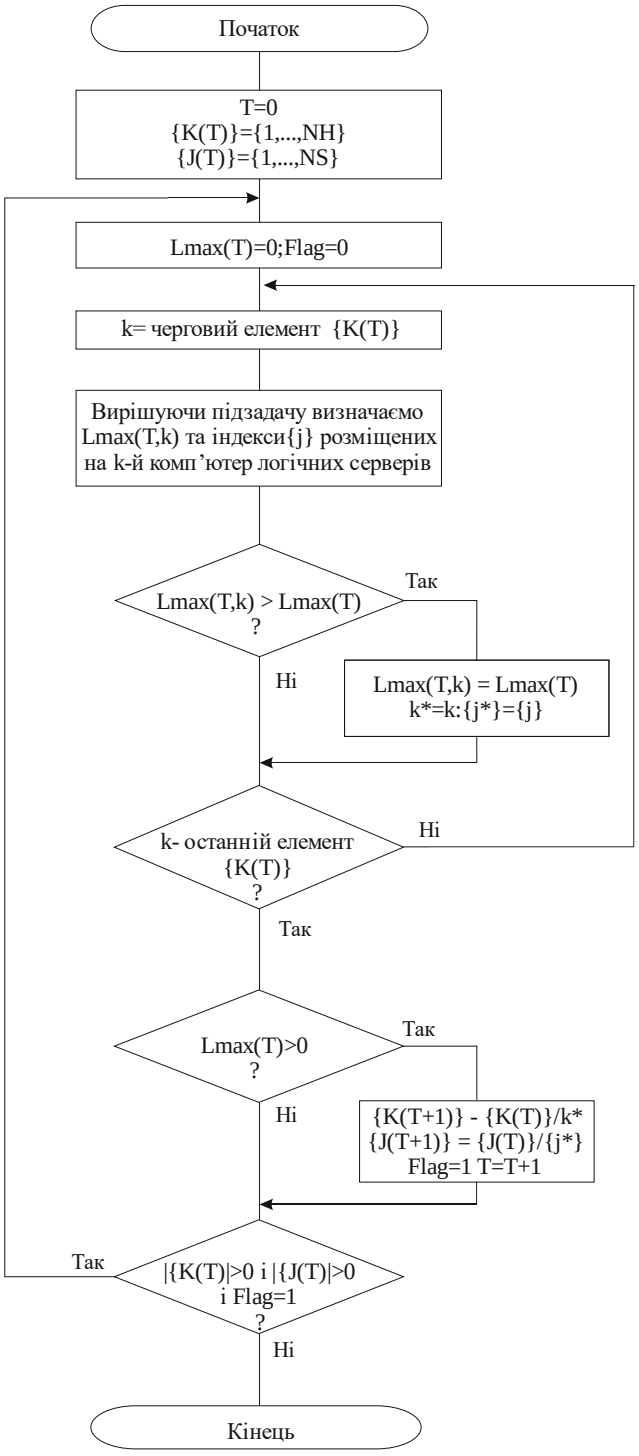


Рис. 1. Алгоритму вирішення задачі в цілому

Таким чином, використовуючи компромісний підхід, що дає схему рішення задачі в цілому, нам вдалося звести нездійсненну стаціонарну математичну модель з невизначеними цільовими функціями до деякої множини цілком вирішуваних математичних моделей (4). Число "великих кроків", в гіршому випадку (коли множина фізичних комп'ютерів спустошується раніше або разом з множиною логічних серверів) складе: *NH*, а загальне

число розв'язуваних підзадач оптимізації по окремим фізичним комп'ютерам: $0.5 * NH * (NH + 1)$. В алгоритмі (рис. 1) кожна підзадача, в свою чергу, являє собою клас задач умовної псевдобулевої оптимізації, для якої також необхідний ефективний спосіб вирішення. Підзадачу на кроці T при заданому $k \in \{K(T)\}$ нескладно представити в наступному вигляді:

$$\begin{cases} \sum_{j=1}^{N} a_{ik} x_j \le b_i, i = 1..M \\ L = \sum_{j=1}^{N} c_j x_j \to \max \\ \forall_j \in [1, N] : x_j \in \{0,1\} \end{cases}, \quad (7)$$

де, N - число змінних, M - число обмежень; матриця $\{a_{ij}\}, i = 1..M, j = 1..N$, - ліва частина, а вектор $\{b_i\}, i = 1..M$ - права частина обмежень; вектор $\{c_j\}, j = 1..N$ - коефіцієнти цільової функції.

Оскільки кількість логічних серверів і кількість комп'ютерів в загальному випадку може бути близько сотні або навіть тисячі, то зроблено висновок про доцільність використання наближених методів для можливості отримання результатів за прийнятний час.

За основу взято наближений метод локального пошуку. Для врахування обмежень модель задачі умовної псевдобулевої оптимізації перетвориться наступним чином:

$$\begin{cases} F = \sum_{j=1}^{N} c_j x_j - P * \sum_{j=1}^{M} a_{ij} x_j \le b_i \to \max \\ \forall_j \in [1, N] : x_j \in \{0,1\} \end{cases}, \quad (8)$$

де, F - скоригована з урахуванням обмежень цільова функція, а P - деяке досить велике додатнє число, таке щоб в будь-якій недопустимій точці (в якій обмеження не виконуються) значення цільової функції було гірше, ніж в будь-якій допустимій точці.

Необхідно відзначити, що вираз (8) формується тільки у випадку, якщо для будь-якого $i = 1..N : R_{i,k} - V_i > 0$. В іншому випадку, очевидно, що логічні сервери не можуть бути розподілені на заданий комп'ютер в силу явної нестачі по одному або декільком типам ресурсів комп'ютера, і підзадачу немає сенсу вирішувати.

Оскільки, очевидно, що в разі великої розмірності підзадачі і складних полімодальних обмежень метод локального пошуку не гарантує знаходження глобального оптимуму або навіть досить якісних субоптимальних рішень, то для посилення можливостей локального пошуку була виконана наступна його модифікація: радіус зон пошуку (максимальне число координат, за якими розглянуті в зоні точки можуть відрізнятися від точки центру зони) не дорівнює строго одиниці, радіус задається як додаткові вхідні дані завдання, позначимо його як *MR*; завдання вирішується не один, а безліч разів для різних стартових точок, які генеруються випадковим чином. Число стартових точок задається як додаткове вхідне завдання, позначимо його як *MS*. Відповідно, в результаті виконання завдання *MS* будь-яку кількість раз отримуємо різні рішення, порівнюємо значення цільової функції в них і вибираємо найкраще рішення.

Таким чином, запропоновано алгоритм вирішення підзадач псевдобулевої оптимізації (рис. 2).

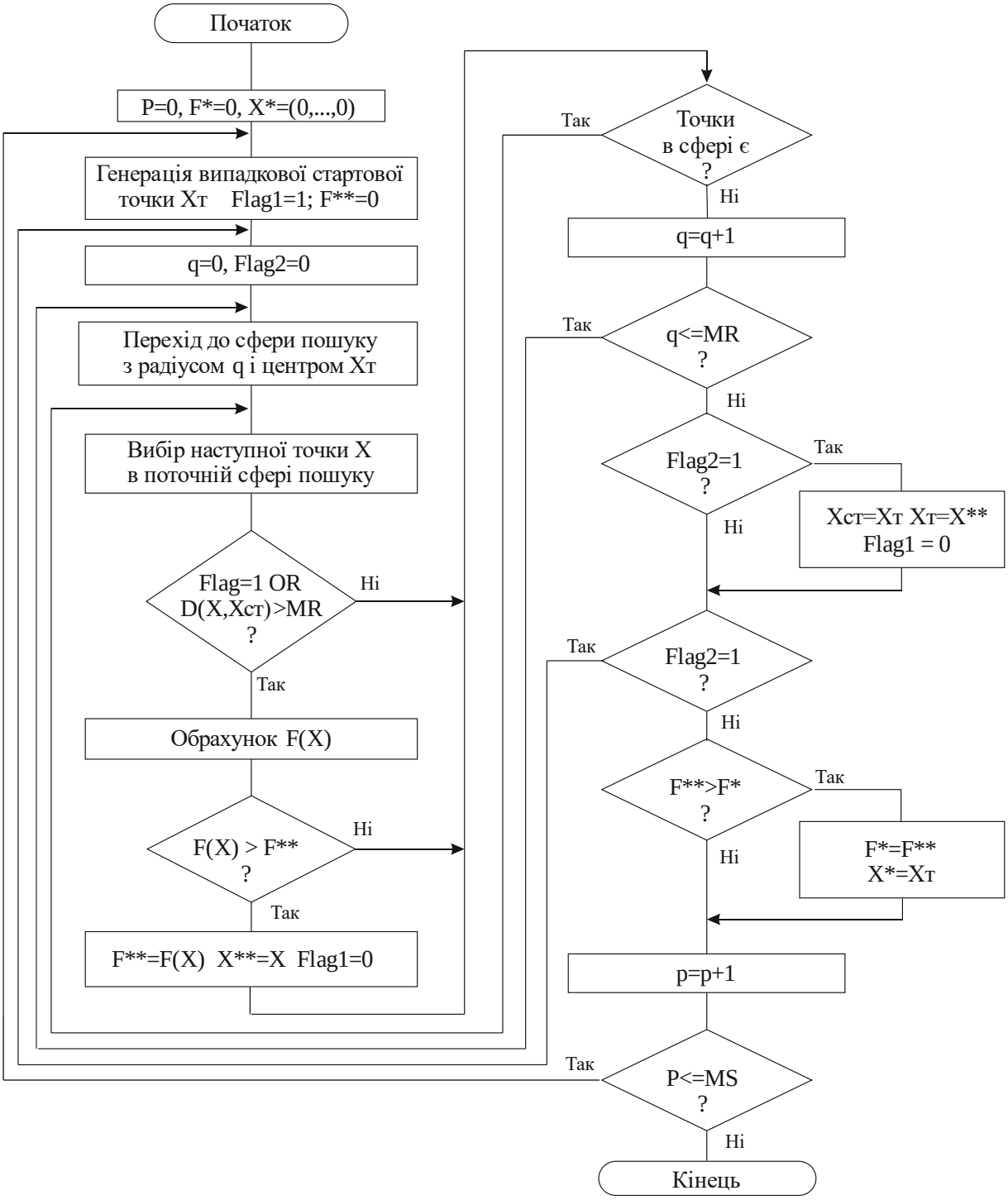


Рис. 2. Алгоритм вирішення підзадач псевдобулевої оптимізації

Таким чином, використовуючи запропоновані методи вирішення завдання пошуку розподілу і підзадач умовної псевдобулевої оптимізації, ми можемо отримати матрицю розподілу $\{X_{kj}\}, k = 1..NH, i = 1..NS$, логічних серверів по комп'ютерам. Використовуючи матрицю розподілу $\{X_{kj}\}$ нескладно також обчислити матрицю завантаження ресурсів комп'ютерів $\{\eta_{kj}\}, k = 1..NH, i = 1..NC$, для оцінки завантаження ресурсів:

$$\eta_{ki} = \begin{cases} \sum_{j=1}^{NS} \frac{x_{kj} O_{ij}}{R_{ik} - V_i}, \text{якщо} : R_{ik} - V_i > 0 \\ 0, \text{в іншому випадку} \\ \forall_i \in [1, NC] : \forall_k \in [1..NH] \end{cases} . \quad (9)$$

Висновки. На основі запропонованих алгоритмів розроблена програмна реалізація алгоритму пошуку оптимального розподілу логічних серверів по комп'ютерам. Також було проведено експериментальне дослідження з оцінки часу вирішення завдань в залежності від її розмірності. Використання технології віртуальних машин є найбільш прийнятним варіантом для підвищення ефективності використання обчислювальних ресурсів. Технологія віртуальних машин надає нові можливості з побудови або реорганізації мережевої інфраструктури. Віртуальні машини, що дозволяють запускати кілька досить добре ізольованих ОС на одному комп'ютері, вирішують проблеми інформаційної безпеки, сумісності додатків, незмінності логічної структури, а також позбавляють від необхідності підбору адекватних апаратних рішень, оскільки розміщення на одному комп'ютері декількох логічних серверів дозволяє істотно підвищити ефективність використання обчислювальних ресурсів.

ЛІТЕРАТУРА:

1. Таненбаум Э С. Современные операционные системы / Э С.Таненбаум, Х. Бос // Питер, 2015 год (4-е изд), 1120 с.

2 Муляр І.В. Оцінка протоколів динамічної маршрутизації для інтегрованих мереж / І.В. Муляр, А.І Сбітнєв., А.В., Джулій, О.С. Лєнков // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К., 2013. – № 43. – С. 158 – 165.

3. Джулій В.М., Методи та алгоритми кластеризації при комплексному аналізі даних / В.М. Джулій, О.М. Горбатюк // Вимірювальна та обчислювальна техніка в технологічних процесах: Міжнародний науково-технічний журнал.-Хмельницький, 2014. – №4. – С. 135-137.

4. Лєнков С.В. Концептуальна схема системи інтелектуальної обробки даних / С.В. Лєнков, В.М. Джулій, О.М. Горбатюк, Н.М. Берназ // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2014. – Вип. № 46. – С.181-190.

REFERENCES:

1. Tanenbaum E S. Sovremennye operatsionnye sistemy / E S.Tanenbaum, H. Bos // Piter, 2015 god (4-e izd), 1120 str.

2. Mulyar I.V. Otsinka protokoliv dynamichnoyi marshrutyzatsiyi dlya intehrovanykh merezh / I.V. Mulyar, A.I Sbitnyev., A.V., Dzhuliy, O.S. Lyenkov // Zbirnyk naukovykh prats' Viys'kovoho instytutu Kyyivs'koho natsional'noho universytetu imeni Tarasa Shevchenka. – K., 2013. – # 43. – S. 158 – 165.

3. Dzhuliy V.M., Metodi ta algoritmi klasterizatsiyi pri kompleksnomu analizi danih / V.M. Dzhuliy, O.M. Gorbatyuk // Vimiryuvalna ta obchislyuvalna tehnika v tehnologichnih protsesah:Mizhnarodniy naukovo-tehnichniy zhurnal.-Hmelnitskiy, 2014.-№4 -S. 135-137.

4. Lenkov S.V. Kontseptualna shema sistemi intelektualnoyi obrobki danih / S.V. Lenkov, V.M. Dzhuliy, O.M. Gorbatyuk, N.M. Bernaz // Zbirnik naukovih prats Viyskovogo institutu Kiyivskogo natsionalnogo universitetu imeni Tarasa Shevchenka. – K.: VIKNU, 2014. – Vip. № 46. – C.181-190

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

к.т.н. Муляр И.В., Гусляков Г.В., Солодеева Л.В.

РАЗРАБОТКА МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ И МЕТОДОВ ЕЕ РЕШЕНИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ НА ОСНОВЕ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

Как правило, в каждой организации своя специфика и свои подходы к снижению затрат на обслуживание, развития корпоративной сети и получения от нее дополнительной прибыли. Задача повышения эффективности использования ресурсов также в каждом конкретном случае решается с учетом особенностей и специфики, присущих организации. Естественно, главным критерием является эффективность, но при выборе каких-либо конкретных подходов к повышению эффективности использования ресурсов следует также учитывать четыре важных критерия: изоляция несовместимого программного обеспечения, безопасность корпоративной сети, надежность оборудования, «прозрачность» для пользователей. На сегодняшний день можно выделить несколько общеизвестных подходов к повышению эффективности использования ресурсов: использование ресурсов для внутренних задач; использования ресурсов для задач сторонних организаций; применение адекватных аппаратных решений; объединение сервисов и снижение числа серверных операционных систем; применение технологии виртуальных машин. В рассмотренных подходах мы, так или иначе, сталкивались с серьезными проблемами информационной безопасности, совместимости программного обеспечения, нарушение некоторой логической структуры размещения служб и функций среди компьютеров сети, а также сложности подбора адекватных аппаратных конфигураций. Но именно с помощью технологии виртуализации можно избежать почти все описанные проблемы, кроме надежности. Однако, на сегодняшний день отсутствует какая-либо методика по планированию нового или реорганизации существующего серверного парка с целью повышения эффективности использования вычислительных ресурсов при применении технологии виртуальных машин.

Соответственно, возникает необходимость в разработке некоторой математической модели для задачи поиска распределения логических серверов по физическим компьютерам с учетом специфики, присущей технологии виртуальных машин, и поиска методов ее решения.

На основе предложенных алгоритмов, математических моделей и методов их решения разработана программная реализация алгоритма поиска оптимального распределения логических серверов по компьютерам.

Ключевые слова: эффективность, технология виртуализации, серверный парк, реорганизация, математическая модель, метод, алгоритм.

Ph.D. Mulyar I.V, Gusliakov G.V., Solodeeva l.V.

THE DEVELOPMENT OF MATHEMATICAL MODELS AND METHODS OF ITS SOLUTION TO IMPROVE THE UTILIZATION OF COMPUTING RESOURCES BASED ON VIRTUALIZATION TECHNOLOGY

Typically, each organization has its own specificity and approaches to reduce maintenance costs, costs for development of corporate networks and obtain the additional profit from it. The problem of improving the effectiveness of resources use is also solved in each specific case depending on features and specifics of the organization. Of course, the main criterion is effectiveness. However, through choosing any specific approach for improving the effectiveness of the resources use we should consider also 4 important criteria like: isolation of incompatible software, security of corporate network, reliability of equipment, «clearness» for users. Nowadays, we can emphasize several already known approaches for improving the effectiveness of the resources use: use of the resources for internal problems; use of the resources for problems of other organizations; appliance of the adequate hardware solutions; combination of services and reduction the number of server operating systems; use of the virtual machine technology. In the previously considered approaches we have faced with serious problems of information security, compatibility of software, breach of some logical structure of placing the services and functions in computers in the network and complexity of selection of the adequate decisions. Exactly, with the help of virtualization technology we can avoid almost all of described problems, except of reliability. However,

nowadays there are not methods of planning the new or reorganization the existing server park for the purpose of improving the effectiveness of using the computing resources with the help of virtual machine technology.

Accordingly, here appears the necessity to design some mathematical model to set an assignment of search of logical servers' allocation in physical computers depending on the specifics, which is common to virtual machine technology, and a search of methods for its solution.

It was developed the software implementation of algorithm of the optimal allocation of logical servers search on the computers, based on the proposed algorithms, mathematical models and methods of their solving.

Keywords: effectiveness, virtualization technology, server park, reorganization, mathematical model, method, algorithm.

УДК 004.852

д.т.н., проф. **Мясіщев О.А.** (ХмНУ)
к.т.н. **Лєнков Є.С.** (ВІТІ)
Білик О.М. (ХмНУ)

РОЗПІЗНАВАННЯ ГРАФІЧНИХ ОБРАЗІВ З ВИКОРИСТАННЯМ НЕЙРОННИХ МЕРЕЖ

У статті розглядаються методи для підвищення ефективності роботи функції системи стеження за об'єктом (ActiveTrack), проблемою в даній системі є те що при великому скупченні людей, або коли ціль рухалась повільно і раптово збільшила швидкість, система втрачає ціль на яку було вказано.

Тому в даній функції пропонується використовувати додатковий пристрій який буде отримувати вхідні дані з відеокамери головного пристрою та вибирати ціль з пульта керування, далі методами розпізнавання образів з використанням бібліотеки OpenCV та використанням нейронної мережі проводиться аналіз даних, пошук на відеозображенні вказаної цілі і передаватимуться дані для скеровування головного пристрою в сторону яку рухається ціль. Для вирішення завдань виявлення перешкод і розпізнавання образів необхідна наявність неспотвореного зображення. Однак більшість об'єктивів телекамер мають викривляє ефектом (аберацією). Об'єктиви, в яких повністю усунена аберація, мають високу вартість і великими масогабаритними характеристиками. Для усунення аберації об'єктиву телекамери пропонується використання алгоритму цифрової корекції спотворень на відеозображенні.

Модуль на якому оброблятимуться вхідні дані складається з одноплатного комп'ютера, вибір обумовлений малими розмірами та масою.

Ключові слова: Розпізнавання образів, нейронні мережі, open cv, детектування, activetrack.

Вступ. Властивість бачити дозволяє нам надійно розпізнавати людей, тварин а також інші неживі об'єкти. В галузі штучного інтелекту або комп'ютерного зору для позначення всіх цих здібностей прийнято використовувати термін розпізнавання образів. До цього відноситься визначення класу конкретних об'єктів, представлених на зображенні (наприклад, обличчя), а також розпізнавання самих конкретних об'єктів (наприклад, особи Тіма Кука). Нижче перераховані прикладні області, які стимулюють розвиток цього науково-технічного напряму.

1. Біометрична ідентифікація. Кримінальні розслідування і контроль доступу на об'єкти, що допускають присутність обмеженого кола осіб, потребують можливість одразу ідентифікувати особу. Операції зняття відбитків пальців, сканування райдужної оболонки ока і фотографування особи призводять до отримання зображень, які повинні бути співставленні з даними, що відносяться до конкретних людей.

2. Вибірка зображень з урахуванням їх вмісту. В текстовому документі можна легко знайти місцезнаходження будь-якого рядка, наприклад “cat”, якщо вона там є; таку можливість надає будь-який текстовий редактор. А тепер розглянемо задачу пошуку в зображенні множини пікселів, які відповідають зображенню кішки. Якби система комп’ютерного зору мала таку можливість, то дозволяла б відповідати на запити, що стосуються вмісту зображень, такі як "Знайдіть фотографію, на якій показані разом Тім Кук і Джон Айв", "Знайдіть фотографію футболіста в стрибку"," Знайдіть фотографію Ейфелевої вежі вночі " тощо, без необхідності вводити ключові слова.

3. Розпізнавання рукописного тексту. До прикладу такого тексту відносяться підписи, блоки адрес на конвертах, суми в чеках і введені електронною ручкою в планшет чи будь-який інший пристрій.

Зір використовується для розпізнавання не тільки об'єктів, але і видів діяльності. Люди здатні впізнавати знайому ходу (здалеку помічаючи свого друга), вираз обличчя (посмішку), жест (наприклад, прохання наблизитися), дія (стрибок, танець) і т.д. Дослідження по розпізнаванню видів діяльності все ще знаходяться на етапі свого становлення, тому в даній статті ми зосередимося на темі розпізнавання об'єктів з використанням нейронних мереж.

Припустимо, у нас є певна кількість еталонних образів - зображень, або ще чого-небудь. Нам дають якийсь спотворений образ, і наше завдання полягає в тому, щоб «розпізнати» в ньому один з еталонних. Яким чином людина це зробить - питання складне. А ось яким чином виконає це завдання штучна нейронна мережа - ми цілком можемо собі уявити.

Говорячи неформально, штучна нейронна мережа являє собою систему «нейронів», взаємодіючих між собою на зразок справжньої нейронної мережі мозку. Кожен нейрон мережі отримує і передає сигнали іншим. Те, як нейрони пов'язані між собою, залежить від типу мережі. Нейронна мережа «навчається» рішенням певної задачі, що, по суті, зводиться до обчислень вагових коефіцієнтів матриці. За допомогою нейронних мереж намагаються вирішувати різні завдання, але в статті буде вирішення питання розпізнавання образів.

Виклад основного матеріалу. Метою роботи є аналіз та вдосконалення існуючих пристроїв, так званих «безпілотників», в яких є можливість слідкування за об’єктом, але мають проблеми в реалізації цієї функції. Завдання - підвищення ефективності розпізнавання і пошуку об’єктів. Тому для вирішення цього завдання будем використовувати наступні методи.

Розпізнавання з урахуванням яскравості

При такому підході за основу береться підмножина пікселів зображення, яка відповідає образу який ми розпізнаєм, і визначаються дані про характеристики як дані про самі вихідні значення яскравості пікселів. Ще один варіант цього методу полягає в тому, що спочатку може бути виконана згортка зображення з різними лінійними фільтрами, після чого значення пікселів в результуючих зображеннях розглядаються як характеристики. Такий підхід виявився дуже успішним при вирішенні таких завдань, як розпізнавання рукописних цифр.

Для створення детекторів обличь, що дозволяють розпізнавати обличчя за допомогою баз даних з прикладами, використовувався цілий ряд статистичних методів, включаючи методи на основі нейронних мереж з необробленими вхідними даними, представленими у вигляді характеристик пікселів; дерева рішень з характеристиками, обумовленими за допомогою різних фільтрів смуг і країв. Деякі результати застосування останнього методу показані на рис 1.



Рис. 1. Приклад розпізнавання обличь з урахуванням яскравості

Одним з недоліків методу, в якому в якості векторів характеристик використовуються необроблені дані про пікселі, є велика надмірність, властива цьому способу представлення. Припустимо, що розглядаються два пікселя, розташовані поруч на зображенні, щоки лиця якоїсь людини; між ними, швидше за все, буде досить висока кореляція, оскільки для них властиві аналогічне геометричне розташування, освітленість і т.д. Для скорочення кількості розмірностей вектора характеристик можна з успіхом застосовувати методи зменшення обсягу даних, такі як аналіз найбільш важливих компонентів; використання таких методів забезпечує розпізнавання образів, подібних обличчю, з більшою швидкодією в порівнянні з тим, що може бути досягнуто з використанням простору більшої розмірності.

Розпізнавання з урахуванням характеристик

Замість застосування в якості характеристик необроблених даних про яскравість пікселів можна використовувати методи виявлення та розмітки просторово локалізованих характеристик, таких як поля і краї. Застосування країв є доцільним завдяки двом описаним нижче важливих причин. Однією з них є зменшення обсягу даних, пов'язане з тим, що кількість країв набагато менше в порівнянні з кількістю пікселів зображення. Друга причина обумовлена можливістю домогтися інваріантності освітленості, оскільки краї (при наявності відповідного діапазону контрастів) виявляються приблизно в одних і тих же місцях, незалежно від точної конфігурації освітленості. Краї представляють собою одномірні характеристики; були також зроблені спроби використовувати двомірні характеристики (ділянки) і безмірні характеристики (точки). Зверніть увагу на те, як відрізняються трактування просторового розташування в підходах з урахуванням яскравості і з урахуванням характеристик. У підходах з урахуванням яскравості ці дані кодуються неявно, як індекси компонентів вектора характеристик, а в підходах з урахуванням характеристик, характеристикою є саме місцезнаходження (x, y).

Невід'ємною властивістю будь-якого об'єкта є інваріантне розташування країв; саме з цієї причини люди можуть легко інтерпретувати контурні малюнки, навіть незважаючи на те, що подібні зображення не зустрічаються в природі. Найпростіший спосіб використання цих знань заснований на класифікаторі по найближчих сусідніх точках. При цьому попередньо обчислюються і зберігаються дані про зміни країв, всім відомим образам. А після отримання конфігурації країв, яка відповідає невідомому об'єкту на зображенні, що є предметом запиту, можна визначити "відстань" цього об'єкта від кожного елемента бібліотеки де зберігаються

образи. Після цього класифікатор по найближчих сусідніх точках вибирає найбільш похожий образ.

Оцінка пози

Інтерес представляє не тільки завдання визначення того, яким є певний об'єкт, але і завдання визначення його пози, тобто його позиції і орієнтації по відношенню до спостерігача. Наприклад, при вирішенні проблеми маніпулювання об'єктами на виробництві доводиться враховувати, що захоплення робота не може взяти об'єкт до тих пір, поки не буде відома його поза. У разі жорстких об'єктів, як тривимірних, так і двомірних, ця проблема має просте і цілком визначене рішення, засноване на методі вирівнювання, який описаний нижче.

У цьому методі об'єкт представляється за допомогою характеристик, або помітних точок m1, m2,…mN в тривимірному просторі (як такі можуть, припустимо, розглядатися вершини багатогранного об'єкта). Координати цих точок вимірюються в деякій системі координат, найбільш підходящою для даного об'єкта. Після цього точки піддаються операції тривимірного обертання R з невідомими параметрами, за якою слідує операція перенесення на невідому величину t, а потім виконується операція проекції, яка призводить до появи точок характеристик зображення p1, p2,… pN на площині зображення. Оскільки деякі точки моделі можуть закривати один одного, а детектор характеристик може пропустити деякі характеристики (або виявити помилкові характеристики, поява яких обумовлена наявністю шуму). Таке перетворення для тривимірної моделі точок mi і відповідних точок зображення pi можна представити таким чином: де R - матриця обертання, t - вектор переносу; Чистим результатом стає трансформація Q, яка призводить точки моделі mi у відповідність з точками зображення pi. При цьому, хоча спочатку трансформація Q не визначена, відомо, що (застосовується до жорстких об’єктів) Q повинна бути однаковою для всіх точок моделі.

Open CV

OpenCV - розроблена Intel на C/C++ бібліотека з відкритим вихідним кодом, здатна значно спростити програмування комп'ютерного зору. Вона надає багато можливостей: детектування, відстеження та розпізнавання осіб, фільтрація Кальмана і різні готові до використання методи штучного інтелекту (II). Крім того через низькорівневий API надається велика кількість базових алгоритмів комп'ютерного зору.

Розуміння роботи методів дозволить отримати хороші результати від використання OpenCV. Тут буде описано, як, використовуючи OpenCV, реалізувати детектування, відстеження та розпізнавання осіб. Крім цього буде показано, як працює кожен метод і представлено кілька трюків для досягнення найкращих результатів.

Перша версія OpenCV була випущена Intel в 1999р. Спочатку для її використання потрібна Image Processing Library. Але ця залежність була видалена і тепер OpenCV може використовуватися незалежно.

OpenCV є багатоплатформною бібліотекою, вона підтримує Windows, Linux і MacOSX. З одним лише исключеним (модуль CVCAM, який буде описаний нижче), її інтерфейси платформо-незалежні.

Особливості

OpenCV має дуже багато можливостей і спочатку може здатися складною, але щоб почати знайомство потрібно зовсім не багато. Тут короткий опис найважливіших функціональних категорій в бібліотеці OpenCV версії 1.0:

Введення/виведення зображень і відео. Ці функції дозволяють читати зображення з файлів або з відео-потоків, а так само створювати зображення і відео.

Основні алгоритми комп'ютерного зору і обробки зображень (середньо- і низькорівневі API). Використовуючи цей інтерфейс можна експериментувати з більшістю стандартних алгоритмів комп'ютерного зору, без необхідності їх кодувати. Це включає пошуку перепадів, ліній і кутів, апроксимація еліпсом, піраміди зображень для різномасштабної обробки,

порівняння з еталоном (pattern matching), різні варіанти перетворень (Фур'є, дискретне косинус-перетворення) і багато іншого.

Модуль високорівневого комп'ютерного зору OpenCV включає кілька високорівневих можливостей, наприклад оптичний потік (optic flow) (використання руху камери для визначення тривимірної структури), калібрування камери і стереозору.

Методи ІІ і машинного навчання. Для додатків, що використовують комп'ютерний зір, часто потрібні методи машинного навчання або інші методи ІІ. Деякі з них доступні в пакеті OpenCV Mashine Learning.

Складання вибірки зображення і перетворення виду. Часто буває корисно обробляти групу пікселів, як блок. OpenCV містить функції для виділення областей зображення, випадкової вибірки, зміни розміру, обгортка, повороту і застосування ефектів перспективи.

Методи для створення і аналізу бінарних (двозначних) зображень. Бінарні зображення часто використовуються в перевірочних системах, які сканують на предмет дефекту форми або кількості частин. Бінарне представлення також зручно, коли об'єкт не рухомий.

Методи для обчислення тривимірної інформації. Ці функції корисні для складання карт і виявлення з використанням стерео оснащення або декількох зображень, отриманих однією камерою з різних точок огляду.

Математичні функції для обробки зображень, комп'ютерного зору і інтерпретації зображень. OpenCV включає часто використовувані алгоритми лінійної алгебри, статистики та обчислювальної геометрії.

Графіка. Цей інтерфейс дозволяє писати текст і малювати на зображеннях. Крім того ці функції корисні для для маркування та створення різних знаків. Наприклад, якщо ви пишете програму для детектування об'єкта, корисно написати на зображенні розмір і положення об’єкта.

Методи GUI. OpenCV містить власні функції для виведення вікон. Вони представляють просту мультиплатформену API для виведення зображень, допускають обробку подій миші та клавіатури і реалізують керуючий елемент повзунок.

Структури даних і алгоритми. З цими функціями ви можете ефективно створювати і маніпулювати великими списками, послідовностями, графами і деревами.



Рис. 2. Показує кілька прикладів можливостей OpenCV в дії: детектування особи, контуру і перепадів

Отже, такі методи покликані для вирішення поставлених задач в яких використовуються методи теорії, методи обробки цифрових зображень, теорії нейронних мереж. Програма, яка використовуватиме алгоритм, буде написана на мовах C# и C++ з використанням бібліотеки OpenCv.

Висновки. Зважаючи на складність завдання розпізнавання образів, а також використання нейронних мереж, завдання має бути розбите на два етапи:

- збір первинної інформації, розробка первинного рішення на основі обробки цифрових зображень з використанням бібліотеки OpenCV;
- підвищення ефективності розпізнавання та обробки зображень з використанням нейронних мереж .

Для вирішення завдань виявлення перешкод і розпізнавання образів необхідна наявність неспотвореного зображення. Однак більшість об'єктивів телекамер мають викривляє ефектом (аберацією). Об'єктиви, в яких повністю усунена аберація, мають високу вартість і великими масогабаритними характеристиками. Для усунення аберації об'єктиву телекамери пропонується використання алгоритму цифрової корекції спотворень на відеозображенні.

ЛІТЕРАТУРА:

1. Бойко И.А. Распознавание объектов на основе видеосигнала, полученного с камеры, установленной на подвижной платформе / Бойко И.А. – М.: Молодой ученый, 2013.
2. Юревич Е.И. Основы робототехники. – М.: БХВ-Петербург, 2007.
3. Степанченко И.В. Нейронные сети для распознавание образов / Степанченко И.В. Волгоград. гос. техн. ун-т. – М.: Волгоград, 2004.

REFERENCES:

1. Boyko I.A. Recognition of objects based on the video signal received from the camera mounted on a moving platform / Boyko I.A. – M.: Young Scientist 2013.
2. Yurevich E.I. Fundamentals of Robotics. – M .: BHV-Petersburg, 2007.
3. Stepanchenko I.V. Neural networks for pattern recognition / Volgograd. state. tehn. Univ. – M.: Volgograd 2004.

Рецензент: д.т.н., проф. Сбітнєв А.І.

д.т.н., проф. Мясіщев О.А., к.т.н. Лєнков Є.С., Білик О.М.

РАСПОЗНАВАНИЕ ГРАФИЧЕСКИХ ОБРАЗОВ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

В статье проведен анализ моделей надежности программного обеспечения (ПО). Наиболее известных моделей надежности ПО сегодня существует около десятка, поэтому в этой работе они сгруппированы по признакам.

Рассмотрены компьютерные системы с централизованной архитектурой приложений файл-сервер и клиент-сервер.

Особое внимание уделено клиент-серверной архитектуре. Существуют различные классификации, но одной из самых распространенных является использование четырех моделей технологии «клиент-сервер»: модель файлового сервера (File Server - FS), модель удаленного доступа к данным (Remote Data Access - RDA), модель сервера БД (Data Base Server - DBS), модель сервера приложений (Application Server - AS).

С целью оценки надежности для систем типа "клиент-сервер" на этапе тестирования определены такие важные характеристики функционирования программного комплекса, как: расчет текущего времени наработки до отказа, расчет среднего времени наработки до отказа за все время моделирования работы системы, расчет вероятности отказа ПО за единицу времени расчет коэффициента готовности.

Ключевые слова: надежность программного обеспечения, модели надежности, клиент-серверная архитектура, программа-клиент, область определения входных данных.

Prof. Myasischev O.A., Ph.D. Lenkov Ye.S., Bilik O.M.

RECOGNITION OF GRAPHIC IMAGES USING NEURAL NETWORKS

In the article the analysis of models of reliability of software (SOFTWARE). The most famous reliability models FOR today there are about a dozen, so in this work they are grouped by characteristics.

Considered a computer system with a centralized application architecture file-server and client-server.

Special attention is paid to the client-server architecture. There are various classifications, but one of the most common is the use of four models of the technology "Client-server": a model of file server (File Server FS), model RDA (Remote Data Access - RDA) model of the DB server (Data Base Server DBS), a model of the application server (Application Server - AS).

To assess reliability for systems of type "client-server" at the stage of testing identified the following important features of the operation of software, such as: calculation of the current operating time fully, the calculation of the average operating time fully during the simulation of the system, the calculation of the probability of failure per unit time, the calculation of the coefficient of readiness.

Keywords: software reliability, reliability models, client-server architecture, the client program, the scope of the input data.

УДК 004.891

д.т.н. с.н.с. **Селюков О.В.** (ТОВ «Укрспецконсалтинг»)
к.т.н., доц. **Огнєвий О.В.** (ХмНУ**)**
к.військ., доц. **Осипа В.О.** (ВІКНУ)
Бабій І.М. (ХмНУ)

РОЗРОБКА МОДЕЛЕЙ НАДІЙНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ТЕХНОЛОГІЇ ТИПУ «КЛІЄНТ-СЕРВЕР»

У статті проведено аналіз моделей надійності програмного забезпечення (ПЗ). Найбільш відомих моделей надійності ПЗ сьогодні існує близько десятка, тому в цій роботі вони згруповані за ознаками.

Розглянуто комп'ютерні системи з централізованою архітектурою додатків файл-сервер та клієнт-сервер.

Особливу увагу приділено клієнт-серверній архітектурі. Існують різні класифікації, але однією з найпоширеніших є використання чотирьох моделей технології «Клієнт-сервер»: модель файлового серверу (File Server - FS), модель віддаленого доступу до даних (Remote Data Access - RDA), модель сервера БД (Data Base Server - DBS), модель сервера додатків (Application Server - AS) .

З метою оцінки надійності для систем типу "клієнт-сервер" на етапі тестування визначено такі важливі характеристики функціонування програмного комплексу, як: розрахунок поточного часу напрацювання повністю, розрахунок середнього часу напрацювання повністю за весь час моделювання роботи системи, розрахунок імовірності відмови ПЗ за одиницю часу, розрахунок коефіцієнта готовності.

Ключові слова: надійність програмного забезпечення, моделі надійності, клієнт-серверна архітектура, програма-клієнт, область визначення вхідних даних.

Вступ. Прогнозування надійності програмного забезпечення (ПЗ) в процесі його експлуатації здійснюється на основі математичних моделей надійності програм.

В роботі [1] приведені імовірнісні моделі надійності. Теорія надійності для апаратного забезпечення розвинена досить добре, і є також можливість застосувати її і до надійності ПЗ. У цих моделях знаходиться число помилок, що залишилися в програмі. Це необхідно знати для завершення процесу тестування, і оцінки вартості супроводу, яка пропорційна кількості помилок, що залишилися в програмі. Також ці моделі дозволяють знаходити надійність програми, яка розуміється як вірогідність, що програма функціонуватиме без помилок впродовж заданого інтервалу часу, а також - середній час між відмовами програми.

Аналіз відомих досліджень і публікацій. На рисунку1 приведена класифікація моделей надійності ПЗ. Найбільш відомих моделей надійності ПЗ сьогодні існує близько десятка, тому в цій роботі вони згруповані за ознаками [1]. В якості класифікаційних ознак вибрані наступні:

– тимчасова структура процесів прояви помилок в ПЗ (час появи помилки, кількість помилок за заданий інтервал часу);

– складність програми (міра складності ПЗ - довжина, кількість функцій або модулів, даних і т.д.);

– розмітка помилок (штучне внесення в ПЗ відомих помилок);

– структура простору вхідних даних;

– структура тексту програми (розподіл помилок за текстом програми).

На практиці прості, елементарні помилки програм і даних можуть призводити до катастрофічних наслідків при функціонуванні ПЗ. В той же час, великі системні дефекти можуть тільки дещо погіршувати експлуатаційні характеристики ПЗ. Тому неможливо ранжирувати типи первинних помилок по мірі впливу на надійність та слід однаково ретельно відноситися до їх виявлення і усунення.

Статистика помилок в комплексних програмах і їх характеристики можуть служити орієнтиром для розробників при розподілі зусиль на відлагодження і оберігати їх від зайвого оптимізму при оцінці досягнутої якості і надійності ПЗ. Вони допомагають:

1. оцінювати реальний стан проекту і планувати необхідну трудомісткість і тривалість до його завершення;

2. вибирати методи і засоби проектування, програмування і тестування.

Реєстрація, збір і аналіз характеристик помилок в програмах є складним і трудомістким процесом. Тому є відносно невелике число робіт, в яких опубліковані реальні характеристики помилок.

При автономній роботі, і на початку комплексного відлагодження доля системних помилок невелика (~ 10%%), але вона істотно зростає (до 35-40%%) на завершальних етапах комплексного відлагодження. В процесі супроводу системні помилки є переважаючими (~ 80%% від усіх помилок).

Різними авторами були зроблені ряд уточнень вищевикладених моделей (до теперішнього часу запропоновані близько 15 математичних моделей для опису кількості помилок в ПЗ різної міри складності). Проте жодна з цих моделей не має явних переваг по точності апроксимації розподілів і прогнозування числа помилок в програмах в порівнянні з простою експоненціальною моделлю.

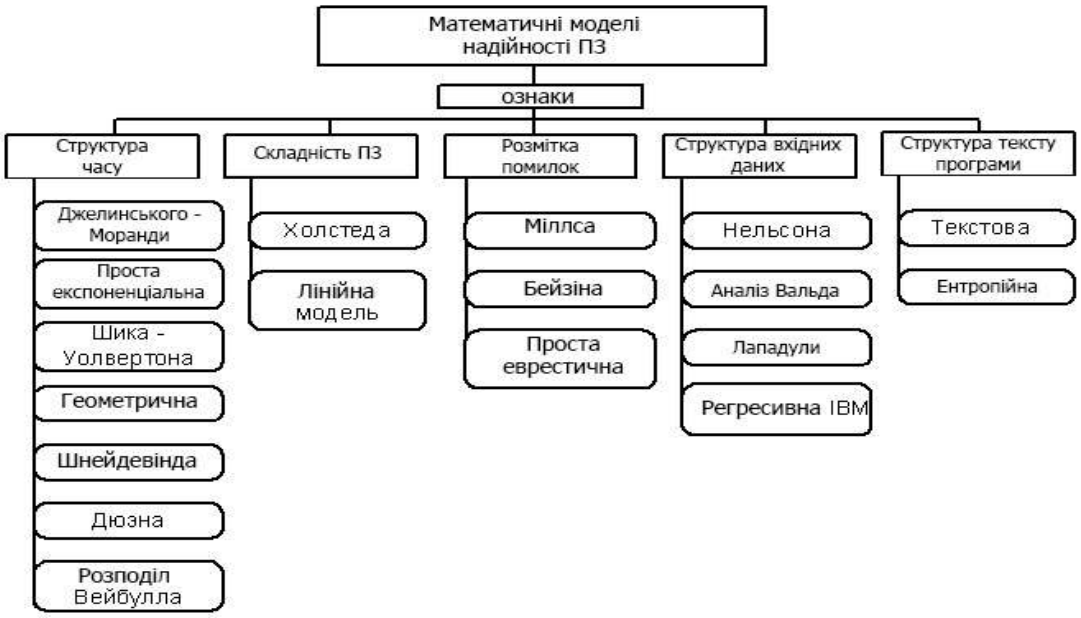


Рис. 1. Класифікація моделей надійності ПЗ

У роботі [2] приводиться порівняння моделей. Моделі Джелинського-Моранди і Шика-Уолвертона доцільні при моделюванні надійності ПЗ невеликого об'єму, а модифікована модель Шика-Уолвертона - для ПЗ великих проектів. Якщо при моделюванні необхідно отримати значення надійності (наприклад, середнє напрацювання повністю), то краще використати геометричні моделі. Деякі моделі не мають рішень (тобто розходяться за певних вхідних умов). Якщо є дані про інтервали часу між помилками, то краще скористатися геометричною моделлю, а якщо є дані про число помилок, що поступають одиницю часу, то краще застосовувати модель Шнейдевінда. Експоненціальна і дискретна моделі були перевірені при тестуванні реальних програм і добре відповідають дійсності [3].

В [2] робиться висновок, що на сьогодні неможливо вибрати найкращу модель серед десятка запропонованих.

Постановка задачі. Теорія надійності як наука отримала розвиток стосовно складних технічних систем. Необхідність і корисність контролю технічних компонентів систем і систем в цілому, з метою перевірки відповідності їх поточних характеристик заданим, доведені практикою. У цьому плані виконана значна кількість робіт по надійності стосовно технічних систем, розроблено безліч моделей забезпечення розумними методами надійності складних систем і їх технічної готовності.

Ці моделі у ряді випадків дозволяють не лише оцінювати показники надійності і готовності технічних систем і їх компонентів, але і дають можливість передбачати значення цих показників на основі накопиченого досвіду. Крім того, ряд моделей дозволяє на основі накопичених даних висловлювати припущення відносно режимів роботи, при яких найчастіше проявляються відхилення від нормального функціонування, а також про підхід до відновлення (ремонту) системи або її компонентів після збою.

Під системою в теорії надійності прийнято розуміти сукупність підсистем або елементів, функціонально об'єднаних відповідно до деякого алгоритму взаємодії при виконанні заданого завдання в процесі застосування за призначенням. Під це визначення системи повністю підходить програмне забезпечення.

Із-за значних невизначеностей в усіх вищеописаних моделях в [1] рекомендується використати декілька моделей одночасно і об'єднувати їх результати.

Таким чином, запропоновані моделі дають задовільний результат при відносно високих рівнях інтенсивності прояву помилок, тобто при невисокій надійності ПЗ. У цих умовах математичні моделі призначені для наближеної оцінки:

1) потенційно можливій надійності функціонування програм в процесі випробувань і експлуатації;

2) числа пропущених помилок;

3) часу тестування, потрібного для виявлення наступної помилки;

4) часу, необхідного для виявлення із заданою вірогідністю більшості наявних помилок.

Можна припустити, що оцінки, приведені для декількох конкретних систем, дозволять прогнозувати ці характеристики для інших проектів. Імовірнісний підхід до надійності ПЗ повинен дати відповідь на одне з найскладніших питань при тестуванні ПЗ - коли треба зупинитися і завершити тестування, тобто, на протязі якого часу треба тестувати програму, щоб вона задовольняла вимогам по надійності? За допомогою запропонованої в цій роботі моделі надійності можна отримати відповідь на це питання.

Виклад основного матеріалу. У міру збільшення числа ПЕОМ та підвищення кваліфікації користувачів, на підприємстві все сильніше усвідомлювалася потреба в швидкому, надійному і зручному способі оперативного обміну великими обсягами даних між комп'ютерами, а головне, між користувачами. Це дозволило б, як мінімум, передавати інформацію між окремими робочими місцями, а як максимум, вирішувати завдання більш високого рівня, об'єднувати окремі автоматизовані місця в інтегровані комплекси. І, природно, попит породив пропозицію - були створені локальні обчислювальні мережі та архітектури файл-сервер та клієнт-сервер.

Як і для файл-серверної архітектури, складовими компонентами клієнт-серверної архітектури є сервер, клієнтські місця і мережева інфраструктура. Однак, на відміну від попереднього випадку, сервер тут є вже не сервером файлів, а сервером баз даних або навіть сервером додатків. Таким чином, на сервер лягає не просто зберігання файлів, а підтримання бази даних в цілісному стані або, в разі сервера додатків, навіть виконання тієї чи іншої частини прикладної задачі. Природно, що вимоги до сервера при цьому можуть зростати в рази [2].

У своєму розвитку технології «клієнт-сервер» пройшли кілька етапів, тому є різні моделі технології. Їх реалізація заснована на поділі структури СКБД на три компоненти:

– введення і відображення даних (інтерфейс з користувачем);

– прикладний компонент (запити, події, правила, процедури та функції, які характерні для даної предметної області);

– функції керування ресурсами (файловою системою, базою даних тощо).

Існують різні класифікації, але однією з найпоширеніших є використання чотирьох моделей технології «Клієнт-сервер»:

1. Модель файлового серверу (File Server - FS) .
2. Модель віддаленого доступу до даних (Remote Data Access - RDA) .
3. Модель сервера БД (Data Base Server - DBS) .
4. Модель сервера додатків (Application Server - AS) .

Для забезпечення надійності програмного забезпечення усі ці моделі мають свої переваги та недоліки.

З метою оцінки надійності системи на етапі тестування необхідно визначити такі важливі характеристики функціонування програмного комплексу, як:

1) розрахунок поточного часу напрацювання повністю;

2) розрахунок середнього часу напрацювання повністю за весь час моделювання роботи системи;

3) розрахунок імовірності відмови ПЗ за одиницю часу;

4) розрахунок коефіцієнта готовності.

Це завдання має сенс і для систем типу "клієнт-сервер", рисунок 2.

Є ПЗ типу "клієнт-сервер". Сервер обслуговує запити від N програм-клієнтів (далі просто клієнти). У ПЗ рівномірно по області визначення вхідних даних (ОВД) (A, B) розташовані Er помилок.

Помилками (відмовами) ПЗ є:

Відмови в програмі. Якщо ПЗ не модифікується, то інтенсивність його відмов залишається постійною.

Внутрішні відмови в програмі. Такі відмови обумовлені фундаментальними обмеженнями алгоритму, що використовується в ПЗ (наприклад, використання евристичних алгоритмів може привести до випадкових відмов).

Відмови, обумовлені обмеженнями при функціонуванні в реальному часі. У даних системах середовище може змінюватися динамічно. Тому якщо планування або розрахунок відгуку занадто великий, то до моменту надходження відгуку середовище може бути вже змінене настільки, що розрахований або спланований відгук не матиме необхідного ефекту.

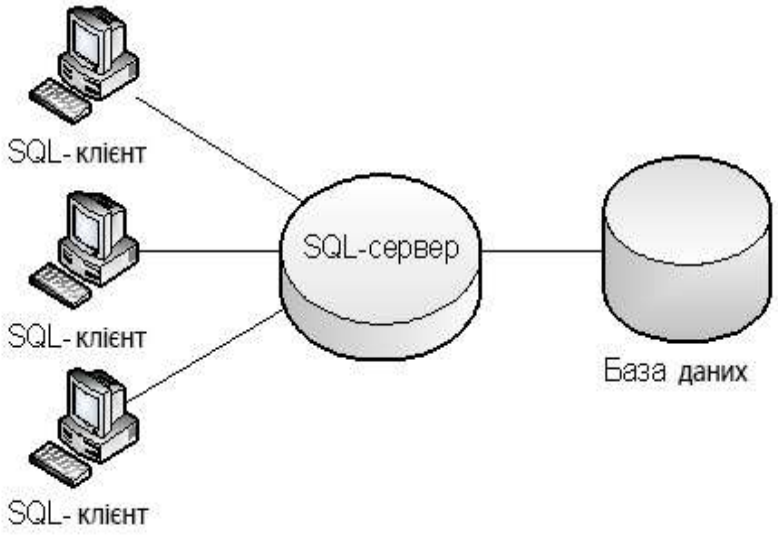


Рис. 2. Типова кліент-серверна структура

Сервер складніший за програми-клієнти з точки зору розробки ПЗ в S разів. S - коефіцієнт складності сервера по відношенню до клієнтів. Кожен k -ий (k = 1, 2, ..., N) клієнт породжує пуасонівський потік даних до сервера інтенсивністю $\lambda зв$. Дані від клієнта розподілені по ОВД за нормальним законом з характеристиками m_k і σ_k, де m_k розподілене між клієнтами рівномірно по усій області вхідних даних, σ_k - розподілене рівномірно на меншій ділянці m_k, що відсікаються, на осі області даних. Це потрібно для імітації нерівномірності використання ОВД при малій кількості клієнтів [3].

На запит клієнта сервер відповідає даними, які розподілені рівномірно по усій області визначення даних (A, B).

На рис. 3 зображений розподіл запитів одного клієнта по області усіх можливих запитів до сервера, а також показаний рівномірний розподіл помилок по ОВД. При попаданні запиту клієнта або відповіді сервера в область ОВД, що містить помилку, вважається, що помилка виявлена і відповідний модуль виводиться з експлуатації для її виправлення:

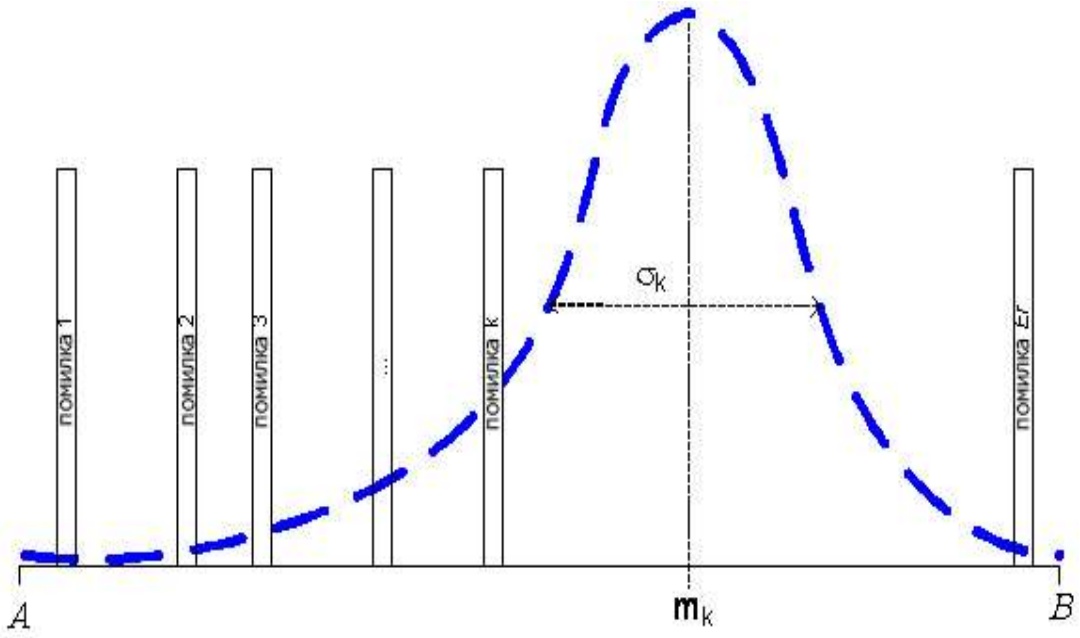


Рис. 3. Розподіл запитів k –го клієнта по області даних

Вхідними даними для моделі є:

P - кількість програмістів, обслуговуючих систему;

K - кількість програм-клієнтів;

α - ширина одного запиту клієнта як частина від ОВД (від 0 до 1, де 1 - це уся ОВД);

Δt - крок ітерації (доба);

s - коефіцієнт складності сервера в порівнянні з програмою-клієнтом;

$\lambda_{зв}$ - інтенсивність потоку звернень одного клієнта до сервера (1/доба);

$\lambda_{випр}$ - інтенсивність потоку виправлення помилки одним програмістом (1/доба);

$\lambda_{внес}$ - інтенсивність внесення помилки при виправленні одним програмістом (1/доба) або

$\rho_{внес}$ - імовірність внести помилку при виправленні одним програмістом;

M - кількість ітерацій (кількість спроб звернень програм-клієнтів до сервера в одному експерименті);

R - кількість експериментів для усереднення;

Er - початкова кількість помилок.

Для моделювання потоків запитів в ПЗ застосовується метод Монте-Карло.

Також є можливість оцінити первинну кількість помилок за наступним алгоритмом : Приймаємо ОВД за одиницю. Кожен клієнт в запиті генерує долю α; від ОВД. За час Δt клієнт звернеться до сервера ($\Delta t \cdot \lambda_{зв}$) разів. За час Δt усі клієнти звернуться до сервера ($\Delta t \cdot \lambda_{зв} \cdot K$) разів. І об'єм даних, який буде в ОВД при цьому рівний ($\Delta t \cdot \lambda_{зв} \cdot K \cdot \alpha$). Оскільки в нашій моделі помилки розподілені рівномірно по ОВД, то за час Δt буде виявлене ($\Delta t \cdot \lambda_{пом}$), де $\lambda_{пом}$ - первинна інтенсивність помилок в системі. Якби за час Δt клієнти звернулися в усю ОВД, то було б виявлено усі Er помилок. Тому, можна записати наступну пропорцію:

$$\frac{\Delta t \cdot \lambda_{зв} \cdot K \cdot \alpha}{\Delta t \cdot \lambda_{пом}} = \frac{1}{Er}.$$

Звідси знаходимо Er :

$$Er = \frac{\lambda_{пом}}{\lambda_{зв} \cdot K \cdot \alpha}.$$

При цьому вважається, що кожен з K клієнтів звернувся до сервера із запитом з даними, що не перетинаються в ОВД. Проте в реальності клієнти найчастіше звертаються до сервера з однотипними запитами, тому вважаємо $K = 1$ Тоді первинну кількість помилок можна оцінити як:

$$Er = \frac{\lambda_{ош}}{\lambda_{обр} \cdot \alpha}.$$

Висновки. Таким чином, вже на етапі тестування можливе передбачення характеристик ПЗ і оцінки часу, що необхідно витратити для досягнення заданого рівня надійності ПЗ при наявних ресурсах, та вироблення рекомендацій по підвищенню надійності ПЗ.

ЛІТЕРАТУРА :

1. Полонников Р.И. Методы оценки надежности программного обеспечения / Р.И. Полонников, А.В. Никандров. – СПб: Политехника, 1992. – 80 с.

2. Мясіщев О.А. Показники надійності захисту інформації у випадку системи із кінцевим числом діалогових каналів / А.В. Джулій, О.А. Мясіщев // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2010. – № 2. – С. 118-124.

3. Лєнков С.В.Динамічні показники оцінки рівня функціональної безпеки інформаційної системи / С.В Лєнков, В.М Джулій, І.В Муляр // Сучасна спеціалізована техніка. Науково-практичний журнал. – 2016. – № 2(45). – С. 59-68.

REFERENCES:

1. Polonnykov R.Y. Metodш otsenky nadezhnosty prohrammnoho obespechenyya / R.Y. Polonnykov, A.V. Nykandrov // – SPb: Polytekhnyka, 1992. – 80 s.

2. Myasishchev O.A. Pokaznyky nadiynosti zakhystu informatsiyi u vypadku systemy iz kintsevym chyslom dialohovykh kanaliv / A.V. Dzhuliy, O.A. Myasishchev // Vymiryuval'na ta obchyslyuval'na tekhnika v tekhnolohichnykh protsesakh. – 2010. – # 2. – C. 118-124.

3. Lyenkov S.V. Dynamichni pokaznyky otsinky rivnya funktsional'noyi bezpeky informatsiynoyi systemy / S.V. Lyenkov, V.M. Dzhuliy, I.V. Mulyar // Suchasna spetsializovana tekhnika. Nakovo-praktychnyy zhurnal. – 2016. – # 2(45). – C. 59-68.

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

д.т.н. с.н.с. Селюков А.В., к.т.н. Огневой А.В., к.військ., доц. Осыпа В.А., Бабий И.М.

РАЗРАБОТКА МОДЕЛЕЙ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ТЕХНОЛОГИИ ТИПА «КЛИЄНТ-СЕРВЕР»

В статье проведен анализ моделей надежности программного обеспечения (ПО). Наиболее известных моделей надежности ПО сегодня существует около десятка, поэтому в этой работе они сгруппированы по признакам.

Рассмотрены компьютерные системы с централизованной архитектурой приложений файл-сервер и клиент-сервер.

Особое внимание уделено клиент-серверной архитектуре. Существуют различные классификации, но одной из самых распространенных является использование четырех моделей технологии «клиент-сервер»: модель файлового сервера (File Server - FS), модель удаленного доступа к данным (Remote Data Access - RDA), модель сервера БД (Data Base Server - DBS), модель сервера приложений (Application Server - AS).

С целью оценки надежности для систем типа "клиент-сервер" на этапе тестирования определены такие важные характеристики функционирования программного комплекса, как:

расчет текущего времени наработки до отказа, расчет среднего времени наработки до отказа за все время моделирования работы системы, расчет вероятности отказа ПО за единицу времени расчет коэффициента готовности.

Ключевые слова: надежность программного обеспечения, модели надежности, клиент-серверная архитектура, программа-клиент, область определения входных данных.

prof. Selyukov A.V., Ph.D. Ognievyi O.V., Ph.D. Osupa V.A., Babiy I.M.

DEVELOPMENT OF RELIABILITY MODELS FOR SOFTWARE TECHNOLOGY TYPE "CLIENT-SERVER"

In the article the analysis of models of reliability of software (SOFTWARE). The most famous reliability models FOR today there are about a dozen, so in this work they are grouped by characteristics.

Considered a computer system with a centralized application architecture file-server and client-server.

Special attention is paid to the client-server architecture. There are various classifications, but one of the most common is the use of four models of the technology "Client-server": a model of file server (File Server FS), model RDA (Remote Data Access - RDA) model of the DB server (Data Base Server DBS), a model of the application server (Application Server - AS) .

To assess reliability for systems of type "client-server" at the stage of testing identified the following important features of the operation of software, such as: calculation of the current operating time fully, the calculation of the average operating time fully during the simulation of the system, the calculation of the probability of failure per unit time, the calculation of the coefficient of readiness.

Key words: software reliability, reliability models, client-server architecture, the client program, the scope of the input data.

УДК 528.94 к.т.н. **Хірх-Ялан В.І.** (ВІКНУ)

АСПЕКТИ АВТОМАТИЗАЦІЇ КАРТОГРАФІЧНО ГЕНЕРАЛІЗАЦІЇ ДЛЯ СТВОРЕННЯ ЕЛЕКТРОННИХ КАРТ ВІДПОВІДНИХ МАСШТАБІВ ТОПОГРАФІЧНОЮ СЛУЖБОЮ ЗБРОЙНИХ СИЛ УКРАЇНИ

У статті розглядаються методологічні та технологічні аспекти автоматизації картографічної генералізації цифрових картографічних даних для створення цифрових (електронних) карт, виробництва топографічної служби Збройних Сил України. Проведений аналіз поставленого завдання, досліджені проведені робіти в даному напрямку та науково-технічні рішення, що пропонуються.

Одним із першочергових завдань топографічної служби Збройних Сил України є підтримання в актуальному стані та оперативному забезпеченн військ (сил) якісними і об'єктивними просторовими даними цифрових (електронних) топографічних карт. Складовою частиною виконання поставлених завдань є автоматизація процессу генералізації картографічного зображення для цифрових топографічних карт різних масштабів.

Ключові слова: генералізація, картографічна генералізація, ГІС, цифрові карти.

Постановка завдання та аналіз існуючих публікацій. З розвитком ГІС як класу автоматизованих систем, ставляться вимоги до удосконалення методів виробництва і відображення геопросторової інформації, яка заснованана даних картографічних баз даних. Виникає необхідність відсікати ту частину інформації, яка не може бути відображена згідно обмеженнямм, які пов'язанийні з масштабом зображення. Таким чином, ставиться завдання автоматизувати генералізацію, тоб-то - відбір і узагальнення зображених на цифровій карті об'єктів відповідно масштабу. Виникає проблема отримання з докладних, детальних цифрових карт, більш узагальнених картографічнихдокументів, тобто цифрових карт меншого масштабу [1]. Сам процес генералізації багато в чому суперечливий. По-перше, деякі елементи не можуть бути показані на карті за умовами простору, але повинні бути відображені на ній в силу своєї власної значущості. Подруге, часто виникає суперечність між геометричною точністю і відповідністю зображення, інакше кажучи, просторові співвідношення об'єктів передаються вірно, а геометрична точність виявляється при цьому порушеною. По-третє, в ході генералізації відбувається не тільки виключення деталей зображення, втрата інформації, але і поява на карті нової узагальненої інформації. У міру абстрагування зникають зокрема і виразніше проступають найістотніші риси об'єкта, виявляються провідні закономірності, головні взаємозв'язки, виділяються геосистеми все більшого рангу.

Одним із проблемних питань при проведенні автоматизованої картографінчної генералізаці є формалізація самого процессу. Необхідним є автоматизувати процесс в цілому, виключити з нього дії картографа-укладача, які як правило мають субєктивный характер. Не всі етапи і процедури можуть бути алгоритмізовані, не всі критерії вдається однозначно формалізувати. Якість генералізації багато в чому залежить від розуміння картографом змістовної сутності зображуваних географічних (геологічних, соціально-економічних і т.п.) об'єктів і явищ, вміння виявити головні типові їх особливості. Досвід показує, що автоматизація карто-графічної генералізації повинна спиратися на інтерактивні, діалогові процедури. [3]

Також проблемним є питання формалізації структури даних вихідної цифрової топографічної карти (ЦТК). Оскільки структура ЦТК представлена у вигляді послідовного і, як правило, не структурованого списку об'єктів не містить інформації, необхідної для автоматичної генералізації. Формалізація структури даних має на меті ідентифікувати об'єкти ЦТК або їх сукупності, визначити топологічні відносини між ними, визначити ступінь їх важливості (пріоритету). Параметри які мають беззаперечний вплив на процес розпізнавання структури та її формалізації є наступні – масштаб карти, що виготовляється,

особливості території, які відображаються, редакційно-технічні вказівки стосовно виготовлення ЦТК на різні райони. Таким чином необхідно виділити основні типи процессів які мають складати бібліотеку функцій та визначають набір формальних параметрів для проведення автоматизації картографічної генералізації [2].

Мета статті. Виділити основні аспекти автоматизації процессів відбору картографічних обєктів, узагальнення кількісних та якісних характеристик обєктів для цифрових топографічних карт.

Викладення основного матеріалу. Процесс картографічної генералізації можливо описати як вибір об'єктів місцевості для відображення на карті. Наскільки детально має бути показаний кожний об'єкт, які ознаки об'єктів будуть важливими для користувача карти, а які - ні. Будь-яка карта - це завжди сильно зменшене зображення ділянки земної поверхні. Просто не можливо детально передати на карті абсолютно всі елементи місцевості, навіть якщо мова йде про карту крупного масштабу. Сутність картографічної генералізації навведена на рис 1.



М 1:50000 М 1:500000

Рис. 1. Ємона та околиці (Болгарія) на топографічних картах різних масштабів

Факторами, що визначають прийняття рішень в процесі генералізації, є: призначення карти; зміст карти; тип карти; масштаб карти; особливості території картографування; вивченність території; особливості оформлення карти. За ступенем важливості їх класифікують наступним чином:

першими є фактори призначення, змісту та типу карти, за ними визначається які саме з об'єктів території є необхідними для правильного сприйняття інформації;

другий важливий фактор для прийняття рішень про склад та, ступінь деталізації геометрії об'єктів карти, кількість якісних та кількісних характеристик місцевості - масштаб карти;

третім фактором є особливості території картографування, при генералізації картографічного зображення проявляється необхідность передати характерні особливості даної території, її відмінність від інших ділянок земної поверхні, за будь-яких умов відобразити окремі об'єкти, що відіграють важливу роль для здійснення певних видів діяльності; Як приклад, можна навести вимоги до відображення джерел води на картах засушливих та звичайних районів. У першому випадку на картах відображаються всі озера, дрібні річки, джерела, колодязі з позначенням їх характеристик, якщо озеро, наприклад, має

розміри занадто малі для даного масштабу карти його показують з перебільшенням розмірів. В той же час на територіях з нормальним режимом зволоження, об'єкти гідрографії показують лише за умов, що їх розміри є більшими за певну встановлену величину. Також суттєво змінюються вимоги до відображення рельєфу на картах одного і того ж масштабу залежно від того, чи є рельєф даної території рівнинним, горбистим або гірським, чи є територія переважно відкритою, чи вона вкрита лісом;

фактор вивченності території або об'єкту картографування визначає наскількі детально відображатимуться об'єкти чи певні ознаки будуть мати лише схематичний загальний вигляд;

фактор формату карти, кількість кольорів, що на ній буде застосовуватись, визначає скільки елементів місцевості чи об'єктів, що подають природні або суспільні явища, може бути вміщено на одиницю площі карти, щоб вона залишалася наглядною.

Методи картографічної генералізації. Відбір об'єктів – один з ключових методів картографічної генералізації, що полягає у визначенні які з об'єктів місцевості доцільно відобразити на карті, виходячи з її змісту та призначення, а також плануємого навантаження.В першу чергу відбір робиться, виходячі з фактору призначення карти: робиться аналіз, які саме об'єкти та характеристики місцевості мають значення для карти даної тематики. Наприклад, якщо мова йде про політико-адміністративну карту, то для користувача є дуже важливим показати які населені пункти входять до тієї, чи іншої адміністративної одиниці, але не дуже важливо показати всі водойми та водотоки. Але наприклад, якщо створюється карта грунтів того ж масштабу, то річкова мережа має дуже важливе значення, в той час як населені пункти крім крупних, що займають значні площі, мають значення лише з точки зору орієнтування по карті. По-друге, відбір об'єктів і відкидання частини з них приходиться виконувати і для карт однакового змісту, але різних масштабів. В цьому випадку прагнуть забезпечити прийнятний рівень навантаження карти. При відборі об'єктів оперують двома кількісними показниками: ценз та норма відбору.

Ценз - це обмежуючий параметр, що визначає значимість об'єктів для нанесення їх на карту даного типу та масштабу. Як приклади цензів, можна навести наступні вимоги щодо нанесення на топографічні карти різних масштабів певних об'єктів гідрографії «4.3.4. Річки та струмки наносять: на картах масштабів 1:10000-1:25000 - всі, незалежно від їх довжини; - на картах масштабів 1:50000-1:200000 - як правило, довжиною в масштабі карти 1 см та більше; - на картах масштабів 1:500000-1:1000000 - як правило, довжиною 1,5 см та більше в масштабі карти».

Норма відбору - це параметр, що визначає, яку кількість об'єктів на одиницю площі карти слід нанести, щоб карта мала прийнятний рівень навантаження та правильно відображала певні ознаки місцевості. Так, наприклад, "Основні положення створення та оновлення топографічних карт" визначають, що на карті масштабу 1:1 000 000 для густонаселених районів слід наносити не більше ніж 120 -140 населених пунктів на 1 кв. дм карти, а для малонаселених - не більше ніж 60-80 населених пунктів на 1 кв. дм карти.

Узагальнення якісних характеристик - метод генералізації, що полягає в зменшенні кількості об'єктів певного типу шляхом узагальнення їх якісних характеристик, і поєднання таким чином об'єктів, що раніше відрізнялися друг від друга певними ознаками, в один.

Узагальнення кількісних характеристик - метод генералізації, що полягає в зменшенні кількості об'єктів карти, які подають значення певних величин, шляхом збільшення довжини інтервалів значень.

Перехід від простих об'єктів до складних як метод генералізації полягає у використанні на дрібномасштабній карті одного складного (інтегрального) об'єкту, що заміняє певну кількість реальних об'єктів місцевості.

Узагальнення контурів - метод генералізації, що полягає у зменшенні кількості деталей у геометрії об'єктів. Наприклад, замість показу всіх згибів русла річки на дрібномасштабній карті показують лише загальний вигляд русла.

Поєднання контурів - один з найскладніших прийомів картографічної генералізації, що полягає у відображенні на карті замість кількох контурів окремих однотипних об'єктів одного спільного контуру. Наприклад, замість кількох дрібних окремих озер на карті може бути показано одно. Але слід враховувати, що цей метод генералізації приводить до суттєвого викаження змісту карти і може легко привести до невірного розуміння користувачем особливостей місцевості.

Показ об'єктів з перебільшенням - метод, що застосовується, коли необхідно показати на карті певні об'єкти або елементи контуру, розміри яких надто дрібні для відображення у даному масштабі карти, але наявність таких об'єктів дуже важлива з для правильного відображення території [8].

Дані зображені у ГІС у цифровій формі, що забезпечує їх введення до комп'ютерного середовища, зберігання, опрацювання й перетворення з метою відтворення вже існуючих картографічних творів або створення нових. Складовими ГІС є банки й бази даних [5].

Серцевину всілякої ГІС складає автоматизована система картографування – комплекс приладів і програмних засобів, що забезпечують створення і використання карт.

Така система складається із ряду підсистем, найважливішими з яких являються підсистеми вводу, обробки і виводу інформації.

Підсистема вводу інформації – це пристрої для перетворення просторової інформації в цифрову форму і вводу її в пам’ять комп’ютера чи в базу даних.

Банки даних для картографічних цілей є інформаційною системою централізованого збереження й колективного використання потрібних для створення карт відомостей у цифровому вигляді. База даних включає два типи інформації: просторову (метричну) то, описову (семантичну). Вони зберігаються в комп'ютерному середовищі у вигляді набору файлів, які відповідають за просторову або описову інформацію про об'єкти карти.

Підсистема обробки інформації складається з самого комп’ютера, системи управління і програмного забезпечення. Створені сотні різноманітних спеціалізованих програм (пакетів програм), які дозволяють вибирати потрібну проекцію, прийоми генералізації і способи зображення, будувати карти, суміщати їх одна з одною, візуалізувати і виводити на друк. Програмні комплекси спроможні виконувати і більш складні роботи: проводити аналіз території, дешифрувати знімки і класифікувати картографовані об’єкти, моделювати процеси, спів ставляти, оцінювати альтернативні варіанти і вибирати оптимальний шлях вирішення [4,5].

Більша частина підсистем обробки інформації працюють в діалоговому (інтерактивному) режимі, в ході якого йде безпосередній двосторонній обмін інформацією між картографом і комп’ютером.

Уся інформація ЦТК виробництва топографічної служби Збройних Сил України формується пошарово, Тобто кожен шар є сховищем цифрової картографічної інформації певного змісту, яка може бути поданою на екран комп'ютера.

При використанні ГІС-технологій автоматизована генералізація контурів (берегової лінії, гідрографії та інших лінійних об'єктів), за умови вдало підібраного алгоритму, майже не потребує ручного редагування, крім окремих випадків, коли потрібно показати острів чи озеро навіть тоді, коли вони не обов'язкові для якогось іншого масштабу. Комп'ютерне виготовлення карт потребує програмного забезпечення, але не вся інформація, яка потрібна для створення карт, може бути формалізована й алгоритмізована.

Складність алгоритмів зростає з ускладненням змісту карти. Труднощі виникають і через протиріччя між вимогами геометричної точності карт і географічною відповідністю до їх змісту, що виникають під час використання на картах позамасщтабних позначень та у процесі генералізації зображення, через складність або навіть неможливість опису математичним апаратом взаємозв'язків між різними об'єктами тощо. Формальне розв'язання проблем створення картографічного зображення, притаманне технічним засобам, може привести до спотворення типових ознак зображених об'єктів (напр., не будуть показані

важливі об'єкти внаслідок їх малих розмірів, чого фахівець не допустить, штучно збільшуючи їх розміри) [6,7].

Розробниками програмного забезпеченння ТОВ "ГІСІНФО", ЗАО КБ «Панорама» [9]. Розробляється технологія часткової автоматизації картографічної генералізації. Наведемо основні її етапи:

Процес перетворення карти складається з ряду етапів:

- формування номенклатурного аркушу карти похідного масштабу;
- перекодування об'єктів;
- генералізація опорних пунктів;
- генералізація гідрографії й гідротехнічних споруджень;
- генералізація кварталів населених пунктів;
- генералізація рельєфу;
- генералізація об'єктів малої довжини або площі;
- зведення із суміжними аркушами.

Формування номенклатурного аркушу карти похідного масштабу складається з наступних прцесів: формування паспорта номенклатурного аркуша; перенос об'єктів з витягуванням на рамку; згладжування топологично-зв'язаних об’єктів; сшивання об'єктів уздовж ліній зведення.

Формування паспорта номенклатурного аркуша. При виконанні завдання **“**Зшивання аркушів карти” рис.2 для кожних чотирьох аркушів цифрової топографічної карти вихідного масштабу автоматично формується один аркуш карти відповідного похідного масштабу:

для 4 аркушів масштабу 1:25 000 - 1 аркуш масштабу 1:50 000;

для 4 аркушів масштабу 1:50 000 - 1 аркуш масштабу 1:100 000.

Вибір аркушів карти вихідного масштабу виконується автоматично по номенклатурі аркуша карти похідного масштабу.

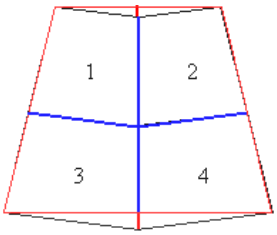


Рис. 2. Зшивання аркушів цифрових топографічних карт

Перенесення об'єктів з витягуванням на рамку. Перенесення об'єктів із чотирьох аркушів вихідної карти в карту похідного масштабу виконується в повному обсязі, за винятком рамок аркушів вихідної карти. При цьому деякі точки об'єктів, що виходять на рамку, мають невеликі розбіжності з метрикою рамки. Максимальні розбіжності показані червоною стовщеною лінією (див. Схему зшивання аркушів топографічних карт). Для виключення розбіжностей при переносі об'єктів виконується автоматичне витягування точок об'єктів до рамки похідного листа (тонка червона лінія) рис. 2.

Згладжування топологично-зв'язаних об’єктів. Автоматичне згладжування метричного опису лінійних і площадних об'єктів карти з обліком наявних просторових топологічних зв'язків виконується відповідно до встановленої точності згладжування (у міліметрах на карті).

Зшивання об'єктів уздовж ліній зведення. По закінченні перенесення об'єктів виконується зшивка об'єктів уздовж ліній зведення. У процесі процедури зшивки об'єктів виконується пошук відповідних пар об'єктів уздовж ліній зшивки з урахуванням семантики. Семантика об'єктів, що зшивають, зберігається з обох об'єктів, окрім випадку наявності в оброблюваних об'єктів суперечливої семантики. При відсутності одного з пари об'єктів, або наявності в об'єктів пари суперечливої семантики зшивка об'єктів не виконується й виводиться повідомлення про помилку до протоколуі помилок. Зшивання об'єктів

виконується відповідно до встановленої величини допуску для зшивання (у міліметрах на карті).

Формування математичної основи. У процесі формування спочатку виконується автоматичне видалення об'єктів математичної основи вихідної карти, потім - автоматичне створення об'єктів математичної основи (горизонтальні й вертикальні координатні лінії прямокутної сітки, точки перетину координатних ліній, виходи паралелей і меридіанів, центральний хрест). Склад створюваних об'єктів математичної основи залежить від масштабу формованої карти.

Перекодування об'єктів. Процедура перекодування використовується для зміни класифікатора карти. При цьому виконується налаштування таблиць відповідності ключів об'єктів і кодів семантичних характеристик класифікатора вихідної карти ключам об'єктів і кодам семантичних характеристик класифікатора похідної карти. У процесі використовуються два класифікатори й таблиця перекодування, що містить списки відповідності ключів об'єктів і кодів семантичних характеристик класифікатора вихідної карти ключам об'єктів і кодам семантичних характеристик класифікатора похідної карти.

Генералізація опорних пунктів. По картах більшого масштабу виконується округлення координат точок планової основи (пункти державної геодезичної мережі, геодезичної мережі згущення, астрономічні пункти, марки й репери нівелірної мережі).

У режимі автоматичної генералізації опорних пунктів у координати точок планової основи заноситься випадкова помилка відповідно до встановленої величини розкиду й наступним округленням із установленою точністю (у міліметрах на карті).

Генералізація гідрографії й гідротехнічних споруд. У процесі процедури генералізації виконується автоматична заміна ділянок площинних об'єктів, що мають ширину менш припустимої (у міліметрах на карті), на ділянки лінійних об'єктів.

Площинні об'єкти перетворяться в лінійні об'єкти відповідно до таблиці перекодування рис. 3.



Рис. 3. Приклад автоматизованої генералізації площинних об’єктів гідрографії (ріка має лінійний вигляд, притоку дотягнуть до нової метрики ріки)

Генералізація кварталів населених пунктів. З метою поліпшення наочності зображення кварталів виконується об'єднання дрібних кварталів, а також збільшення ширини проїздів. Обробка кварталів виконується в три етапи: автоматизоване формування проїздів; зміщення кварталів, видалення зайвих проїздів; автоматизоване формування кварталів.

Генералізація рельєфу. Генералізація рельєфу містить у собі генералізацію ізоліній (горизонталей, ізобат) і генералізацію точкових об'єктів рельєфу.

У процесі генералізації ізолінії (горизонталі) або віддаляються, або перетворяться до точкових об'єктів з абсолютною висотою. Разом з віддаленими горизонталями, що, віддаляються також бергштріхи й підписи, які їм належать.

Генералізація об'єктів малої довжини або площі. У процесі генералізації об'єктів малої довжини або площі обробляються лінійні й площадні об'єкти карти. Ступінь малості довжини визначається встановленої в параметрах задачі характеристикою. Мінімальна довжина об'єкта (у міліметрах на карті), ступінь малості площі – характеристикою. Мінімальна площа об'єкта (у міліметрах на карті). При обробці об'єктів виконуються наступні процеси: зшивання лінійних незамкнутих об'єктів малої довжини; зшивання площинних об'єктів малої площі; заміна типу лінійних і площинних об'єктів на точкові об'єкти. Прилеглі лінійні незамкнуті об'єкти малої довжини одного типу й площадні об'єкти одного типу зшиваються. Зшивання лінійних об'єктів виконується при розміщенні в допуску близькості між кінцевими точками метрик (характеристика Максимальна відстань зшивання лінійного об'єкта**).** Зшивання площинних об'єктів виконується при розміщенні в допуску близькості самих об'єктів (характеристика Максимальна відстань зшивання площинного об'єкта).

Незшиті об'єкти малої довжини або площі перетворяться в точкові об'єкти відповідно до таблиці перекодування рис. 4.

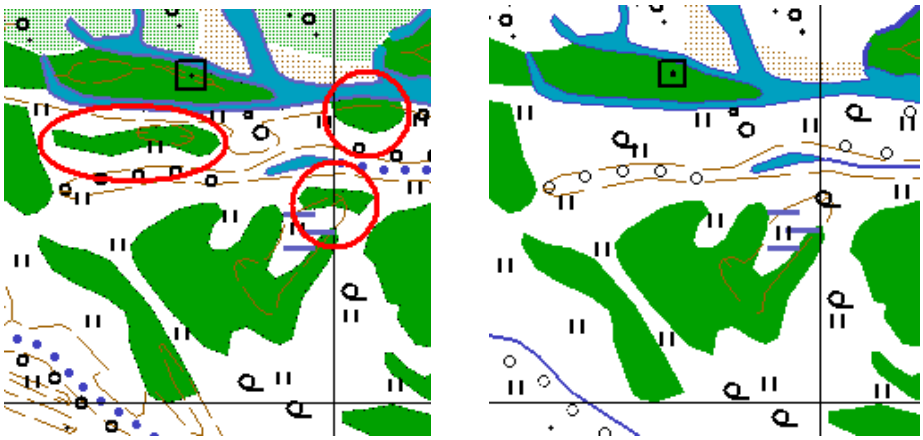


Рис. 4. Ліси малої площі до виконання процедури автоматичної вибірки малих об'єктів, ліси малої площі відалені в процесі роботи процедури

Зведення із суміжними аркушами. Зведення номенклатурних аркушів електронної карти має на меті програмно-візуальний контроль і редагування інформації про об'єкти, що виходять на рамку з метою визначення однозначних, погоджених характеристик суміжних об'єктів відповідно до правил цифрового опису.

Після виконання прикладної задачі засобами редактору векторної карти проводиться візуальний аналіз результатів обробки.

Висновки. Виходячи з вищезазначеного, слід зауважити, що основним аспектом автоматизованої генералізації цифрової картографічної інформації є формалізація задачі генералізації, що на даний момент пов’язана з деякими технічними складностями. А саме, неоднорідність самого завдання по генералізації різних картографічних матеріалів, значні протиріччя при формалізації задачі генералізації для різних районів картографованої території. Необхідно визначити параметри які мають беззаперечний вплив на розпізнавання структури ЦТК – масштаб карти, редакційно-технічні вказівки стосовно виготовлення ЦТК на різні райони. Розроблена та запропонована технологія автоматизації процесу генералізації базується на перекодуванні об'єктів, що в свою чергу передбачає створення нових уніфікованих класифікаторів карти для різних масштабів ЦТК та районів картографування.

ЛІТЕРАТУРА:

1. Зулгарина Д.А. Сплайн-аппроксимация как метод автоматизированной генерализации [Електронний ресурс] / Д.А. Зулгарина // SWorld. – 2011. – Режим доступу :

http://www.sworld.com.ua/index.php/ru/technical-sciences-311/informatics-computer-science-and-automation-311/7998-as-a-method-of-automated-splaynapproksimatsiya-generalization.

2. Хлебникова Т.А. Технология автоматизированной генерализации при картографировании / Т. А. Хлебникова, С. В. Колосков // Геодезия и картография. – 2005. – № 6. – С. 38–41.

3. Бровко Е.А. Государственный топографический мониторинг. Автоматизированная генерализация цифрового картографического изображения. Методологические и технологические аспекты (Ч.1) / Е. А. Бровко, Р. Э. Софинов // Геодезия и картография. – 2015. – № 11. – С. 20–25.

4. Берлянт А.М. Картография: учебник для вузов / А.М. Берлянт – М.: Аспект-Пресс, 2001. – 336 с.

5. Божок А.П. Картографія : підручник / А.П. Божок А. П., Молочко А. М., Остроух В. І.; за ред. А. П. Божок. – К. : ВПЦ "Київський університет", 2008. – 271 с.

6. Козаченко Т.І. Картографічне моделювання: навчальний посібник / Т. І. Козаченко, Г.О. Пархоменко, А.М. Молочко; під ред. А. П. Золовського. – Вінниця: Антекс-У ЛТД, 1999. – 328 с.

7. Можливості використання комп'ютерної техніки для створення картографічної продукції [Електронний ресурс] / Geograf.com.ua. – Режим доступу :
http://www.geograf.com.ua/library/geoinfocentre/22-geoinfocentre-kartography/285-referat09.

8. Картографічна генералізація [Електронний ресурс] / GeoGuide. – Режим доступу :
http://www.geoguide.com.ua/survey/survey.php?part=map&art=map500.

9.Технології автоматизованої генералізації : Проекти – комплексні рішення по розробці спеціалізованих ГІС на основі ГІС "Карта 2011" [Електронний ресурс] / Розроб. : ЗАО "КБ Панорама". – Режим доступу : http://panorama.vn.ua/projects/19.php.

REFERENCES:

1. SWorld (2011). Splajn-approksymacyja kak metod avtomatyzyrovannoj generalyzacyy [Spline as a method for automated generalization]. Available at: http://www.sworld.com.ua/index.php/ru/technical-sciences-311/informatics-computer-science-and-automation-311/7998-as-a-method-of-automated-splaynapproksimatsiya-generalization.

2. Hlebnykova T.A., Koloskov S.V. Tehnologyja avtomatyzyrovannoj generalyzacyy pry kartografyrovanyy [Technology of automated generalization for mapping]. Geodezyja y kartografyja [Surveying and mapping], 2005, no. 6, pp.38–41.

3. Brovko E.A., Sofynov R. E. Gosudarstvennij topografycheskyj monytoryng. Avtomatyzyrovannaja generalyzacyja cyfrovogo kartografycheskogo yzobrazhenyja. Metodologycheskye y tehnologycheskye aspekti [State topographical monitoring. Automated generalization of digital cartographic images. Methodological and Technological Aspects], Geodezyja y kartografyja [Surveying and mapping], 2015, no 11, pp. 20–25.

4. Berljant A.M. (2001) Kartografyja [Cartography] Moscow, Aspekt-Press publ., 336 p. 57 (In Russian).

5. Bozhok A.P., A.M. Molochko, V.I. Ostrouh (2008). Kartografyja [Cartography] Kyiv, Kyi'vs'kyj universytet publ., 271 p.

6. Kozachenko T.I., Parhomenko G.O., Molochko A. M. (1999) Kartografichne modeljuvannja [Cartographic modeling]. Vinnycja: Anteks-U LTD publ., 328 p.

7. Mozhlyvosti vykorystannja komp'juternoi' tehniky dlja stvorennja kartografichnoi' produkcii' [Possibilities of using computer technology for creating cartographic products] Available at: http://www.geograf.com.ua/library/geoinfocentre/22-geoinfocentre-kartography/285-referat09.

8. Kartografichna generalizacija [Cartographic generalization] Available at: http://www.geoguide.com.ua/survey/survey.php?part=map&art=map500.

9. Tehnologii' avtomatyzovanoi' generalizacii': Proekty – kompleksni rishennja po rozrobci specializovanyh GIS na osnovi GIS "Karta 2011" [Technologies automated generalization: Projects - integrated solutions to develop specialized GIS-based GIS "Map 2011"] Available at: http://panorama.vn.ua/projects/19.php.

Рецензент: к.т.н., с.н.с. Жиров Г.Б., провідний науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка

к.т.н. Хирх-Ялан В.И.

АСПЕКТЫ АВТОМАТИЗАЦИИ КАРТОГРАФИЧЕСКОЙ ГЕНЕРАЛИЗАЦИИ ДЛЯ СОЗДАНИЯ ЭЛЕКТРОННЫХ КАРТ СООТВЕТСТВУЮЩИХ МАСШТАБОВ ТОПОГРАФИЧЕСКОЙ СЛУЖБОЙ ВООРУЖЕННЫХ СИЛ УКРАИНЫ

В статье рассматриваются методологические и технологические аспекты автоматизации картографической генерализации цифровых картографических данных для создания цифровых (электронных) карт, производства топографической службы Вооруженных Сил Украины. Проведен анализ поставленной задачи, исследованы проведенные работы в данном направлении и научно-технические решения, которые предлагаются.

Одной из первоочередных задач топографической службы Вооруженных Сил Украины является поддержание в актуальном состоянии и оперативное обеспечение войск (сил) качественными и объективными пространственными данными цифровых (электронных) топографических карт. Составной частью выполнения поставленных задач является автоматизация процесса генерализации картографического изображенния для цифровых топографических карт различных масштабов.

Ключевые слова: генерализация, картографическая генерализация, ГИС, цифровые карты.

Ph.D. Khirkh-Ialan V.I.

ASPECTS OF AUTOMATION FOR CARTOGRAPHIC GENERALIZATION CREATING ELECTRONIC MAPS OF APPROPRIATE SCALE TOPOGRAPHIC SERVICE ARMED FORCES OF UKRAINE

The article deals with methodological and technological aspects of automated cartographic generalization of digital map data for the creation of Digital (electronic) maps, production of topographic service of the Armed Forces of the Ukraine. The analysis of the problem, studied the work carried out in this direction and technological solutions that are offered.

One of the priorities Topographic Service of the Armed Forces of Ukraine up to date operational support of troops (forces) quality and objective spatial data, An integral part of the implementation of the tasks is to automate the process of generalization of cartographic images for digital topographic maps of different scales.

Keywords: generalization, cartographic generalization, GIS, digital maps.

УДК 681.518.5

Ph.D. **Gostev V.V.** (KNU)
Ph.D. **Pampuha I.V.** (MIKNU)
Ph.D. **Savkov P.A.** (MIKNU)
Ph.D. **Savkova V.P.** (KNU)

A TYPICAL FUZZY CONTROLLER

In the article was made an analysis of the Bandwidth capacity data, which are indicating that when using the PI-method, the bandwidth capacity of channel with overload decreases with increase of the UDP-stream density.

A typical controller based on fuzzy logic (Fuzzy Logic Controller, FLC) is described in the article. Functional scheme of the FLC is presented. The structure of fuzzy controller is given. The table of fuzzy rules of the controller and its architecture is presented. Experimental data on queue lengths are presented. A review of controllers based on REM-method of active queue management (FREM, STREM, FEM) is given and conclusions concerning their impact on the router parameters are made.

It is proved that when the PI-method is used, the bandwidth capacity of channel with overload decreases with increase of the UDP-stream density. The RED-method has more stable bandwidth capacity when the UDP-stream density is varied. However, the highest and the most stable results are observed when using the FLC controller. The main advantage of the FLC-controller is that the length of the queue is stable with variation of the network parameters.

Keywords: fuzzy controller, fuzzy controller architecture, the membership functions of the input and output variables.

Introduction. In the article was made an analysis of the Bandwidth capacity data, which are indicating that when using the PI-method, the bandwidth capacity of channel with overload decreases with increase of the UDP-stream density. The RED-method has more stable bandwidth capacity when the UDP-stream density is varied. However, the highest and the most stable results are observed when using the FLC controller.

The main advantage of the FLC-controller is that the length of the queue is stable with variation of the network parameters.

Typical controller based on fuzzy logic, membership functions of the input and output variables and fuzzy rules used for the controller are described in the paper. Response surface of fuzzy controller is presented. Topology and results of simulations are presented.

Problem statement. The buffers of network routers are overloaded due to non-uniform growth of capacities of channels. Basic methods of active queue management and congestion avoidance (RED, PI, REM) can not fully cope with the management of traffic with complex dynamics, high burst and non-linearity of load changes. As a result, an overload of the router buffer occurs and global synchronization of TCP flows takes place [1]. This in turn reduces the effective data rate and degrades quality parameters, such as packet loss ratio, delays and delay variations.

When using DropTail, a passive queue management method for TCP traffic manadement, the global synchronization takes place. This phenomenon is that when the buffer is overflowed, a reset of all incoming packets takes place, and all the transmitters of TCP/IP network initially reduce the TCP window, and then synchronously increase it, causing a new overload. As a countermeasure to global synchronization, the REM-algorithm of randomly-exponential drop/labelling of incoming packets during the buffer overflow was developed. The algorithm is based on a mesure ("price") of overload.

There are also some modifications of REM (FREM, STREM, FEM) which were developed for improvement of the network characteristics.

A controller based on fuzzy logic (FLC) is used to ensure the normal operation of the active queue management systems based on the REM-method. The FLC showed good results in management of non-linear systems with complex dynamics.

A typical controller based on fuzzy logic (FLC) is described in the article. A review of controllers based on REM-method of active queue management (FREM, STREM, FEM) is given and conclusions concerning their impact on the router parameters are made.

Results of calculations and oscillogramms. The theory of fuzzy sets describes and operates by imprecise concepts, and also makes vague conclusions. Fuzzy control is particularly useful when the investigated processes are too complex for analysis and when the information sources are interpreted qualitatively. Availability of mathematical tools for description of vagueness allows to build an adequate model of reality.

The FLC (Fig. 1) decides to change the current value of the probability of the package drop/labeling Pdrop taking into account the following parameters: errors of current queue length Qerror, its change during the measurement derror, and appropriate set of rules based on expert judgment. For the input variables, the value of membership function u is calculated, i.e. the degree of confidence that the input variable is the fuzzy (linguistic) variable, such as "large", "small" and "medium". The membership functions are selected from condition that the sum of all the functions of the input variable should be equal to one.

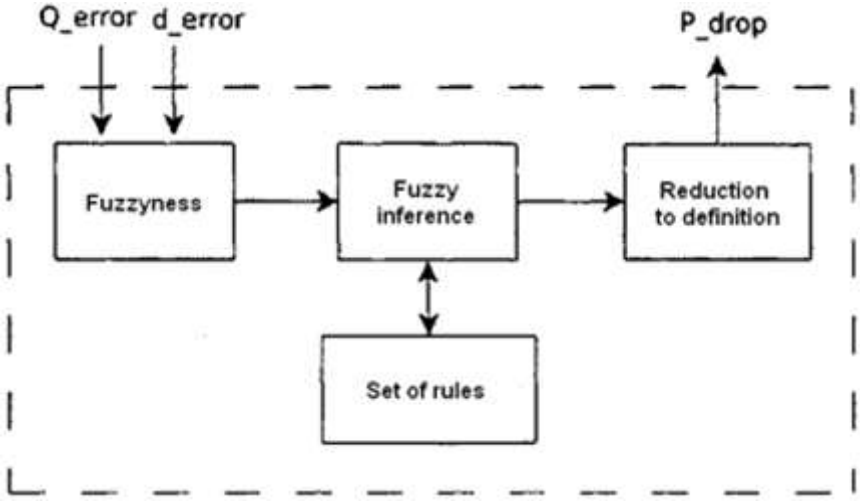


Fig. 1. Architecture of FLC

One of the most common algorithms of fuzzy inference is the Mamdani algorithm. Fuzzy inference is based on a set of rules: the value of truth for each rule premise is calculated (operation minimum). An example of linguistic rule: IF (Q_{error} = "LARGE") and (d_{error} = "SMALL") THEN (P_{drop} = "MEDIUM"). All fuzzy sets derived from rules are aggregated together and a single fuzzy set ^{C} is formed (operation maximum). Reduction to definition is done, for example, by using a discrete method of "center of gravity":

$$P_{drop} = \frac{\sum_{j=1}^{m} y_j \cdot \mu_C y_j}{\sum_{j=1}^{m} \mu_C y_j}, \quad (1)$$

where y_j is a discrete value of the output variable from ^{m} values,

and μ_C is membership function of aggregated set ^{C}.

The main advantage of the congestion control algorithms based on fuzzy logic, is that they do not use the mechanism of dropping packets, but calculate packet losses according to a pre-configured fuzzy logic with use of queue length and the buffer usage ration [3]. So, the proposed algorithms reach higher bandwidth capacity, more stable values of the queue length. As a result, they improve the ability of routers to manage congestion in TCP/IP networks in comparison with schemes which use basic AQM-algorithms. The main objective of the AQM methods is tracking the congestion level in the network and notification the message sources (input packets) about this, in order to reduce their transmission rate. In actual practice, overloads occur when the required

bandwidth exceeds the available capacity of the communication channel, which results in drastic deterioration of the network characteristics since the packet loss increases and the channel usage decreases. In order to prevent these problems, a fuzzy logic is widely used in TCP/IP networks which can well adapt for dynamic environment without accurate model and provides the non-analytic approach in design of dynamic and fast control schemes.

The main element of the AQM system is a fuzzy controller (Fig. 2), which does not use the mechanism of packets dropping, but calculates the packet losses according to the input queue length and the buffer usage ratio. This allows to improve performance of routers in the IP networks with dynamic environment [2].

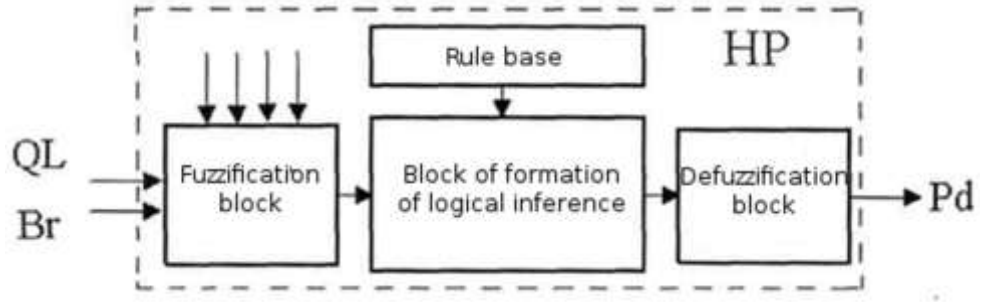


Fig. 2. Structure of fuzzy controller

A typical fuzzy controller includes three main blocks:

1. fuzzification block;
2. block of formation of logical inference;
3. defuzzification block.

The fazzificator is necessary to convert the input data into an appropriate set of linguistic variables that are needed in the decision making block. A number of fuzzy control rules that characterize dynamic behavior of the system is defined in the FLC rule base. Decision making block is used to form inferences from the fuzzy control rules.

The FLC has two inputs, which are designed to obtain information on the queue length (QL) and the buffer usage ratio Br. The packet-dropping probability Pd is transmitted to the FLC output. The controller calculates the probability of packet dropping according to the queue length, current buffer usage ratio and a set of fuzzy linguistic rules. The linguistic rules are generally defined as follows:

1) Rule 1 : ;
2) Rule 2 : ;

…….

3) Rule ^{k} : **IF QL = A_k AND Br = B_R $TH_{EN\ Pd}$ = c_k;**

Symmetric triangular and trapezoidal membership functions are used as the membership functions. The queue length is classified in three linguistic variables: QL = (short, medium, long), where "short" means that the queue length is in normal state, "medium" means that the queue is in state of overload prevention, "long" means that the queue length is overloaded. Figure 3a shows the membership function of the "queue length" variable.

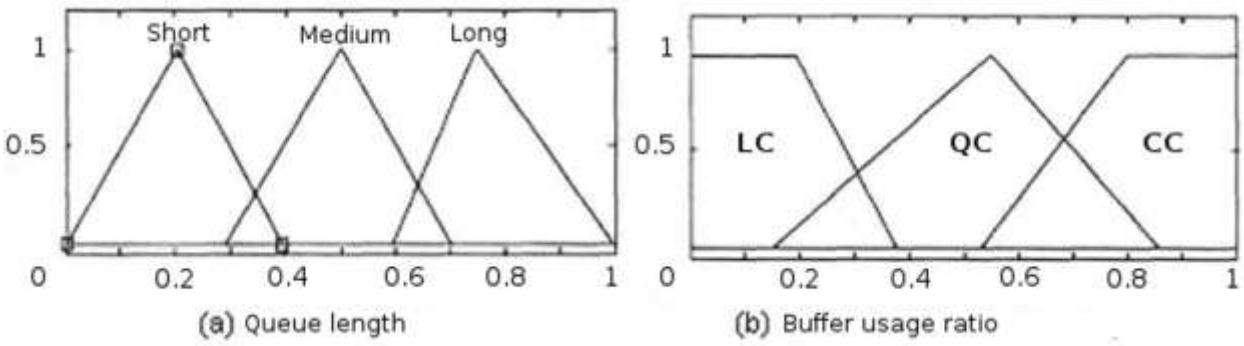


Fig. 3. Membership functions of input variables
"queue" and " buffer usage ratio"

The buffer usage ratio (Figure 3.b) is determined by Br variable, which has three states:

1. "low congested" (LC);
2. "quite congested" (QC);
3. "completely congested" (CC).

The probability function of packet dropping Pd is shown in Fig. 4 for five possible values:

1) Very low (VL);
2) Low (L);
3) Medium (M);
4) High (H);
5) Very high (VH).

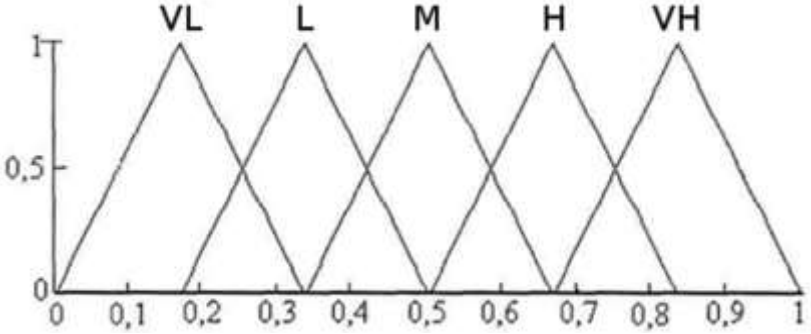


Fig. 4. The membership functions of the output variable "probability of packets dropping"

The fuzzy rules of the controller are written in Table 1

Table 1

Queue length QL	Buffer usage ratio Br		
	Normal state	Prevention of overloads	Overloads
Short	VL	VL	M
Medium	VL	L	H
Long	L	M	VH

Complete links between the input and output variables (response surface) of fuzzy controller are presented in Fig. 5.

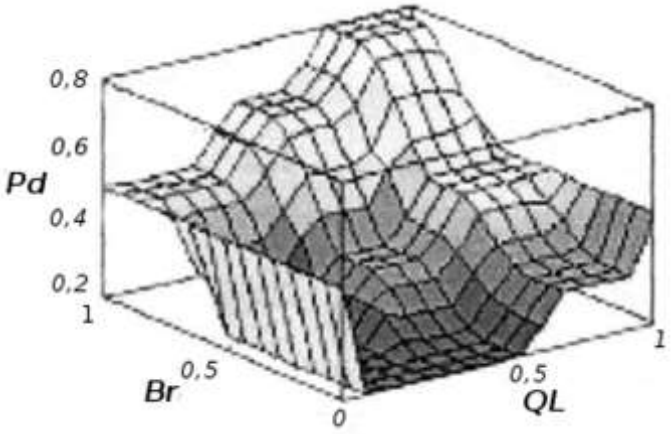


Fig. 5. Response surface of fuzzy controller

Fig. 6 shows the architecture of a fuzzy algorithm **AQM**, which includes classifying model (CM), models of packets dropping (MPD) and model of fuzzy controller (FLC). The CL denotes communication link. The input-to-output ratio is expressed by the set of linguistic rules.

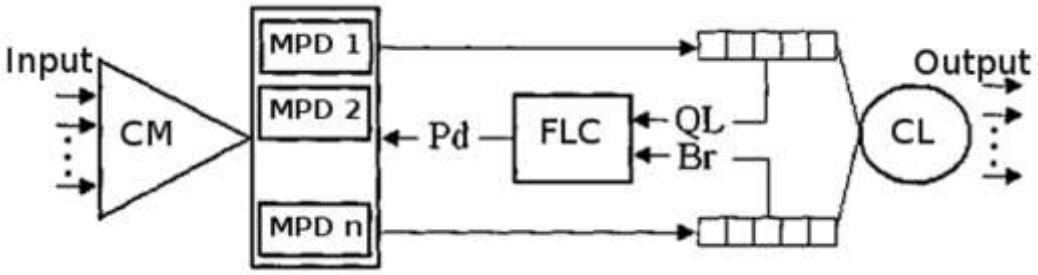


Fig. 6. Architecture fuzzy AQM algorithm

When the queue length is short and the buffer usage ratio is low, the probability of packet dropping is low. When the queue length is large and the buffer usage ratio is high, the probability of packets dropping is high. In this system, the algorithm can correspondingly adapt the probability of packets dropping by means of "learning."

Let us consider modeling the TCP/IP network operation with use of a fuzzy controller and AQM-methods (RED and PI) [1-4]. Topology of the simulated network is shown in Fig. 7.

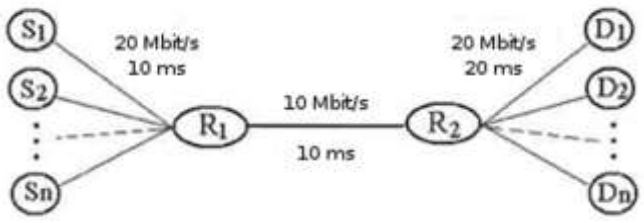


Fig. 7. Topology of modeling

The simulated TC/IP network consists of message sources S_1, S_2, .- S_n, message receiving devices D_1, D_2, .-D_n and two routers R_1 and R_2 between which there is an overloaded line with 10 Mb/s bandwidth of 10 ms delay. The buffer size of the router is 300 packages, and the expected queue length is 100 packages. In addition, support for explicit congestion notification (ECN) is activated in all sources. Duration of simulation was 100 seconds.

In the first stage of modeling, N = 100 (Fig. 8, a) and N = 600 (Fig. 8, b) message sources are included into the system.

When the number of sources is 100, the queue length never exceeds the buffer size of the router. As Fig. 8a shows, the queue length is the highest when the RED-algorithm is used. The queue slightly oscillates when the PI-method is used, while the queue length of the FLC is lower and more stable.

When N = 600, the queue length for RED-method also has a high value and unstable character since RED-algorithm requires some time respond to the increasing number of connections. Queue length for PI-method has a stable character, but the reaction is slow. When using the FLC, the lowest queue length is observed with increasing number of network connections. When dealing with uncertain events, the fuzzy algorithm utilizes advantage of fuzzy logic. Even without an accurate model, it can effectively use resource of the buffer to avoid oscillations caused by the increase of the number of connections and provides a stable queue length.

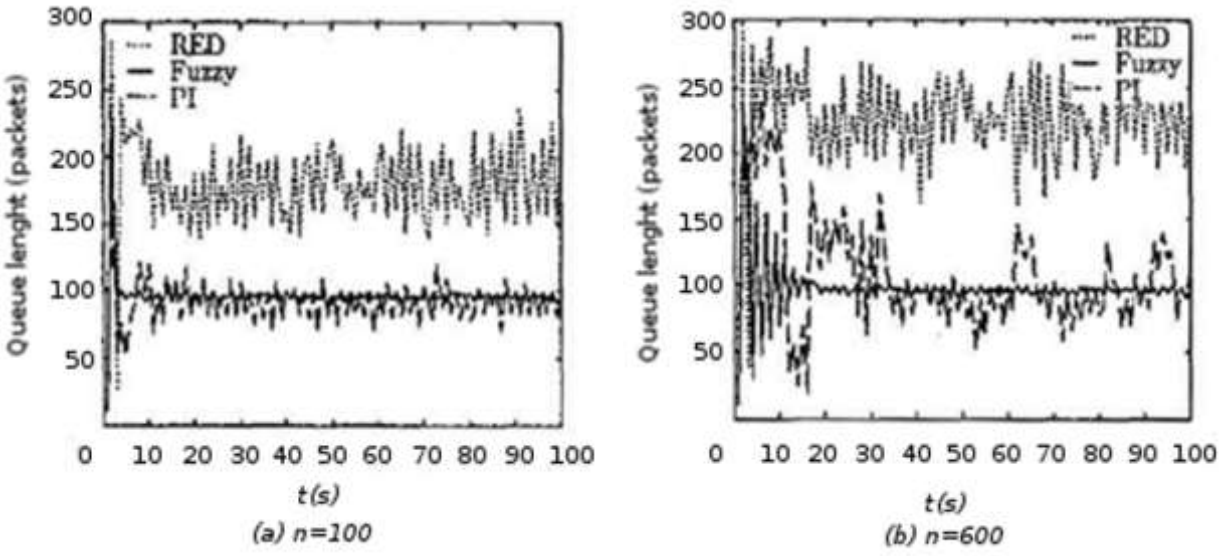


Fig. 8. Queue length for various TCP connections

So, the FLC provides the lowest possible and more stable queue length when the number of connections is changed.

At the second stage of simulation, the bandwidth capacity of the given methods was studied. Results of experiments are shown in Fig. 9.

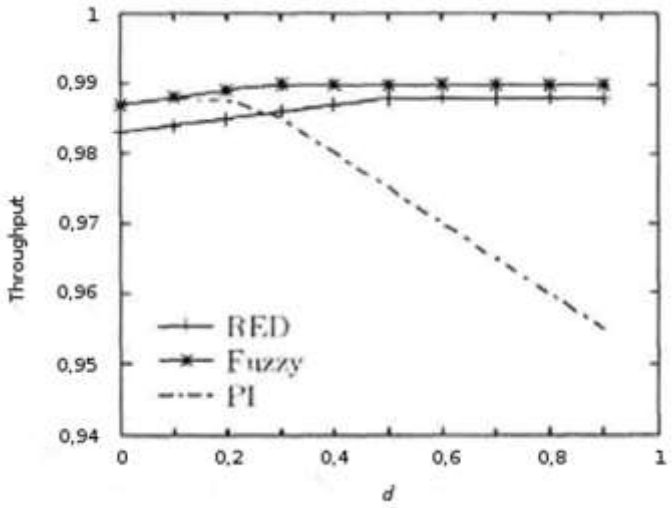


Fig. 9. Bandwidth capacity

The subject of studies at this stage was the impact of UDP-streams. The **UDP** stream density varied from 0.1 to 0.9.

Conclusions. The data presented in Fig. 9 indicate that when using the PI-method, the bandwidth capacity of channel with overload decreases with increase of the UDP-stream density. The RED-method has more stable bandwidth capacity when the UDP-stream density is varied. However, the highest and the most stable results are observed when using the FLC controller.

The main advantage of the FLC-controller is that the length of the queue is stable with variation of the network parameters.

REFERENCES:

1. Gostev V.I, Scurtu S.N. Automatic system of active queue management in networks TCP/IP: Monograph. - Nizhyn: Nezhinskii State University Nikolai Gogol, 2013. - 528 p.

2. Gostev V.I. New design method of fuzzy controllers for automatic control systems. - Palmarium academic publishing, (Germany). - 2013. - 217 p.

3. Gostev V.I. Design of Fuzzy Control System for automatic control systems: Monograph. - Nizhin LLC Publishing house "Aspect-Poligraf" - 2009. - 416 p.

4. Gostev V.I, Scurtu S.N. Fazi of active queue management in networks TCP/IP: Monograph. - Nizhin LLC Publishing house "Aspect-Poligraf" - 2011. - 464 p.

Рецензент: д.т.н., проф. Сбітнєв А.І.

к.т.н., с.н.с. Гостєв В.В., к.т.н., доц. Пампуха І.В.,
к.т.н., доц. Савков П.А., к.т.н. Савкова В.П.

ТИПОВИЙ НЕЧІТКИЙ РЕГУЛЯТОР

У статті проаналізовано показники пропускної здатності, які вказують, що коли використовується PI-метод, то пропускна здатність перевантаженого каналу зменшується зі збільшенням щільності UDP-потоку.

У статті описаний типовий регулятор на основі нечіткої логіки (РНЛ). Представлена функціональна схема КНЛ, а також структура нечіткого контролера. Репрезентована таблиця нечітких правил контролера і його архітектури. Описані експериментальні дані по довжині черги. Проведено огляд контролерів на основі REM-методу активного управління чергою (FREM, STREM, FEM), також зроблені висновки про їх вплив на параметри маршрутизатора.

Доведено, що при використанні PI-методу, пропускна здатність каналу з перевантаженням зменшується зі збільшенням щільності UDP-потоку. RED-метод має більш стабільну пропускну здатність при зміні щільності UDP-потоку. Проте, найвищі і найстабільніші результати спостерігаються при використанні КНЛ. Основною перевагою РНЛ є те, що довжина черги стабільна при зміні параметрів мережі.

к.т.н.., с.н.с. Гостев В.В., к.т.н., доц. Пампуха И.В.,
к.т.н., доц. Савков П.А., к.т.н. Савкова В.П.

ТИПИЧНЫЙ НЕЧЕТКИЙ РЕГУЛЯТОР

В статье был проведен анализ показателей пропускной способности, которые указывают, что когда используется PI-метод, то пропускная способность перегруженного канала уменьшается с увеличением плотности UDP-потока.

В статье описан типичный регулятор на основе нечеткой логики (РНЛ). Представлена функциональная схема РНЛ, а также структура нечеткого контроллера. Репрезентирована таблица нечетких правил контроллера и его архитектуры. Описаны экспериментальные данные по длине очереди. Произведен обзор контроллеров на основе REM-метода активного управления очередью (FREM, STREM, FEM), также сделаны выводы о их влиянии на параметры маршрутизатора.

Доказано, что при использовании PI-метода, пропускная способность канала с перегрузкой уменьшается с увеличением плотности UDP-потока. RED-метод имеет более стабильную пропускную способность при изменении плотности UDP-потока. Тем не менее, самые высокие и самые стабильные результаты наблюдаются при использовании РНЛ. Основным преимуществом КНЛ является то, что длина очереди стабильна при изменении параметров сети.

UDC 004.89

Kubiavka N.B.
(military institute of the national university, Kiev, Ukraine)

THE CONTROL OF INFORMATION SUPPORT OF THE PROCESSES OF INFLUENCE ON THE OPPONENT

In this research, the classification features of the information impact on interaction contractors knowledge with their individual feature of perception and defines the classes of information representations with a given exposure and counterparty interaction. Base of theory of the non-force interaction gives you opportunity to ground and formally represent scientific and methodological tools of management on impact, which should provide improvement of ways for preparing and conducting operations on the information impact on the enemy, the implementation of countermeasures, that will be most informative and clear, simple, efficient and minimally costly. Also issues of information management are examined not from the position of maximum informing of influenced contractors, but from the position of the necessary information influence on them. Using the proposed classification allows you more accurately and efficiently plan special military operations in the field of information impact on the enemy. This is the main purpose of this study.

Keywords: information technology; special information operations; theory of non-force interaction.

Entry. As is known that in the information war, the aggressor is attributes to the victim what he does. The victim in the eyes of the consumer of information becomes the aggressor, and the aggressor – in justify avenger. This is actually information infection. Infection for which there is no "vaccine". Yes, indeed, today in Ukraine there are no effective tools that would be able to confront the information "virus". It is possible for a software virus, an effective anti-virus exist and for information of "viruses" you need to create certain security technologies, that filter information content and fill it protecting information "pills" and it is important to bring them to the "infected body" instead.

Statement of the problem. Our country is only trying to confront the information noise. And ordinary citizens, could hardly distinguish the truth from the information provocations. If we do not take the necessary countermeasures, will "ripe" next fruits of this war: a depressive society, the slave mentality, a complete incomprehension of the processes occurring in the state, apathy, aggression, distrust to everyone and everything. Today, the main impact of information policy of the aggressor is aim at the manipulation of consciousness of ukrainians and destabilization inside the country [1-2].

How to provide effective information influence on the broad strata of the population, an action which could confront the information infection? How to restore the positive attitude of ukranians to their homeland, European country?

Making analysis of the latest researches and publications the author has found that Ukraine is in the third year of a hybrid war and failed to create efficient instruments for the effective confrontation on information expansion of the enemy. In the researched articles the question of assessment processes of informational management, which is need to make the right decisions the significant volume of scientific works is given, but if research problems of making the most favorable decisions [3-6], no attention is paid to issues of information management. But if describe methods of management of information during the informational influence [7-12], almost no attention is paid to the influence of this information on decision makers, and the decisions themselves. Examining the ways and tools of opposition to information infection, we stumble on a paradox: on the one hand, we need different ways to influence on different audiences of our society, and on the other, building trust between polarized groups to build overall confidence. Allow this and base on the Theory of non-force interaction (the Theory) and developed on its base tools [13-18] the author of this article proposed and laid the Foundation for the creation of information

technology support and maintenance of special information operations, that provide an unprecedented advantage in the course of realization of information effects and, above all, protection.

As the result of the analysis of the sources allocated previously unsolved part of General problem which the article deals.

Presentation of the basic material.

In our time we are suffering not so much because of the lack of information as from excess, unnecessary information, unrelated to the outcome of crisis situations. Find the ability to separate the useless from the important, and you feel that you are control the situation [19].

Management of information support of the processes of impact on the opponent.

Management information support should be aimed at ensuring the constant availability of relevant information, which has such features as targeting, timeliness, reliability, completeness. Relevant information important for making management decisions because it contains data that should be used for calculations in preparing information that will be provided to the counterparties of interaction. Irrelevant information (noise information) is irrelevant, redundant data, which do not have useful actions on the object of influence. The usage of irrelevant information may lead to lowering of the level of influence or its impossibility. One of the most challenging tasks of creating such a management system is to convert tacit (implicit) knowledge to explicit counterparties (explcit). What is achieved only using relevant information, with mandatory determination of the ultimate goals of the impact. With the aim of creating information technology (fig. 1) that will find the necessary (relevant) information that would respond the criteria of the most influential actions on the counterparty of interaction and would provide this information, taking into account his personal preferences and individual moral and psychological qualities, i.e. the creation of information technology management awareness, you first need to determine what information and what is the impact on the company.

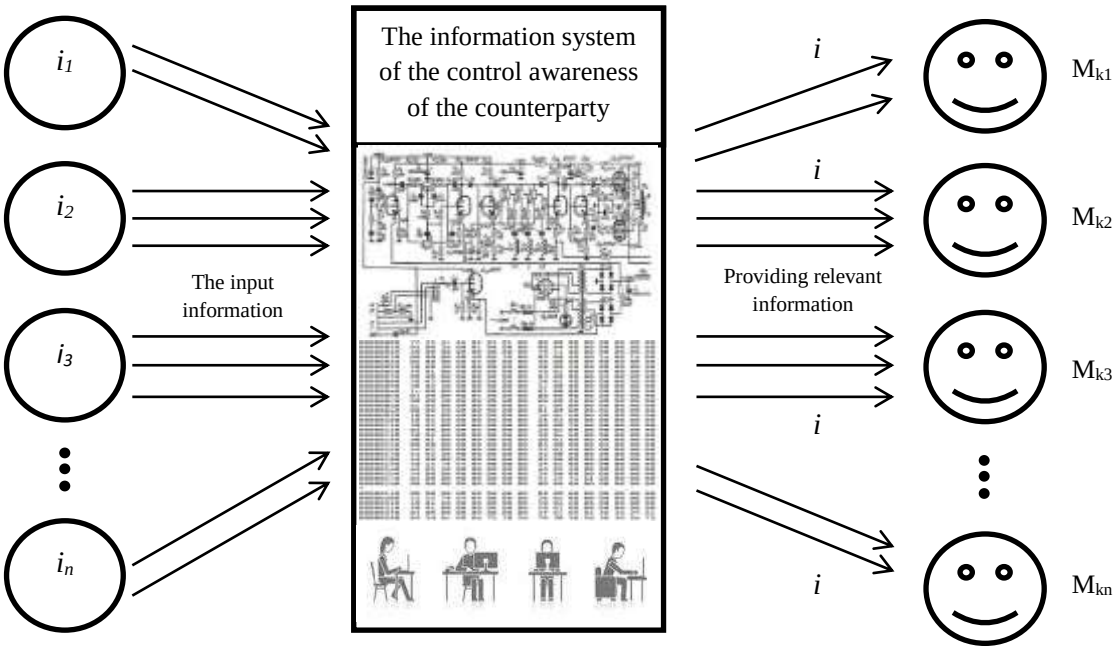


Fig. 1. Information technology impact on the counterparty of interaction

With this aim, the author elucidate the priority issues of this problem, namely:

- necessity to classify the features of the impact of information on knowledge of counterparties of interaction with the personality of their perception;

- necessity to represent the classes of information representations with a given influence on counterparty interaction.

Classification of the impact of information on knowledge of the counterparty of interaction by peculiarities of their perception.

For effective management on knowledge of counterparty of interaction it is necessary to determine what information and how it will effect on his decision, to select the most relevant information and to consider the best ways of presenting this information. To solve this problem, we should classify objects of influence by the specific of informational perception and known relation to it. So the information provided to the Muslim that Christianity is the only correct religion will cause storm poured out emotions, as a maximum, and another confirmation of the correctness of conducting thousands of years of wars between the "true" believers and "infidels." On this basis, selected characteristics, which will provide classification for search and provision of information are:

1. Race - Negron, Caucasoid and Mongoloid. Some researchers also identify Australoid;

2. The national identity. So the Russian marketers have found that the same promotional video has a positive effect on the Russians, but the Ukrainians (as an example) causes a different attitude to the products that are advertised;

3. Sex. There is virtually no such thing about which men and women agreed to the opinions. We remain a mystery for one another and essentially live in two isolated, only occasionally crossing each other, realities of respectively, the impact on women and men must differ;

4. Age identity [20, p. 39]. Now adopted the following age periods: infancy (birth to 1 year); preschool education (1-3 years); preschool education (3-6 years) primary school age (6-10 years); adolescence (10-15 years); adolescence: the first period (senior school age 15-17 years), second period (17-21 years); Mature age: first period (21-35 years), second period (35-60 years); old age (60-75 years); old age (75-90 years); the oldest old (90 and above) and for each age period is the most acceptable information should have its own specific "taste" and "color". For the further work we define another option, which in the opinion of the author is more approximated to reality:

Children;
The youth that studies;
The youth that works;
Entrepreneurs;
Workers;
Military serves;
Retired people.

5. Membership by the perception of information [21].

All people perceive and memorize information differently. So, those who receive information through the auditory channel are called **auditory learners**. They are great listeners, remember details of the story and perceive intonation, tone of speech, have sharp hearing and an excellent memory.

Visual is the person who receives most of their information through vision. They are 30% of the population.

Kinesthetic - one who perceives the information through other senses (touch, smell, etc). They are 40% of the population.

There are also people who have the perception of information occurs by means of logical reasoning, with numbers, characters, logical proofs, they are called **discretes**.

It is clear that any person in his life uses different channels of perception. It can be visual, but this does not mean that the other senses are almost not working. If more channels are open to receive new information, the more efficient the process of perception.

6. Occupation, work, hobbies or lifestyle.

The above classification will help us to understand the special approach to every human being, as a person, and later to transfer this knowledge to family, group, country, possibly the world.

Classes of information representations with determine exposure on counterparty interactions.

The most important properties of information as we all know are: objectivity and subjectivity, completeness, reliability, adequacy, availability, relevance, accuracy and value.

It has been determined that the main types of information representations are: graphics, sound, text, numeric and video information.

And the most common methods of presenting information are: language (oral communication), writing, press, books, radio, film, television and computer.

Using proposed properties of information, the specificity of human nature to perceive the information and on the base of effected research propose classification of the information content of the representations with a given exposure to the interaction counterparty according to the age and business facilities according to the criterion of the maximum response (change in worldview), which is given below:

1. The information content is acceptable for children:
1.1. What will give a praise;
1.2. What is the punishment;
1.3. About entertainment events and festivals;
1.4. About getting a high marks of the success;
1.5. About favorite dishes and preferences;
1.6. About the injustice against them;
1.7. Regarding the failure of the promises;
1.8. About idols and Pets;
1.9. About the need for homework and school responsibilities;
1.10. About the threat to the life and health of a loved one.
2. The information content acceptable to young people, what works:
2.1. What will give a praise or a positive rating of work;
2.2. What is the punishment or negative evaluation of labor;
2.3. About the health of a loved one;
2.4. On the level of wages;
2.5. The level of payment for utilities;
2.6. About the fluctuations of the exchange rate and prices of products and goods;
2.7. About the situation in the area of holding of Antiterrorist operation on the Eastern part of Ukraine;
2.8. About sanctions of the international community to the aggressor state;
2.9. On the activities of the state leadership and the high fighting capacity of the army to ensure the protection of the country;
2.10. About the "atrocities" against the prisoners from terrorist groups in the East of the country;
2.11. About the bad facts in the life of their army (their distortion, naked lies);
2.12. About the threat to the life and health of a loved one.
3. The information content is acceptable for young students:
3.1. What will give a praise or positive evaluation of study;
3.2. What is the punishment or negative assessment study;
3.3. About changes in the educational program of students;
3.4. Status of scholarships and fees for the dormitory;
3.5. About public events and institutions;
3.6. On national consciousness and the certainty;

3.7. About the situation in the area of holding of Antiterrorist operation on the Eastern part of Ukraine;

3.8. About sanctions of the international community to the aggressor state;

3.9. On the activities of the state leadership and the high fighting capacity of the army to ensure the protection of the country;

3.10. About the bad facts in the life of their army (their distortion, naked lies);

3.11. On the possibility of self-realization after study;

3.12. About the threat to the life and health of a loved one.

4. The information content is acceptable for entrepreneurs:

4.1. What will give a positive assessment of business activity;

4.2. What will give a negative evaluation of entrepreneurial activities;

4.3. About the health of children and loved ones;

4.4. About the state of affairs and the income growth of the enterprise;

4.5. The level of payment for utilities;

4.6. About fluctuations in the foreign exchange market;

4.7. About the situation in the area of holding of Antiterrorist operation on the Eastern part of Ukraine;

4.8. About sanctions of the international community to the aggressor state;

4.9. On the activities of the state leadership and the high fighting capacity of the army to ensure the protection of the country;

4.10. About the "atrocities" against the prisoners from terrorist groups in the East of the country;

4.11. About the bad facts in the life of their army (their distortion, naked lies);

4.12. About the threat to the life and health of a loved one.

5. The information content acceptable to workers:

5.1. What will give a praise or a positive rating of work;

5.2. What is the punishment or negative evaluation of labour;

5.3. About the health of children and loved ones;

5.4. On wages;

5.5. The level of payment for utilities;

5.6. About the fluctuations of the exchange rate and prices of products and goods;

5.7. About the situation in the area of holding of Antiterrorist operation on the Eastern part of Ukraine;

5.8. About sanctions of the international community to the aggressor state;

5.9. On the activities of the state leadership and the high fighting capacity of the army to ensure the protection of the country;

5.10. About the "atrocities" against the prisoners from terrorist groups in the East of the country;

5.11. About the bad facts in the life of their army (their distortion, naked lies);

5.12. About the threat to the life and health of a loved one.

6. The information content is acceptable for military servers:

6.1. What will give a praise or positive evaluation of serve;

6.2. What is the punishment, or negative performance appraisal;

6.3. About the health of children and loved ones;

6.4. Of allowance;

6.5. The level of payment for utilities;

6.6. About the fluctuations of the exchange rate and prices of products and goods;

6.7. About the situation in the area of holding of Antiterrorist operation on the Eastern part of Ukraine;

6.8. About sanctions of the international community to the aggressor state;

6.9. On the activities of the state leadership and the high fighting capacity of the army to protect the country and the level of social security of servicemen;

6.10. About the "atrocities" against the prisoners from terrorist groups in the East of the country;

6.11. About the bad facts in the life of their army (their distortion, naked lies);

6.12. About the threat to the life and health of a loved one.

7. The information content acceptable to the pensioners:

7.1. What will give a praise;

7.2. That carries a sentence;

7.3. On the health status of children, grandchildren and loved ones;

7.4. On the state pension and social security;

7.5. The level of payment for utilities;

7.6. About the fluctuations of the exchange rate and prices of products and goods;

7.7. About the situation in the area of holding of Antiterrorist operation on the Eastern part of Ukraine;

7.8. About sanctions of the international community to the aggressor state;

7.9. On the activities of the state leadership and the high fighting capacity of the army to ensure the protection of the country;

7.10. About the "atrocities" against the prisoners from terrorist groups in the East of the country;

7.11. About the bad facts in the life of their army (their distortion, naked lies);

7.12. About the threat to the life and health of a loved one.

Information sense, that given, should be applied selectively, depending on the functional role and in accordance with the functional tasks of the components of exposure. But most importantly, it needs to be present in some information models, which allow to formally work them in the system of management of knowledge (relation to reality), which will allow you to make decisions that will lead to optimal and kvazioptimal actions of the counterparty of interaction. Which will able to optimize the information environment in the processes of management of information impacts and to determine the functional role of content representations in their management.

This issue will focus in the following works of the author.

Conclusions. In the article was given classification of the influence of information on the knowledge of the counterparties of interaction with their individual feature of perception, as well as defined classes of information representations with a given exposure and counterparty interaction.

The basic idea of the classification is to represent out to provide scientific and methodological tools of management on impact, which should provide improvement of ways for preparing and conducting operations on the information impact on the enemy, the implementation of countermeasures, that will be most informative and clear, simple, efficient and minimally costly. Also issues of information management are examined not from the position of maximum informing of influenced contractors, but from the position of the necessary information influence on them. Usage of proposed classification allows you more accurately and efficiently plan special military operations in the field of information impact on the enemy. What will be the background of victories in the information war with the enemies of our country.

Reviewer: doctor of technical Sciences, Professor Kravchenko O., Professor, Department of technology management faculty of information technology, national University of Ukraine named after Taras Shevchenko, Kiev.

LITERATURE:

1. Larychev O. (2002). Teoryja y metody prynjatyja reshenyj. [2-e yzd., pererab. y dop], *Kyiv,* Logos, 392 *p*. (in Ukrainian).

2. http://www.milnavigator.com/uk/realiï-informacijnoï-vijni-v-ukraïni/

3. http://gazeta.dt.ua/technologies/lyalkovodi-svidomosti-_.html

4. Voyna v kyberprostranstve: uroky y vuvodi dlya Rossyi (2013).[Nezavysymoe voennoe obozrenye], no. 46(787). pp. 1–4. (in Russia).
5. Levchenko O. (2014). Klasyfikatsiya informatsiynoyi zbroyi za zasobamy vedennya informatsiynoyi borot'by. [Suchasni informacijni tehnologii' u sferi bezpeky ta oborony], no. 2, pp. 142-146. (in Ukrainian).
6. Chernoruckyj Y. (2005). Metody prynjatyja reshenyj. [SPb], BHV-Peterburg, 416 p. (in Russia).
7. Bushuev S. (2010). Kreatyvnye tehnologyy upravlenyja proektamy y programmamy [monografyja]. «Sammыt-Knyga», 768 p. (in Ukrainian).
8. Nejtan Jau. (2013). Yskusstvo vyzualyzacyy v byznese. Kak predstavyt' slozhnuju ynformacyju prostыmy obrazamy. Mann, Yvanov y Ferber, Moskva, 352 p. (in Russia).
9. Ros' A. (2011). Informatsiyna bezpeka derzhavy u voyenniy sferi: navchal'nyy posibnyk / Ros' A.O., Bychenok M.M., Vishchun V.V., Dzyuba T.M., Zamaruyeva I.V., Katin P.Yu., Shemayev V.M. [NUOU], 324 p. (in Ukrainian).
10. Horbulin V. (2009). Problemy zakhystu informatsiynoho prostoru Ukrayiny: monohrafiya [V. Horbulin, M. Bychenok. Intertekhnolohiya], 136 p. (in Ukrainian).
11. Rusnak I. (2000). Rozvytok form i sposobiv vedennya informatsiynoyi borot'by na suchasnomu etapi [I.Rusnak, V.Telelym // Nauka i oborona]. no 2, pp. 18–23. (in Ukrainian).
12. Solovtsov N. (1999). Klassyfykatsyya y sposobu prymenenyya "ynformatsyonnoho oruzhyya" [N. Solovtsov, B.Y. Hlazov, D.A. Lovtsov, Stratehycheskaya stabyl'nost']. no 4, p. 17–22. (in Russia).
13. Teslja Ju., Kubjavka L., Mykolenko A., Kubjavka M. (2014). Vykorystannja tehnologij informacijnogo vplyvu pid chas pidgotovky ta vedennja bojovyh dij. [Suchasni informacijni tehnologii' u sferi bezpeky ta oborony], no. 2 (20), pp. 147-152. (in Ukrainian).
14. Kubjavka M., Kubjavka L., Teslja Ju. (2015). Mozhlyvosti zastosuvannja teorii' nesylovogo vplyvu v vijs'kovij kontrrozvidci. [Scientific Journal «ScienceRise], no. 2/1(7), pp. 18-22. (in Ukrainian).
15. Kubjavka M., Kubjavka L., Teslja Ju. (2016). Osnovy informacijnyh tehnologij suprovodzhennja procesiv vplyvu na kontragentiv vzajemodii' [Praci Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu Shevchenka], no. 52, pp. 123-128. (in Ukrainian)
16. Teslja Ju. (2010). Vvedenye v ynformatyku Pryrody. [Juryj Teslja], Kyiv, Maklaut, 256 p. (in Ukrainian).
17. Teslja Ju. (2014). The Non-Force Interaction Theory for Reflex System Creation with Application to TV Voice Control. [VI Mizhnarodna konferencija: «International Conference on Agents and Artificial Intelligence (ICAART 2014) »], 352 p. (in Francij).
18. Teslja Ju. (2005). Nesylovoe vzaymodejstvye. [Juryj Teslja], Kyiv, Kondor, 196 p. (in Ukrainian).
19. Dzheff O`Lyry. (2005). Pryntsypy tsenturiona: uroky boyu dlya lideriv na liniyi frontu, [Fenyks], 296 p. (in Ukrainian).
20. Krutetskyy V. (1972). Osnovu pedahohycheskoy psykholohy. [Prosveshchenye]. 255 p. (in Russia).
21. http://dnevnik.bigmir.net/groups/article/20340

Без рецензії.

Кубявка М.Б.

УПРАВЛІННЯ ІНФОРМАЦІЙНИМ СУПРОВОДЖЕННЯМ ПРОЦЕСІВ ВПЛИВУ НА ПРОТИВНИКА

У даному дослідженні дається класифікація особливості впливу інформації на знання контрагентів взаємодії за їх індивідуальною особливістю сприйняття, а також визначаються класи інформаційних представлень з заданим впливом на контрагента взаємодії. Взята за основу теорія несилової взаємодії дає можливість обґрунтувати та формально представити науково-методологічні інструменти управління впливами, які повинні забезпечити значне покращення шляхів підготовки і проведення операцій з інформаційного впливу на противника, здійснення контрзаходів та будуть максимально інформативно зрозумілі, прості, результативні і мінімально затрати. Питання управління інформацією розглядаються не з позицій максимального інформування контрагентів впливу, а з позицій необхідної інформаційної дії на них. Використання запропонованої класифікації дає можливість більш точно і результативно

планувати спеціальні військові операції в сфері інформаційного впливу на противника. Це і є основною метою даного дослідження.

Ключові слова: інформаційні технології; спеціальні інформаційні операції; теорія несилової взаємодії

Кубявка М.Б.

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМ СОПРОВОЖДЕНИЕМ ПРОЦЕССОВ ВОЗДЕЙСТВИЯ НА ПРОТИВНИКА

В данном исследовании дается классификация особенности влияния информации на знание контрагентов взаимодействия по их индивидуальной особенностью восприятия, а также определяются классы информационных представлений с заданным воздействием на контрагента взаимодействия. Взятая за основу теория несилового взаимодействия дает возможность обосновать и формально представить научно-методологические инструменты управления воздействиями, которые должны обеспечить значительное улучшение путей подготовки и проведения операций по информационному воздействию на противника, осуществления контрмер и будут максимально информативно понятные, простые, результативные и минимально затрате. Вопросы управления информацией рассматриваются не с позиций максимального информирования контрагентов влияния, а с позиций необходимого информационного воздействия на них. Использование предложенной классификации дает возможность более точно и результативно планировать специальные военные операции в сфере информационного воздействия на противника. Это и является основной целью данного исследования.

Ключевые слова: информационные технологии; специальные информационные операции; Теория несилового взаимодействия.

УДК 356.13
д.пед.н., д.э.н., проф. **Апатова Н.В.** (Тавр.НУ)

СТРУКТУРА УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ ПРИ КОМПЬЮТЕРНОМ ОБУЧЕНИИ

В статье рассматривается структура учебной деятельности, ее основные компоненты и этапы формирования при традиционном и компьютерном обучении, обосновывается необходимость учета выделенных особенностей при разработке компьютерных программ учебного назначения для самостоятельного, в том числе, дистанционного обучения.

Усвоение учебной информации при компьютерном обучении связано с эмпирической, эвристической, репродуктивной по преобразованию модели и получению нового знания и практической видами деятельности. Данные и другие виды учебной деятельности подробно характеризуются.

Построены математические модели процесса обучения, позволяющие формализовать оценку формируемых компетенций. Компетенции раскрыты через знания и умения, в модели оцениваются факторы знакомства с учебным материалом, запоминания и понимания, на основе экспертных оценок выставляется количественная оценка.

Ключевые слова: учебная деятельность, виды учебной деятельности, компьютерное обучение, математическая модель процесса обучения, компетенции.

Постановка проблемы. Развитие дистанционной формы обучения и перенос значительной нагрузки на самостоятельную работу обучающихся всех уровней образования поставил проблему качественного усвоения учебного материала в условиях большого объема информации и сжатых временных сроков. Попытки унифицировать обучающие базовые программы привели к тому, что преподаватели копируют тексты традиционных учебников и снабжают их некоторым количеством вопросов и заданий, не учитывая компьютерную форму представления и сложности чтения с мониторов, которые, в свою очередь, часто имеют малый размер (мобильные телефоны, планшеты).

Для решения данной проблемы необходимо обратиться к истокам первых программ компьютерного обучения, в том числе, к разработанной в Кибернетическом Центре им. В.М. Глушкова системе СПОК (Система Программирования Обучающих курсов), которая, в силу технической ограниченности, была использовала, в основном, алфавитно-цифровые мониторы, но позволяла достигать, за счет вывода на один экран небольших фрагментов учебного материала, хорошего педагогического эффекта.

Анализ структуры учебной деятельности для каждой учебной дисциплины дает возможность детально структурировать учебный материал, отобрать существенное для его усвоения, проводить постоянный контроль знаний и умений, лежащих в основе формируемых компетенций. Учет накопленного психолого-педагогического опыта в компьютерном обучении в сочетании с новыми используемыми SMART-устройствами позволит перевести самостоятельное обучение, в том числе, дистанционное с использованием Интернет, на новый качественный уровень. Формализация процесса обучения путем выделения значимых его факторов и установления зависимостей между ними, позволит более объективно выставлять оценки обучаемому по результатам контроля его компетенций.

Анализ последних достижений и публикаций. Самой структуре учебной деятельности в последнее время уделяется недостаточное внимание и трудно выделить научные работы, посвященные именно данному вопросу. Однако имеется ряд статей, в которых рассматривается построение индивидуального маршрута обучения [1], движение информационных потоков в процессе обучения [2], моделирование информационных структур в организации учебной деятельности [3], проектирование учебной деятельности в

контексте непрерывного образования [4] и формирование профессионального интеллекта в структуре учебной деятельности студентов [5].

Юрловской И.А. и Гучмазовой К.П. раскрыта типология индивидуальных образовательных маршрутов студентов как механизма индивидуализации профессионального становления будущих учителей. Описан алгоритм прохождения индивидуального маршрута. Предложенный алгоритм может быть применен как к учебному процессу, так и к внеурочной деятельности обучающегося, а каждый «шаг» конкретизируется специальными техниками и приемами в зависимости от содержания деятельности и индивидуальных особенностей, уровня сформированности его субъектности в конкретном виде деятельности [1]. Несмотря на безусловный интерес полученных результатов, они носят теоретический характер и не содержат механизм их применения к конкретным учебным дисциплинам.

Тындыкарь Л.Н. формализует информационные потоки между двумя автоматизированными системами вуза, рассматривает средства их оптимизации и увязки с учебным процессом [2], но оставляет без внимания обучаемого, для которого эти потоки предназначены.

Неворотов Б.К. и Моисеев М.Б. рассматривают моделирование информационных структур в организации учебной деятельности [3], определяя условия, при которых формальная модель становится средством управления познавательной деятельности. Моделью представления служит граф, содержащий отношения, формально связывающие элементы учебного материала. Фактически авторы реализуют идею формирования учебного действия, рассматривая его как элемент рефлексии. Контроль предполагает выполнение комплексных заданий на усвоение смысла учебного материала. Однако сами авторы в своих выводах подчеркивают. Что предложенная модель служит лишь инструментом для выявления элементов познания и освоения учебного материала.

Рыбакина Н.А. выделяет два вида учебной деятельности, свойственной непрерывному образованию: классическую и развивающую, а также обосновывает возможность и необходимость использования теории контекстного образования в качестве концептуальной основы проектирования учебной деятельности нового типа – контекстного, раскрывает особенности структуры и процесса данного типа учебной деятельности [4]. Несмотря на декларируемый новый тип учебной деятельности, описание его этапов с использованием более современных терминов в принципе не отличается от традиционных этапов учебной деятельности и структуры их полностью изоморфны.

Слепко Ю.Н. исследует формирование профессионального интеллекта в структуре учебной деятельности студентов [5], особый интерес представляют результаты анализа взаимосвязи между формированием учебной деятельности и профессиональным интеллектом. Ставя задачей детальный анализ процесса формирования профессионального интеллекта, автор применяет методы корреляционного анализа, множественного регрессионного анализа, анализа корреляционного отношения. Используемые в работе методы позволили автору уточнить существующие представления не только о связи успешности учебной деятельности и профессионального интеллекта, но и о влиянии последнего на успешность обучения студентов.

Несмотря на широкий охват указанными авторами поставленной проблемы, остаются неизученными вопросы, связанные с формированием учебных действий при компьютерном обучении, широко используемом в настоящее время при самостоятельной работе обучаемых.

Цель данной работы – выделить те компоненты учебной деятельности, которые наиболее эффективно использовать и развивать при компьютерном обучении и которые можно использовать как факторы для построения формальных моделей, позволяющих адекватно оценивать формируемые компетенции.

Изложение основного материала. В отечественной психологии учение рассматривается как процесс, главными компонентами которого являются знания и действия,

переходящие в устойчивые стереотипы, называемые умениями. Профессиональные компетенции, формируемые в высших учебных заведениях, состоят из знаний и умений. Третий компонент – навыки, являются составной частью умений и относятся к более простым профессиональным действиям, они, в отличие от умений в целом, не имеют творческой основы.

Понимание процесса учения как формирование знаний и умений, восходит еще к Я.А. Коменскому, который определил знания частично как чувственные представления, а главным образом - как понятия и их системы, описывающие объекты и явления в их общих внешних свойствах, связях, и объясняющие их сущность. И.Ф. Гербарт учение считал первой ступенью, следом за которым шло развитие, совершенствование общих познавательных процессов. Такой же точки зрения придерживался Л.С.Выготский, сформулировавший общие принципы культурно-исторической концепции, на которых строились теории учения А.Н. Леонтьева, П.Я. Гальперина, Д.Б. Эльконина и В.В. Давыдова. Под учением, как и многие основатели психологии и педагогики, Л.С. Выготский понимал приобретение знаний, умений и навыков, а под развитием - приобретение общих качеств и способностей. Определение деятельности наиболее четко дано И.И. Ильясовым: "Деятельность - обозначение процессов взаимодействия человека и общества с объектами действительности" [6, с. 140]. А.Н. Леонтьев подчёркивал, что, для того, чтобы овладеть знаниями и умениями, необходимо осуществить деятельность, адекватную той, которая воплощена в этих знаниях и умениях. Процесс учения рассматривался как процесс управления деятельностью, компонентами которого являются объекты воздействия, акты его преобразования, а также продукт, условия и средства преобразования. Различается внешняя практическая деятельность, в рамках которой происходит усвоение, и внутренняя, умственная деятельность. При этом считалось, что структуры внутренней и внешней деятельности совпадают [7]. П.Я. Гальперин создал теорию поэтапного формирования умственных действий. Предметом усвоения в процессе обучения при этом считается действие. Действие структурировано и включает предмет преобразования, продукт (цель), средства, а также сам процесс преобразования. Знания включаются во все компоненты действия. Процесс преобразования заключается в создании (или актуализации) имеющейся ориентировочной основы действия (ООД), осуществление самого преобразования, контроля и коррекции. Ориентировочная основа действия явилась психологическим механизмом регуляции преобразований. П.Я. Гальпериным и Н.Ф. Талызиной введены три критерия ООД: полнота (полная-неполная), обобщенность (обобщенная-конкретная), способ ее получения (самостоятельно или от учителя). В случае неполной, конкретной, полученной самостоятельно ООД, уяснение и дальнейшая обработка материала обучаемыми проходит с ошибками, с недостаточным выделением существенных признаков и пониманием содержания; в случае полной, конкретной, данной «в готовом виде» ООД учение проходит более уверенно, с пониманием, с четким выделением существенных и несущественных признаков понятий; в случае полной, обобщенной, также данной в «готовом виде» ООД происходит наиболее эффективное обучение.

Усвоение знаний понимается как процесс усвоения действий по применению этих знаний. Содержанием знаний являются понятия, служащие отличительными признаками объектов и явлений. Действия поэтапно подводятся под понятия. При этом создается мотивация к усвоению понятия, уточняется состав признаков понятий, порядок и уровень использования понятия в изучаемом объекте или явлении. Такой подход продуктивен применительно к современным информационным технологиям, особенно на стадии разработки содержания компьютерного обучения. Он позволяет не только создать семантическую сеть, отражающую предмет или тему, связывающую основные понятия и их свойства существенными отношениями, но также создать изоморфный граф, узлами которого являются формируемые соответствующие каждому понятию действия, а рёбрами - различной степени детализированные пути формирования ООД. Н.Ф. Талызина включает в

средства поэтапного усвоения приёмы познавательной деятельности - мышления, памяти, внимания, - важнейшими из которых являются логические приёмы мышления: выделение свойств объектов, определение понятий, распознавание, выведение следствий, умозаключений, классификация и доказательство [8]. В.В. Давыдов выделяет две формы теоретического мышления и рассматривает их как две процедуры: анализ и восхождение к конкретному [9]. Учение при этом трактуется как "квазиисследование", состоящее из выделения всеобщих отношений, ведущих принципов, ключевых идей данной области знаний, моделирования этих отношений, овладение способами перехода от всеобщих отношений к их конкретизации и обратно, от модели к объекту и обратно. На замещение объектов знаками указывает и Г.П. Щедровицкий, понимая под знаниями способы перехода от объектов к знакам, движение в знаковых системах и обратный переход к объектам [10].

Развёрнутая структура знаний и действий подробно описана И.И.Ильясовым в [6]. При разработке предметной информационной технологии каждый элемент структуры конкретизируется, связывается с отработкой элементарного навыка, заменяется операцией. Детализация структуры и состава знания и действия позволяет учесть все приведённые компоненты в содержании учебной программы, повышая тем самым эффективность компьютерного обучения.

Основным в процессе обучения перечисленные теоретики считают усвоение знаний. А.Н. Леонтьев считает, что для усвоения учащийся должен осуществить восприятие объекта (способа действия с ним), понять свойства объектов в их сходстве и различиях (осуществить деятельность по выявлению свойств и способов действий с ними), использовать освоенные действия для поиска, проверки и объяснения полученных знаний.

Процесс усвоения знаний, согласно положениям Н.Ф. Талызиной и П.Я. Гальперина, осуществляется в шесть этапов: 1) мотивация 2) уяснение схемы ориентировочной основы действия; 3) выполнение действия в материализованной форме (т.е. действия с объектами, представленными в виде знаков, схем, моделей); 4) выполнение действия в громкой речи; 5) выполнение действия в речи про себя; 6) выполнение действия в умственной форме (оперируя образами и понятиями, без участия внешних знаков и форм). И.И. Ильясов выделяет три вида действий, связанных с уяснением содержания: восприятие и декодирование исходного содержания, переработку и уяснение содержания, фиксацию переработанного и уясненного содержания, т.е. выделят практически те же этапы, которые, несколько в другой модели, описывает когнитивная психология. Однако, детализация этих этапов в когнитивной психологии отсутствует, а И.И. Ильясов обработку и усвоение знаний рассматривает как две большие группы операций: 1) при смысловой обработке содержания осуществляются категоризация, соотнесение, обобщение, группировка и т.д.; 2) при фиксации содержания (включении во внутреннюю когнитивную структуру обучаемого) происходит переход к знаковым системам естественных и искусственных языков, форма которых не связана с содержанием, а также к изобразительным знакам, подобным содержанию. Первая группа операций соответствует обработке информации в кратковременной памяти обучаемого, вторая - переносу и хранению в долговременной памяти, т.е. запоминанию и отработке.

Суммируя наиболее известные, кратко описанные выше теории, можно выделить следующие виды (этапы) деятельности, связанные с усвоением учебной информации при компьютерном обучении.

1. Эмпирическая деятельность как этап восприятия:
- отражение фона, заполняющего поле экрана дисплея;
- концентрация внимания и отражение отдельных единичных объектов на фоне;
- отражение выделенных единичных объектов и конкретной ситуации;
- отражение конкретной ситуации в комплексе.

2. Эвристическая деятельность по распознаванию ситуации:

- абстрагирование от конкретности, в которой представлена ситуация, создание знаковой модели;

- поиск алгоритма преобразования модели для решения поставленной задачи, привлечение имеющихся знаний.

3. Репродуктивная деятельность по преобразованию модели и получению нового знания.

- преобразование модели по избранному алгоритму;

- интерпретация результатов преобразования, оценка адекватности полученной модели имеющимся у обучаемого знаниям;

- оценка адекватности решения поставленной задаче.

4. Практическая деятельность, связанная с отработкой навыка:

- закрепление умения в подобных ситуациях;

- формирование умения в необычных ситуациях;

- формирование ассоциативных умений в необычных ситуациях.

Последний вид (этап) практической деятельности относится к воспитанию стратега, который для решения данной конкретной задачи будет использовать весь арсенал имеющихся знаний и умений, искать похожие ситуации, т.е. ассоциации.

Все виды деятельности, независимо от конкретного содержания, включают следующие компоненты: потребности и мотивы, задачи, действия, операции. Особенности компьютера как инструмента человеческой деятельности, заключаются в обеспечении доступа к большим объемам информации и ее переработке, усилении познавательно-исследовательских возможностей человека, организации обмена информацией по содержанию выполняемой деятельности и создании новой человеко-машинной коммуникативной системы. Психолого-педагогические проблемы компьютеризации обучения были в свое время рассмотрены украинским психологом Е.И. Машбицом, но в его исследованиях больше внимания уделялось этапам когнитивной деятельности, связанной с целеполаганием в обучении [11].

Нами было показано, что компонентами учебной деятельности при компьютерном обучении являются: 1) учебная задача; 2) система учебных действий; 3) моделирование содержания объектов усвоения; 4) преобразование модели; 5) действия самооценки и контроля [12].

Учебную задачу ставит преподаватель. Поскольку компьютер не способен на эмоции, при постановке задачи, разъяснении методов ее решения и контроля путей решения учащегося, необходимо особое внимание уделять мотивации, имея, наряду с традиционным учебным планом (или сценарием программы) мотивационный план. Тактика мотивации, состоящая в подбадривании, похвале, вызове на соревнование и т.п., увязывается с решениями, создающими условия для стимуляции учебы. Мотивационные аспекты учебы можно классифицировать в соответствии с такими специфическими параметрами, как соревновательность, заинтересованность, самоконтроль, уверенность и удовлетворение. При компьютерном обучении необходимо определять мотивационное состояние обучаемого, реагировать с целью мотивации на действия рассеянных, менее уверенных или недовольных обучаемых, а также поддерживать тонус уже мотивированных обучаемых.

Структура мотивационной основы деятельности обучаемого отражает перечисленные компоненты учебной деятельности, представляя их как этапы обучения. На первом - сосредоточении внимания на учебной ситуации - необходимо дать обучаемому информацию об актуальности и практической значимости темы, заинтересовать, развить стремление к получению нового знания. На втором - конкретизировать вопросы, помогающие овладению способами рациональной учебной деятельности, развивающие теоретическое мышление. На третьем этапе - выборе решения - необходимо создать индивидуальную установку на данную деятельность. На последнем этапе, когда обучаемый нуждается в оценке и корректировке действий, ему необходимо предоставить возможность выбора вида помощи, выдавать эту

помощь в доброжелательной форме, выдавать, в случае затруднений, дополнительные задачи, алгоритмические предписания по их решению и мотивационные указания.

Система учебных действий, связанных с усвоением материала, подробно описана выше. Пункты 2, 3 и 4 относятся к внешнему моделированию (в отличие от внутреннего, умственного, обеспечивающего усвоение знания) и означают возможность компьютера представлять на экране дисплея ту предметную среду, в содержание которой вводится учащийся. Правильно задать объект или явление в виде компьютерной модели можно при следующих условиях: когда будут выделены основные структурные элементы объекта и его системообразующие связи и определены типы знаковых средств, обеспечивающие реализацию выделенных связей на экране дисплея. Информационные технологии дают возможность оперативного преобразования моделей, причём при этом могут использоваться не только компьютер, но и различные установки, устройства, работающие под руководством компьютера и позволяющие наиболее полно изучить объект или явление. Такие модели выступают как средства организации действий самого учащегося, развивают его научно-теоретическое мышление, позволяют по-новому представлять объект усвоения, манипулировать им, моделируя внутреннюю структуру и включая его в различные внешние отношения.

Система контрольно-корректировочных действий включает общие контрольные действия, связанные с преобразованием объекта действия, усвоением его структуры; действия контроля, специфичные для определённого предметного содержания; самоконтроль, использующий имеющиеся навыки проверки правильности решения; корректировочные действия. Общее контрольное действие включает: объект - структурные и функциональные компоненты действия, на которое направлен контроль; продукт - оценочное знание, характеризующее соответствие или несоответствие произведённого действия требуемому или эталонному; средства - образцы компонентов контролируемого действия, содержащихся в схеме ориентировочной основы этого действия или в самой ориентировочной части действия субъекта; операции: а) сравнение, сличение каждого компонента, зафиксированного в ориентировочной схеме с соответствующими компонентами его ориентировочной основы; б) выбор адекватного объекта корректировочного воздействия. Корректировочное действие направлено на устранение обнаруженного в результате контроля рассогласования и получение требуемого продукта, заданного целью действия. Для осуществления самоконтроля контрольно-корректировочные компоненты учебной деятельности должны быть предметом специального усвоения обучаемым, а также он должен руководствоваться сознательно поставленной целью обучения.

Таким образом, компьютер в учебном процессе может применяться в следующих основных функциях:

1) как средство организации познавательной деятельности путем внешнего (предметного) и внутреннего (умственного) моделирования;

2) как средство реализации наиболее полной системы учебных действий, а также их контроля и коррекции;

3) как средство создания новых форм учебного процесса, моделирования совместной деятельности типа «преподаватель – компьютер - обучаемы», «компьютер - обучаемый», «компьютер - группа обучаемых», «преподаватель – компьютер - группа обучаемых». Имеющиеся в Интернет интерактивные средства (чаты, форумы, скайп) позволяют реализовать все виды совместной деятельности при самостоятельной работе обучаемых и в аудиторных занятиях.

Ряд исследований показали, что наиболее эффективной формой компьютерного обучения является «преподаватель – компьютер - группа обучаемых». Имеются следующие типы задач, решение которых возможно при использовании компьютера как средства обучения: 1) дидактические задачи (повышается эффективность их решения за счет

использования справочных и экспертных систем в обучении); 2) организация контроля и тренировки при сохранении традиционной формы обучения; 3) новые дидактические задачи (например, имитация эксперимента); 4) моделирование содержания объектов усвоения.

Анализ различных психологических и педагогических теорий позволил выявить две качественные компоненты учения: статичную и динамическую. Несмотря на различие позиций, авторы психолого-педагогических исследований выделяют в процессе обучения как управляемые, так и управляющие компоненты. Это, в свою очередь, позволяет построить некоторую модель с входными параметрами - состояние обучаемого до процесса обучения, характеристики самого процесса и состояние обучаемого после прохождения некоторого курса. Почти все авторы инвариантной частью обучения как статичного явления считают знания, умения и навыки (компетенции определенного уровня), с небольшим разбросом как в сторону расширения (исторический опыт, культурно-исторический опыт), так и в сторону сужения (оперантное поведение, формирование некоторого условного рефлекса). Препарированию подвергаются сами знания, их природа (смежность знака и объекта, связи между объектами и явлениями, понятия и их системы), а также процесс их усвоения. В основном, проводится аналогия между процессами усвоения знания и процессами мышления в целом (восприятие материала, осмысление и овладение им), а также между процессами усвоения знаний и процессами переработки информации (внимание и селективное восприятие, кратковременное запоминание, кодирование и переход в долговременную память, хранение, воспроизведение, генерация ответа, внешнее выполнение действия, получение обратной связи). Расположив различные теории обучения в хронологическом порядке, можно проследить, как постепенно дифференцировался сам процесс обучения, как от более крупных действий по усвоению знаний и умений произошёл переход к выделению элементарных операций и фаз обучения, так и обратно, к синтезу из элементарных действий более крупных и их взаимосвязи.

Компьютерное обучение позволяет наиболее полно реализовать и проконтролировать рассмотренные компоненты и этапы обучения, а также построить ряд моделей, как самого процесса обучения, его предмета и объекта (обучаемого).

Рассмотрим модель оценивания результатов обучения на основе часто используемой пятибалльной системы, в случае необходимости полученные различные суммы баллов могут быть приведены к этой шкале. В процессе исследования были получены две регрессионные модели выставления оценки обучаемому в компьютерном учебном курсе по результатам контроля нескольких факторов, рассматриваемых как входные параметры моделей.

Первая модель - трёхфакторная, учитывала следующие факторы:

X_1 - знакомство обучаемого с учебным материалом,

X_2 - запоминание основных положений,

X_3 - понимание.

Каждый фактор принимал два значения: -1 и 1, соответствующие плохому и хорошему знакомству с материалом, запоминанию и пониманию. Была построена матрица планирования эксперимента, в которой функцией отклика явились оценки, выставленные экспертами по совокупности значений факторов. Произведение факторов означает их взаимное влияние, например, понимание способствует лучшему запоминанию учебного материала, а без знакомства с материалом невозможно его запоминание.

В результате получено два уравнения - для минимальной (несколько заниженной) оценки знаний обучаемого (1) и максимальной (2). Диапазон оценок был от 1 до 5, что позволяет в дальнейшем масштабировать полученные оценки на любую шкалу.

$$Y_{min} = 3 + 0{,}25X_1 + 0{,}5X_2 + 0{,}75X_3 + 0{,}25X_1X_2 + 0{,}25X_2X_3 \quad (1)$$

$$Y_{max} = 3{,}875 + 0{,}357X_1 + 0{,}375X_2 + 0{,}875X_3 \quad (2)$$

Для шестифакторной модели учитывались показатели:

X_1 - мотивация,
X_2 - знакомство с материалом,
X_3 - запоминание,
X_4 - формирование понятий,
X_5 - формирование умений,
X_6 - формирование навыков.
Получены следующие уравнения (3) и (4):

$$Y_{min} = 2{,}8 + 0{,}09X_1 + 0{,}15X_2 + 0{,}25X_3 + 0{,}37X_4 + 0{,}478X_5 + 0{,}531X_6 + 0{,}125X_4X_5 + 0{,}156X_4X_6 + 0{,}157X_5X_6 \quad (3)$$

$$Y_{max} = 3{,}984 + 0{,}109X_1 + 0{,}171X_2 + 0{,}234X_3 + 0{,}359X_4 + 0{,}422X_5 + 0{,}574X_6 . \quad (4)$$

Адекватными оказались максимальная модель для трёх факторов и минимальная - для шести. Отсюда следует, что при проверке более общих знаний следует несколько завысить оценку обучаемому, а при более дифференцированном контроле - предъявить строгие требования к элементарным компонентам. Также очевидно, что при компьютерном обучении легко выделить и проверить контролируемые компоненты, а также более гибко варьировать их значениями.

Параметрами формальных моделей могут также служить другие статические и динамические показатели процесса обучения.

Выводы. Рассмотренная структура учебной деятельности и учебных действий, а также этапов их формирования, позволила произвести обобщение данных действий, осуществить их классификацию и выделить особенности учебных действий при компьютерном обучении. Определение факторов процесса обучения дало возможность формализовать оценку знаний при компьютерном обучении, сделать качественные выводы. Дальнейшие эксперименты с данными моделями и построение аналогичных с большим количеством факторов дает возможность математически моделировать и исследовать учебный процесс.

ЛИТЕРАТУРА:

1. Юрловская И.А., Гучмазова К.П. Индивидуально-образовательный маршрут студентов как механизм индивидуализации образовательного процесса современного педагогического вуза // Мир науки. – 2016. – Т. 4. –№ 2. – С. 51.
2. Тындыкарь Л.Н. Разработка метода организации движения информационных потоков образовательного процесса // Вестник государственного университета морского и речного флота им. Адмирала С.О. Макарова. – 2016. – № 1 (35). – С. 197-206.
3. Неворотов Б.К., Моисеев М.Б. Моделирование информационных структур в организации учебной деятельности // Омский научный вестник. – 2015. – № 3 (139). – С. 108-112.
4. Рыбакина Н.А. Проблемы проектирования учебной деятельности в контексте непрерывного образования // Педагогика и психология образования. – 2016. – № 1. – С. 62-71.
5. Слепко Ю.Н. Формирование профессионального интеллекта в структуре учебной деятельности студентов // Ярославский педагогический вестник. – 2016. – № 3. – С. 211-216.
6. Ильясов И.И. Структура процесса учения. – М.: МГУ, 1986. – 200 с.
7. Леонтьев А.Н. Деятельность. Сознание. Личность. – М.: Политиздат, 1975. – 117с.
8. Талызина Н.Ф. Педагогическая психология. – М.: Академия, 1998. – 288 с.
9. Давыдов В.В. Проблемы развивающего обучения. -М.: Педагогика, 1986. – 240 с.
10. Щедровицкий Г.П. Знак и деятельность. Кн. II: Понимание и мышление. Смысл и содержание. 7 лекций 1972 г. – М., 2006. – 353 с.
11. Машбиц Е.И. Психолого-педагогические проблемы компьютеризации обучения. – М.: Педагогика, 1988. – 192 с.
12. Апатова Н.В. Информационные технологии в школьном образовании. – М.: РАО, 1994. – 228 с.

REFERENCES:

1. Urlovskaya I.A., Guchmazova K.P. Individualno-obrazovatelniy marshrut studentov kak mehanizm individualizacii obrazovatelnogo processa sovremennogo pedagogicheskogo vuza [Individual and educational students route as a mechanism of individualization of the educational process of modern pedagogical university] // Mir nauki. 2016. V.3. № 2. S 51.
2. Tyndykar L.N. Razrabotka metoda organizacii dvijenia informacionnyh potokov obrazovatelnogo processa [The development of a method of organization information flows movement of the educational process] // Vestnik gosudarstvennogo universiteta morskogo I rechnogo transporta. 2016. № 1 (35). S.197-206.
3. Nevorotov B.K., Moiseev M.B. Modelirovanie informacionnyh structur v organizacii uchebnoy deyatelnosti [Modeling of information structures in the organization of learning activities]// Omskiy nauchniy vestnik. 2015. № 3 (139). S. 108-112.
4. Rybakina N.A. Problemy proectirovania uchebnoy deyatelnosti v context nepreryvnogo obrazovania [Problems of designing learning activities in the context of lifelong education] //. Pedagogika I psihologia obrazovania. 2016. № 1. S. 62-71.
5. Slepko U.N. Formirovanie professionalnogo intellecta v structure uchebnoy deyatelosti studentov [Creation of professional intelligence learning activities students structure] // Yaroslavskiy pedagogicheskiy vestnik. 2016. № 3. S. 211-216.
6. Iliasov I.I. Structura processa uchenia [The structure of learning process]. – M.: MGU, 1986. – 200 s.
7. Leontiev A.N. Deyatelnost. Soznanie. Lichnost [Activities. Consciousness. Personality] – M.: Politizdat, 1975. – 117 s.
8. Talyzina N.F. Pedagogicheskaya psihologia [The educational psychology]. – M: Academia, 1998. – 288 s.
9. Davidov V.V. Problemy razvivauchego obuchenia [The problems of developing communication]. – V.: Pedagogika, 1986. – 240 s.
10. Schedrovizkiy G.P. Znak I deyatelnost [The sign and the activities]. Kn. II: Ponimanie I myshlenie. Smysl I soderjanie. 7 lekciy 1972. - M., 2006. – 353 s.
11. Mashbic E.I. Psihologo-pedagogicheskie problemy computernogo obuchenia [Psychological and pedagogical problems of computerization of education]. – M.: Pedagogika, 1988. – 192 s.
12. Apatova N.V. Informcionnye tehnologii v shkolnom obrazovanii [Information technology in school education]. – M.: RAO, 1994. – 228 s.

Без рецензії.

д.пед.н., д.е.н., проф. Апатова Н.В.

СТРУКТУРА НАВЧАЛЬНОЇ ДІЯЛЬНОСТІ ПРИ КОМП'ЮТЕРНОМУ НАВЧАННІ

У статті розглядається структура навчальної діяльності, її основні компоненти і етапи формування при традиційному і комп'ютерному навчанні, обґрунтовується необхідність врахування виділених особливостей при розробці комп'ютерних програм навчального призначення для самостійного, у тому числі, дистанційного навчання.

Засвоєння навчальної інформації при комп'ютерному навчанні пов'язано з емпіричної, евристичної, репродуктивної по перетворенню моделі і отримання нового знання і практичної видами діяльності. Дані та інші види навчальної діяльності докладно характеризуються.

Розбудовані математичні моделі процесу навчання, які дозволяють формалізувати оцінку формуємих компетенцій. Компетенції розкриті через знання та уміння, в моделі оцінюються фактори знайомства з навчальним матеріалом, запам'ятовування й розуміння, на основі експертних оцінок виставляється кількісна оцінка.

Ключові слова: навчальна діяльність, види навчальної діяльності, комп'ютерне навчання, математична модель процесу навчання, компетенції.

prof. Apatova N.V.

THE STRUCTURE OF EDUCATIONAL ACTIVITIES COMPUTER TRAINING

The article describes the structure of educational activity, its main components and stages of the traditional and computer training, the necessity of accounting selected features in the development of computer programs for educational purposes for self, including distance learning.

The assimilation of educational information by computer training includes the empirical heuristic, reproductive patterns for transform new knowledge and practical activities. These and other learning activities are characterized in detail.

The mathematical model of the process of learning to enable an assessment to formalize the formed competencies. Competencies are disclosed through the knowledge and skills they are valued in the model as factors of acquaintance with the material, memory and understanding, based on expert judgment exhibited quantitative assessment.

Keywords: learning activities, learning activities, of computer training, a mathematical model of the process of learning, competence.

УДК 004.056.5

д.т.н., проф. **Бойченко О.В.** (Тавр.НУ)
Тупота Е.С. (Тавр.НУ)

DLP-ТЕХНОЛОГИИ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В статье исследованы возможности использования систем типа Data Leak Prevention для выявления внешних вмешательств и утечки корпоративной информации. Определены отличительные признаки технологии исследования на основе DLP-систем для анализа защищенности распределенной информационной системы управления предприятием.

Установлено, что инновационные DLP-системы наиболее эффективно использовать для построения системы информационной безопасности в экономической сфере в части организации обнаружения фактов несанкционированной передачи конфиденциальных драанных неавторизованным пользователям.

Обоснована актуальность применения исследованной технологии для усовершенствования системы мер хранения клиентской базы экономического предприятия путем оперативного мониторинга каналов утечки.

Разработана методика рационализации выбора DLP-системы соответственно особенностям деятельности предприятия в условиях возможных угроз информационной безопасности и ключевых аспектов по оптимизации системы экономической безопасности.

Ключевые слова: информационная система, информационная безопасность, DLP системы, мониторинг утечек.

Постановка проблемы. Актуальность исследования обусловлена необходимостью разработки новых подходов в решении защиты коммерческих данных фирмы в условиях

широкого и повсеместного роста фактов несанкционированного доступа к ресурсам компании и утечек информации.

При ведении любой коммерческой деятельности на данном этапе развития современного общества важнейшим аспектом является информация. Потеря данных является критичной для фирмы, поскольку это может привести к потере клиентской базы предприятия.

Анализ экспертных исследований современной проблематики экономической безопасности предприятий в части утечек корпоративной информации, проведенный аналитическим центром «InfoWatch», показывает 1505 случаев потери важных данных коммерческой деятельности (рис. 1), что на 10% больше по сравнению с 2014 годом. При этом 32% обнаруженных проникновений относятся к внешним угрозам.

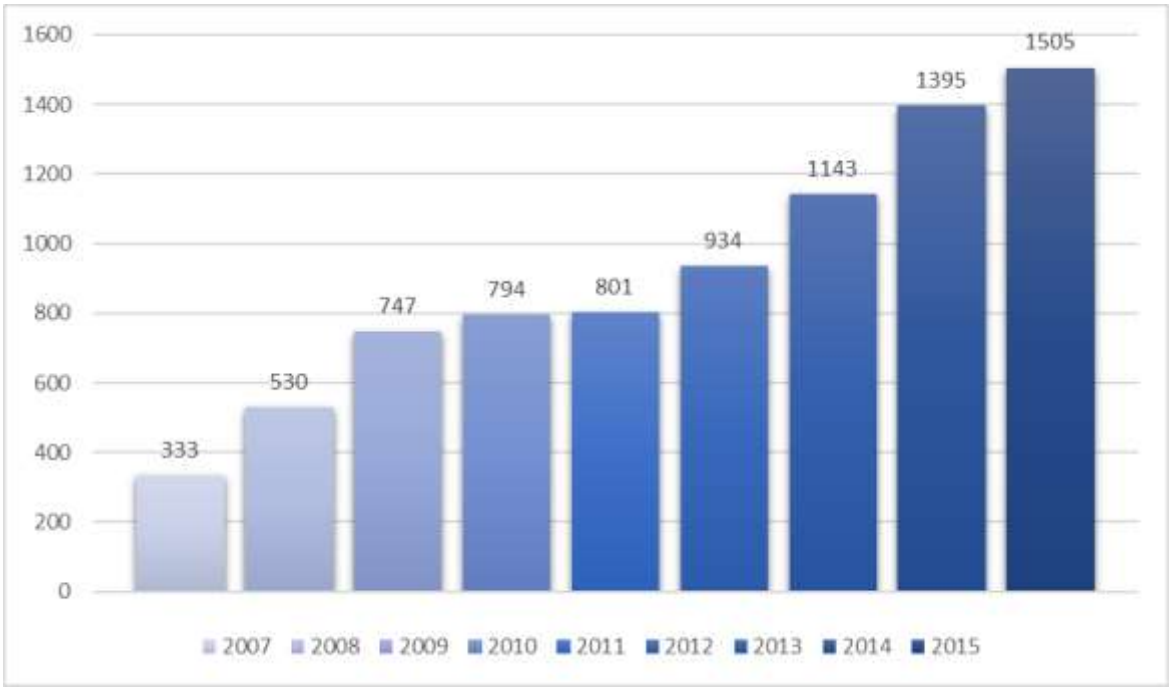


Рис. 1. Количество утечек коммерческой информации на предприятиях за 2007-2015 гг.

Анализ характера выявленных утечек показывает, что в большинстве случаев утечка организована с помощью атаки на массивы данных (клиентская база, база поставщиков, база посредников и т.д.). Кроме того, установлено, что 8% эпизодов, связанных с потерей данных, являются проникновениями с несанкционированным доступом к информации с последующим ее изменением и превышением прав доступа [1].

Приведенные результаты исследования определяют необходимость разработки новых способов и методов в системе защиты данных распределенной корпоративной информационной системы.

Постановка задачи. Цель исследования состоит в проведении анализа механизмов защиты коммерческих данных предприятия на основе DLP-систем, а также разработки новых методик их применения для оптимизации функционирования системы экономической безопасности.

Изложение основного материала. Информационная безопасность является ключевым аспектом в деятельности предприятия. Риски, связанные с утечкой данных, влияют на его привлекательность для инвесторов и клиентов.

Опыт показывает, что вероятность образования внутреннего канала утечки информации (пользовательский аспект) в компании выше, чем утечка данных по причине взлома (внешний аспект) [2]. Наиболее часто это связано с неправомерными или халатными действиями сотрудника предприятия по ошибочной отправке информации не зарегистрированному адресату. Потому для организации обнаружения несанкционированной передачи конфиденциальных данных неавторизованным пользователям на предприятиях необходимо внедрять инновационные технологии исследования, в частности на основе DLP-систем.



Рис. 2. Потенциально опасные каналы утечки информации

Главным достоинством DLP-технологий является то, что их внедрение в процессы автоматизации управления деятельностью предприятия обеспечивает создание условий для предотвращения утечек конфиденциальной информации и других коммерческих данных.

Кроме того, программный комплекс DLP позволяет вести учет состояния потенциально опасных каналов связи, по которым возможно могут проходить утечки корпоративной информации (рис. 2.)

Результаты экспертных заключений указывают на необходимость для каждого предприятия, в соответствии с принятым регламентом (политикой безопасности), организовывать систему контроля над потенциально опасными каналами связи. Особого внимания требует необходимость обеспечения своевременного контроля бизнес-процессов в части обработки и использования конфиденциальной информации в комплексном сочетании кадровой политики по подбору лиц, ответственных за своевременный контроль сетевой активности рабочих мест [3].

Отдельной проблемой, наряду с внедрением программного комплекса, является необходимость эффективного функционирования аппаратного комплекса консоли централизованного управления DLP системой. Исследования определяют, что в настоящее время наиболее надежными комплексами являются системы таких мировых брэндов, как Hewlett-Packard, IBM, EMC, Dell и т.д.

Следует также отметить, что такие системы строятся на анализе потока данных

(«алгоритме обнаружения»), функционирующего внутри информационной системы (ИС).

Использование такого алгоритма при обнаружении потока утечки данных в системе приводит к немедленному срабатыванию активной компоненты DLP, и передача потока блокируется. При этом DLP-система проводит обязательный анализ данных, входящих в защищаемую систему, а выявление степени конфиденциальности информации и дальнейшее ее блокирование происходит благодаря проведению аналитических операций по выявлению содержания пакетов. Однако следует отметить, что не все DLP-системы эффективно определяют содержание передаваемого пакета данных вследствие того, что отдельным программным продуктам свойственно нахождение специальных маркеров, характерных для конфиденциальной информации (гриф документа, мета-код, значение хэш-функций и т.д.).

Характеризуя отличительные признаки анализируемой технологии, особо следует выделить задачу анализа потока данных, являющейся ключевой для DLP-системы в целом. Наряду с этим, современный этап развития информационно коммуникационных технологий позволяет интегрировать в DLP-систему большое количество инновационных нетривиальных методов анализа, позволяющих повысить эффективность технологий исследования в целом [4].

При этом современные технологии в области исследования условно можно разделить на две группы (рис. 3).



Рис. 3. Методы анализа потоков данных в DLP-системах

Детальное изучение указанных методов позволяет заключить, что морфологический анализ, входящий в группу проактивных методов, является самым популярным способом нахождения утечек конфиденциальной информации. Его суть состоит в нахождении ключевых слов в передаваемых текстах.

В аналогичную группу входит статистический анализ данных. Суть данного метода заключается в расчете вероятностей утечки определенной информации с предприятия. Однако данный метод отличается большей сложностью в реализации, так как требует необходимости разработки дерева решений для последующего проведения анализа.

Метод шаблонного сравнения также представляет достаточно высокую продуктивность за счет простой интеграции в программную среду информационной системы на основе шаблонов, свойственных конфиденциальной информации данного предприятия.

Характеризуя анализ цифровых отпечатков и цифровых меток (вторая основная группа методов), следует отметить, что он представляет собой совокупность конкретных характеристик документа, по которым его впоследствии можно будет распознать. Суть метода заключается в присвоении меток информации, доступность которых характерна только для клиентских модулей DLP-системы.

Особо следует выделить основную задачу DLP-систем, связанную с мониторингом, идентификацией и защитой конфиденциальной информации предприятия.

Для решения указанной задачи DLP-система, прежде всего, нацелена на обеспечение защиты в каналах утечек, связанных с:

- внешними устройствами;
- информацией, находящейся в сетевом доступе;
- средствами сетевой печати;
- Веб-ресурсами;
- передачей файлов по каналам HTTP, HTTTPS, FTP;
- электронной почтой;
- программами взаимодействия с клиентами.

Как указывалось, ранее, внутри информационной системы каждому потоку данных присваиваются метки и тэги. Использование такого подхода в дальнейшем обеспечивает более точный анализ контента, что, в свою очередь, создает условия для администратора по заданию определенных правил для отбора потоков. Кроме того, в режиме реального времени обеспечивается анализ всех событий передачи данных внутри системы, а также осуществляется блокировка нежелательных потоков.

Анализируя основные приложения для обеспечения функционирования рассматриваемой системы, прежде всего, следует выделить программный продукт Websense Data Security Suite, который обеспечивает высокий уровень мониторинга по каналам передачи электронной почты, а также сообщений MS Exchange, HTTP, FTP, HTTPS.

Кроме того, система может отправлять уведомления администратору о факте передачи конфиденциальной информации и полностью блокировать нежелательные потоки. Вместе с этим, в комплекте с системой представлен ряд готовых стандартных шаблонов и надстроек, что позволяет создавать условия для эффективного разграничения доступа к информации, а также ее удалению и изменению.

Опыт показывает, что для расширения функционала данной DLP-системы необходимо использовать специализированные программы, такие как Data Endpoint, Data Monitor, Data Protect, Data Discover. При этом, простота внедрения системы обусловлена наличием специального мастера. Однако недостатком данной системы является отсутствие русификатора, что может затруднить внедрение технологии в российских кампаниях.

Falcongaze SecureTower является отечественной разработкой, основанной на поиске конфиденциальной информации за счет ключевых слов, тег, подписей и т.д. Такой подход обеспечивает отслеживание трафика по всем контролируемым каналам связи.

Особенностью данного продукта является полная интеграция в среду Skype, что создает дополнительные условия защиты информации за счет осуществления перехвата голосовых сообщений. Кроме того, система обеспечивает отслеживание работы сотрудников предприятия использованием функции периодического производства скриншотов экрана сотрудников. Дополнительно система так же осуществляет контроль на уровне IP-адресов, создавая определенные карты посещения.

Функционально структура Falcongaze SecureTower состоит из сервера перехвата трафика, сервера контроля рабочих станций и сервера обработки информации. Еще одним явным преимуществом данной системы является ее легкая масштабируемость, что является весьма актуальным для развивающихся компаний [5].

Проведенные исследования указывают, что большинство известных DLP-систем имеют одинаковый функционал, однако могут иметь конкретные преимущества для бизнеса (таблица 1).

При этом каждому предприятию среднего бизнеса для решения вопросов обеспечения конфиденциальности информации на основе внедрения DLP-систем, необходимо исходить из номинальной стоимости комплекса в целом и максимального количества контролируемых каналов. Кроме того, предприятию необходимо обеспечить ответственного администратора системы и ответственного за безопасность системы в целом. В целом каждый выбранный комплекс может обеспечивать полную гарантию сохранности корпоративной информации на

предприятии. Анализ данных таблицы позволяет заключить, что на предприятии среднего масштаба (примерно 250 рабочих мест) стоимость комплекса DLP обойдется приблизительно в 1 000 000-2 500 000 руб.

Таблица 1

Сравнительная таблица наиболее известных DLP-систем

Название Критерий оценки системы	Falcongaze SecureTower	Websense Data Security Suite	InfoWatch Security Monitor
Общие характеристики			
Модульность	Нет	Да	Нет
Место установки	Оператор, сервер	Оператор, сервер	Оператор, сервер
История попыток взлома	Да	Да	Да
Анализ контекста утечек	Нет	Да	Нет
Количество «ответственных» мест	2	Любое количество	Ограниченное количество
История осуществлённых взломов	Да	Да	Да
Рабочая Лицензия	Каждое рабочее место	-	Контролируемые каналы
Контролируемые каналы			
IM	Да	Да	Да
HTTP/HTTPS; FTP	Да	Да	Да
Skype	Видео, звук, текст	Нет	Текст
Почта	Да, корпоративная и личная	Да, корпоративная и личная	Да, корпоративная и личная
Социальные сети	Да	Да	Да
Внешние подключаемые устройства	Отсутствует	Полный контроль	Дополнительная надстройка
Сетевая печать (с возможностью оптического распознавания текста OCR)	Да	Да	Информация отсутствует
Аналитические характеристики			
Определение и анализ не правильного шифрования	Да	Да	Да
Анализ подозрительного трафика	Да	Да	Да
Анализ мультимедийных вложений	Нет	Да	Да
Остановка передачи несанкционированных сообщений	Нет, происходит информировани е контролера системы	Происходит обучение системы оператором	Да, система определяет автоматически
Хранение отчетности	Да	Да	Да
Стоимостные показатели			
Цена рабочего места	6000 руб.	8000-10000 руб.	Информация отсутствует

Полученные научные результаты. Таким образом, в результате проведенного исследования установлено, что эффективная деятельность современных предприятий не возможна без использования инновационных технологий защиты конфиденциальной информации, что обусловлено высоким уровнем утечек информации, прежде всего по внешним каналам (33% за 2015 год).

По результатам исследования разработана таблица, использование которой обеспечивает рационализацию выбора конкретной DLP-системы для предприятия путем ориентировки на выделение ключевых аспектов, отличающих программные комплексы различных фирм.

Выводы. В системе информационной безопасности фирмы DLP-системы являются эффективным инструментом, который позволяет создавать условия для решения проблем защиты конфиденциальной информации. Это обеспечивает значительное снижения риска потери критических данных, высокий уровень мониторинга каналов утечки, возможность контроля периметра корпоративной ИС наряду с доступностью стоимости в установке на действующих системах управления.

Дополнительный эффект внедрения систем достигается комплексным использованием с другими мерами контроля несанкционированного влияния на информационные ресурсы предприятия.

ЛИТЕРАТУРА:

1. Бойченко О.В.Технологии data leak prevention в системе защиты коммерческих данных / О.В. Бойченко, Е.С. Тупота // Региональная информатика. Юбилейная XV Санкт-Петербургская междунар. конфер., 25-28 окт. 2016 г., сборник тезисов. - С-ПБ, 2016. – С.146-147.

2. Бойченко О.В. Пользователь в системе информационной безопасности АСУ / О.В. Бойченко // Теория и практика экономики и предпринимательства: XII Междунар. науч.-технич. конф., 23-25 апреля 2015 г.: тезисы докладов. – Симферополь, 2015. – С. 12-15.

3. Жабин С.Ф. Исследование систем обнаружения вторжений операционного уровня информационных систем / С.Ф. Жабин, А.Е. Захаров // Тезисы научно-технического семинара «Координационный совет по информатизации Владимирской области», 2008. – С. 34-37.

4. Фенюк М.В. Аналіз недоліків систем автоматизованого захисту інформації та методів біометричної автентифікації, які в них використовуються / М.В. Фенюк // ММС, 2012. – №3. – С.116-123.

5. Шимон Н.С. Способы и средства защиты от сетевых атак в Единой информационно-телекоммуникационной системе органов внутренних дел // Вестник ВИ МВД России, 2009. – №1. – С.164-167.

REFERENCES:

1. Bojchenko O.V., Tupota E.S. (2016) Tehnologii data leak prevention v sisteme zashhity kommercheskih dannyh [Data Leak Prevention Technologies in systems of economics security enterprise] Regional’naja informatika. Jubilejnaja XV Sankt-Peterburgskaja mezhdunar. konfer., 25-28 okt. 2016 g., sbornik tezisov, S-PB, 2016. – pp.146-147 (In Russian).

2. Bojchenko O.V. Polzovatel v sisteme informacionnoj bezopasnosti ASU [Users in security systems like ASC] / O.V. Bojchenko // Teorija i practica economici i predprinimatelstva. – Simferopol, 2015. – pp. 12-15. (In Russian).

3. Zhabin S.F., Zaharov A.E. (2008) Issledovanie sistem obnaruzhenija vtorzhenij operacionnogo urovnja informacionnyh sistem [Research of systems which detect on operational-level information systems] Tezisy nauchno-tehnicheskogo seminara «Koordinacionnyj sovet po informatizacii Vladimirskoj oblasti», 2008. – pp. 34-37. (In Russian).

4. Fenjuk M. V. Analiz nedolikiv sistem avtomatizovanogo zahistu informacii ta metodiv biometrichnoї avtentifikacii, jaki v nih vikoristovujut’sja [Analysis of the shortcomings of automated information security and biometric authentication techniques used in them] MMS, 2012. - №3. - pp.116-123 (In Ukraanian)

5. Shimon Nikolaj Stepanovich Sposoby i sredstva zashhity ot setevyh atak v Edinoj informacionno-telekommunikacionnoj sisteme organov vnutrennih del [Ways and means of protection against network

attacks in a Single information-telecommunication system of Internal Affairs] // Vestnik VI MVD Rossii, 2009. - №1. - pp.164-167. (In Russian)

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

д.т.н., проф. Бойченко О.В., Тупота О.С.

DLP-ТЕХНОЛОГІЇ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті досліджено можливості використання систем типу Data Leak Prevention для встановлення зовнішніх втручань й витоку корпоративної інформації. Визначені відмітні ознаки технології дослідження на основі DLP-систем для аналізу захищеності розподіленої інформаційної системи управління підприємством.

Встановлено, що інноваційні DLP-системи найбільш ефективно застосовувати для розбудови системи інформаційної безпеки в економічній галузі в частині організації виявлення фактів несанкціонованої передачі конфіденційних даних неавторизованим користувачам.

Обґрунтована актуальність застосування досліджуваної технології для удосконалення системи заходів зберігання клієнтської бази економічного підприємства шляхом оперативного моніторингу каналів витоку.

Розроблено методику раціоналізації вибору DLP-системи відповідно особливостям діяльності підприємства в умовах можливих загроз інформаційної безпеки та ключових аспектів з оптимізації системи економічної безпеки.

Ключові слова: інформаційна система, інформаційна безпека, системи DLP, моніторинг витоків.

prof. Boychenko O.V., Tupota E.S.

DLP TECHNOLOGY IN THE SYSTEM OF ECONOMIC SECURITY OF ENTERPRISE

This Article reveals the possibility of using systems such as Data Leak Prevention for identifying external interference and leakage of corporate information. The distinctive features of technology study on the basis of DLP-systems for security analysis of distributed information system of enterprise management were identified.

Innovative DLP system is most effective to use to build information security system in the economic sphere on the detection of unauthorized transmission of confidential data to unauthorized users.

Actuality of application of the studied technologies to improve the system of measures of a client base of economic enterprise by online monitoring of leakage channels were also established.

Method of rationalizing the choice of a DLP system according to characteristics of enterprise activity in terms of possible information security threats and key aspects for the optimization of the system of economic security were developed.

Key words: information system, information security, DLP systems monitor leaks.

УДК 811.11 к.е.н., доц. **Горячева К.С.** (ВІКНУ)

АНАЛІЗ ФУНКЦІОНАЛЬНОГО ПОТЕНЦІАЛУ АБРЕВІАТУР В АНГЛОМОВНІЙ ПОЛІТИЧНІЙ СФЕРІ

Тенденція до економії мовних засобів присутня в усіх системах мови (фонетична, лексична, семантико-граматична, синтаксична) виявляється на різних рівнях функціонування мовних одиниць – речень, словосполучень, слів, морфем, фонем.

Продуктивним видом лексичної компресії є абревіація. Скорочування виразів та їх поєднання таке ж давнє, як і письмо, оскільки люди завжди враховували принцип економії мовних засобів. Розв'язання проблем абревіатури та її функціонального потенціалу доречно вивчати на основі політичного дискурсу, так як він включає в себе більшість сфер людської діяльності і відображає сучасні тенденції розвитку мови та її складових.

Ключові слова: абревіатура, лексично-семантичне коло, семантичне значення, полісемічний ряд, політичний дискурс.

Вступ. Кожна іноземна мова – це живий організм, що зазнає різних змін. Процес становлення живої мови, її удосконалення ніколи не припиняється. Мовні системи рухаються у певному напрямку, який можна розглядати як "еволюцію мови". Метою такого руху є передача все більшої інформації за одиницю часу. А оскільки одиниця часу є константою, то модифікації зазнає власне мова та засоби її вираження. Тенденція до економії мовних засобів присутня в усіх системах мови та виявляється на різних рівнях функціонування мовних одиниць.

Актуальність. Неповнота досліджень явища абревіатури в англомовному дискурсі і відсутність єдиної класифікації абревіатур в англійській мові, що доречно вивчати на основі політичного дискурсу, оскільки він включає в себе більшість сфер людської діяльності і відображає сучасні тенденції розвитку мови та її складових.

Об'єктом дослідження є абревіатури зі статей англомовних політичних газет та журналів.

Постановка завдання. В статті вивчається і визначається функціональний потенціал в англомовній політичній сфері.

Наукова новизна полягає в тому, що абревіатури в англомовній політичній сфері класифіковані відповідно до лексико-семантичних кіл, для чого визначено місце абревіатур полісемантичного поля в словниках абревіатур та скорочень.

Виклад основного матеріалу. Щоб визначити функціональний потенціал абревіатур в англомовній політичній сфері звернемося до словників абревіатур, адже місце в словнику тієї чи іншої абревіатури допоможе нам з визначенням функціонального потенціалу.

Частина досліджуваних абревіатур має незначну або несуттєву відмінність в написанні, при цьому значення таких абревіатур не змінюється. Назви предметів та явищ виражених абревіатурами даного типу мають два варіанти абревіатурної форми, одна з яких має від 1 до 3 додаткових алфавітних літер, які доповнюють основні літери спрощеного варіанту самої абревіатури. Ці додаткові літери абревіатури можуть стояти як на початку так в середині, і на кінці скороченого слова. Прикладом таких абревіатур можуть бути такі одиниці як:

The United States federal earned income tax credit (EITC or EIC), the United States Environmental Protection Agency (EPA or USEPA), the United States Department of Health and Human Services (HHS or USDHHS), the National Council of the Churches of Christ in the USA (NCCCUSA or NCC), special operations forces (SOF or SF), The United States of America (USA or US), The United States Department of Veterans Affairs (VA or USDVA), "weapon of mass destruction" (WMD or WoMD), California (CA, Calif., Cali., US-CA), Florida (FL, Fla. US-FL), Michigan (MI, Mich.US-MI ISR), intelligence, surveillance, and reconnaissance Task Force (ISR or ISR TF). Остання наведена організація має навіть іншу назву, яка утворює іншу абревіатуру,

проте саму суть значення не змінює. Це - Surveillance, Reconnaissance, and Intelligence Group (SRIG).

Отже, в умовах економії часу та місця навіть самі абревіатури мають конкуренцію між собою. Так коротші абревіатури (*EIC, HHS, VA* та *NCC)* мають переваги перед повними абревіатурними скороченнями цих же словосполучень (*EITC, USDHHS, USDVA* та *NCCCUSA).*

Однак, це не завжди спрацьовує. Для таких абревіатур як *SOF* чи *SF* важливим є не обсяг інформації, а її вимова, а також наголошення на важливості всіх елементів в абревіатурі. Так «О», яка відповідає за «operations», вказує на невід'ємність та цінність цього слова в абревіатурній структурі special operations forces.

Серед абревіатур зустрічаються синоніми, які різняться своєю формою написання, хоча мають пряме відношення до об'єкта, який вони позначають. Серед досліджуваних нами абревіатур ми знайшли такі:

*Chief executive officer (**CEO**) – managing director (MD), chief executive (CE), the Democrats (**D**) – Social and Liberal Democrats (SLD), Liberal Democrats (Lib Dems), European Union (**EU**) – the European Communities (EC), the Federal Bureau of Investigation (**FBI**) – the Bureau of Investigation (BOI), "Grand Old Party" (**GOP**) – the Republican Party (**R**), National Collegiate Athletic Association (**NCAA**) - Intercollegiate Athletic Association of the United States (IAAUS), the Republican Jewish Coalition (**RJC**), the National Jewish Coalition (NJC), the fast track negotiating authority (FTNA) – trade promotion authority (**TPA**), human immunodeficiency virus infection (**AIDS**) - acquired immunodeficiency syndrome (**HIV**), electronic health record (EHR) – electronic patient record (EPR) та electronic medical record (EMR).*

За даними результатами важко визначити, яка закономірність вживання тієї чи іншої абревіатури мала більший вплив. В даних групах синонімів мовці вживали ту чи іншу абревіатуру з різних принципів. Перш за все це економія місця та часу. Це стосується таких абревіатур ***D**, SLD, Lib Dems; **TPA**, FTNA.* Іншою причиною є застарілість, неактуальність абревіатури – ***NCAA,** IAAUS.* Абревіатура IAAUS передувала абревіатурі NCAA, хоча обидві вони означають один і той же об'єкт. Проте в даній категорії зустрічаються абревіатури, обидва варіанти якої рівноправно вживаються в мовленні. *GOP* та *R; AIDS* та *HIV; EHR, EPR* та *EMR.*

І останню групу, яку слід розглядати серед абревіатур – це абревіатури, які мають однакову зовнішню форму, проте мають різне звукове оформлення при повному розкритті абревіатури. Це не є явище полісемії, оскільки семантичне значення абревіатури відноситься до одного об'єкту.

Серед досліджуваних абревіатур ми можемо бачити такі приклади як:

GI – «Government Issue» або «General Issue», але також як і «galvanized iron», «державне майно», «основне заперечування» та «оцинкований метал» - все це вказує на один і той же об'єкт – солдати США. *SUV – sport utility vehicle або suburban utility vehicle.* «Спортивний» та «загородній» відносяться як синонімічні значення в даній абревіатурі.

Іншою категоріальною групою у лексико-семантичному колі є антоніми. Вони зустрічаються значно рідше, ніж синоніми. Серед досліджуваних нами абревіатур можна навести такі приклади: *Mr. – Mister та Mrs. – Mistress*, які є протиставленням статі людини та розрізняють звернення до чоловіка чи жінки. А також абревіатури латинського походження, які позначають протилежні явища часу – день та ніч. Відповідно абревіатури для них - *a.m.* та *p.m.*

Полісемія також відіграє важливу роль у визначенні парадигматичних відношень абревіатури у в з іншими одиницями речення. Досліджуючи абревіатури в електронному словнику абревіатур та акронімів http://www.allacronyms.com/ ми дізналися, що абревіатура має різну кількість тих чи інших значень. Кількісні показники коливаються від одиниць до кількох сотень. Можна сказати, що найбільшу полісемію має така абревіатура як CA. Вона має в собі 812 значень, які непов'язані між собою. Далі в напрямку спадання слідують AP –

619 та MS – 615. Серед наших абревіатур, що досліджувалися Association Press займає 5 позицію в полісемічному ряді та Mr. – більше ніж 20. P.M. – має 527 одиниць різного значення, нас цікавить post meridiem, і воно знаходиться на 13 місці в даному полісемічному ряді.

Найменшу кількість варіантів в полісемічному ряді мають такі абревіатури як: CO2, акронім LULAC, графічні абревіатури Calif., G-7, G-8. Всі вони мають лише по одному значенню, і не мають багатозначності. 3 значення має абревіатура ESPN, 4 – LBJ, 6 – NAACP. Семантичні значення цих абревіатур, які було вжито в досліджуваних текстах, займають перші позиції в полісемічному ряді.

В цілому, щоб представити цілісну картину полісемічного ряду абревіатур та їх місце у словнику слід звернутися до рис. 1.



Рис. 1

Найчастіше абревіатури мають значень від 10 до 20, відповідно 13 % від загальної кількості абревіатур. А на другому місці знаходяться абревіатури, які займають по 11 %, і ми маємо 2 групи: від 2 до 10 значень та від 150 до 200. По 10 % відходить абревіатурам, які мають від 20 до 30 значень та від 100 аж до 150. 9 % займають абревіатури, які в своєму полісемічному ряді мають від 60 до 70 значень; 5% - від 300 до 350 значень; 4 % - від 40 до 50 значень та від 70 до 80 значень; 3 % - від 50 до 60 значень; по 2 % - від 80 до 90 значень, від 200 до 250 значень, від 250 до 300 значень, від 400 до 450 значень, від 450 до 500 значень, від 600 до 650 значень. І по 1 % складають абревіатури від 90 до 100 значені , від 350 до 400 значень і від 800 значень і вище.

На діаграмі рис. 2, бачимо місце абревіатурного значення, який досліджували в словниковому ряді полісемантичного поля. 49 % належить тим абревіатурам, які стоять першими в полісемантичному ряді. Отже, можна сказати, що дані абревіатури мають найбільшу частоту вживання та асоціюються саме з тим значенням, які зустрічалися в досліджуваних текстах політичної сфери.

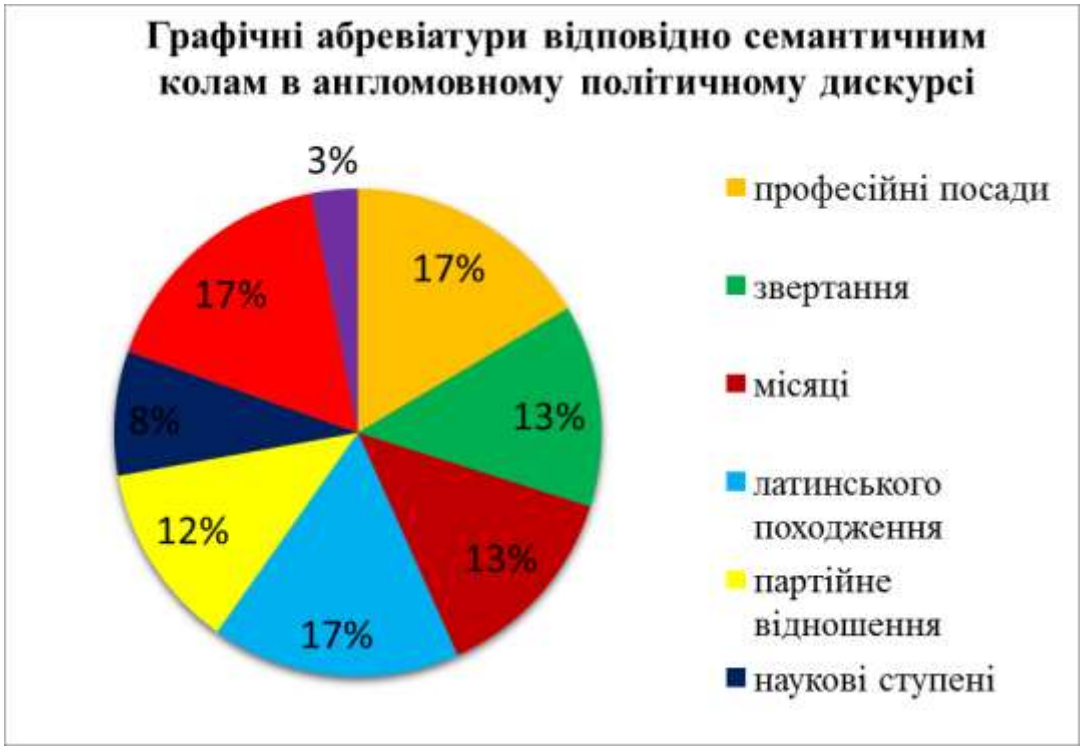


Рис. 2

Проаналізувавши обидві діаграми, ми можемо сказати, що в політичному дискурсі використовуються різноманітні абревіатури з різною кількістю семантичних значень. Проте навіть серед такої кількості як 500 чи 600 значень, значення, які були використані в політичному дискурсі мають першочергові місця, що вказує на значущість даного значення в мовленні.

Наприклад, абревіатура VA зустрілася в даному контексті:

*«Other priorities for the young veteran's group this year include ending the **VA** backlog, strengthening the post-9/11 GI Bill, helping veterans get jobs and improving health care for all veterans.»*

Серед 192 можливих семантичних значень підходить лише одне і воно знаходиться на першому місці серед інших значень:

1) Veterans Affairs, 2) Veterans Administration, 3) visual acuity, 4) volt ampere, 5) vital area, 6) volcanic ash, 7) vacuum aspiration, 8) Value-Added, 9) Velocity at Apogee, 10) Virginia, 11) virtual address і т.д. На цьому семантичне наповнення даної абревіатури в словнику не завершується.

Але не всі абревіатури, які використовували в політичному дискурсі займали одне з перших трьох місць. Так, наприклад, абревіатура республіканської партії GOP – *Grand Old Party. З*начення даної абревіатури має бути розкрите в нижче наведеному прикладі і посідає 9-те місце.

«Over the weekend, he gave the Republican Party a 60 percent chance of taking back the Senate, clarifying the GOP *would gain a total of six seats.»*

А ось розкриття значення даної абревіатури в словнику: 1) Government of Pakistan, 2) Ground Operations Panel 3) General Operating Procedures, 4) Good Operating Practices, 5) Gross Operating Profit, 6) General Operational Plot, 7) Government of Panama 8) Government of the Philippinesм **9) Grand Old Party**, 10)Ground Observer Post, 11) Ground Operations Procedure, 12) Group of Pictures 13) Gallant Old Party і т.д. аж до 38 значення.

Є такі випадки, коли абревіатурне значення в нашому контексті займало одне з останніх або навіть останнє місце серед усіх значень абревіатури. Наприклад, наведемо таку абревіатуру як SOPA. Текстовим прикладом буде фрагмент:

«No doubt causing heartburn for the U.S. entertainment and internet content providers, the chairman also took aim at moves to make the internet highway companies (viz, Google, Facebook) legally responsible for content (he specifically called out recent legislative proposals such as ***SOPA*** *and PIPA as examples).»*

Всі значення абревіатури *SOPA* в словнику наступні:

1) Synchronous Orbit Particle Analyzer, 2) Senior Officer Present Afloat, 3) Survey of Pain Attitudes, 4) Society of Professional Archeologists, 5) Synchronous Orbit Plasma Analyzer, 6) syndrome of primary aldosterone's, 7) Southern Oregon Photographic Association 8) Standard Operating Procedures Amplified, 9) **Stop Online Piracy Act**.

Отже, кожна абревіатура має різне місце в словнику, проте порівнюючи їх із загальною кількістю значень однієї і тієї ж самої абревіатури, можна сказати, що абревіатури, які зустрілися в досліджуваних джерелах, знаходяться на перших десяти місцях на відміну від інших, які можуть займати соте місце у всьому полісемічному ряді.

Висновки. З даного дослідження ми можемо сказати, що в політичному дискурсі в англійській мові існує велика кількість абревіатур. Проте не всі абревіатури відносяться до суто політичної термінології, оскільки політична діяльність багатогранна і включає лексику всіх сфер людського існування.

При визначенні функціонального потенціалу абревіатур в англомовній політичній сфері виявлено, що лексико-семантичне поле абревіатур має різний об'єм. Синонімічні ряди складаються здебільшого лише з двох або трьох синонімів.

ЛІТЕРАТУРА:

1. Алексеева Н. Н. Типология сокращенных лексических единиц современного английского языка / Н. Н. Алексеева. – М.: Наука, 1984. – 151 с.

2. Борисов В. В. Аббревиация и акронимия. – Москва, 1972. – 156 с.

3. Дюжикова Е. А. Аббревиация сравнительно со словосложением: структура и семантика / Е. А. Дюжикова. – М.: МГУ, 1997 – 340 с.

4. Нагорна Л.П. Політична мова і мовна політика: діапазон можливостей політичної лінгвістики. – К.: Світогляд, 2005. – 315 с.

5. Clemens Raymond, Graham Timothy Introduction to Manuscript Studies Cornell University Press. 2007. – 320.

REFERENCES:

1. Alekseeva N. (1984). Typology of brief lexical units of modern English.- M.:Nauka, 1984, 151 p. (In Russian).

2. Borisov V. (1972). Abbreviation and acronymus. – Moscow, 1972, 156 p. (In Russian).

3. Dyuzhykova E. (1997). Abbreviation comparatively with drafting of word: structure and semantics. – M.: MGU, 1997, 340 p. (In Russian).

4. Nahorna L. (2005). Political language and language politics: range of possibilities of political linguistics. – K.: Svitohlyad, 2005, 315 p. (In Ukrainian).

5. Clemens R., Graham T. (2007). Introduction to Manuscript Studies. - Cornell University Press, 2007, 320 p.

Рецензент: к.е.н., доц. Костюк В.Р., зав. кафедри фундаментальних економічних наук, ВНЗ IV рівня аккредитації «Національна академія управління»

к.э.н., доц. Горячева К.С.

АНАЛИЗ ФУНКЦИОНАЛЬНОГО ПОТЕНЦИАЛА АБРЕВИАТУР В АНГЛОЯЗЫЧНОЙ ПОЛИТИЧЕСКОЙ СФЕРЕ

Тенденция к экономии языковых средств присутствующая во всех системах языка (фонетическая, лексическая, семантико-грамматическая, синтаксическая) проявляется на разных уровнях функционирования языковых единиц - предложений, словосочетаний, слов, морфем, фонем.

Продуктивным видом лексической компрессии является аббревиация. Сокращение выражений и их сочетание такое же давнее, как и письмо, поскольку люди всегда учитывали принцип экономии языковых средств. Решение проблем аббревиатуры и ее функционального потенциала уместно изучать на основе политического дискурса, так как он включает у себя большинство сфер человеческой деятельности и отображает современные тенденции развития языка и его составляющих.

Ключевые слова: аббревиатура, лексически-семантический круг, семантическое значение, полисемичный ряд, политический дискурс

Ph.D. Goryacheva K.S.

FUNCTIONAL PETENTIAL OF ABBREVIATION IN ENGLISH POLITICAL SPHERE

A tendency to tongue cost effectiveness being in all systems of language (phonetic, lexical, semantic and grammatical, syntactic) and it appears on the different levels of functioning of language units - sentences, word-combinations, words, morphemes, phonemes

The productive type of lexical compression is abbreviation. Reduction of expressions and their combination are the same old, as well as letter, as people always took into account principle of tongue cost effectiveness. Decision of problems of abbreviation and her functional potential appropriately to study on the basis of political explanation, so as he includes for itself most spheres of human activity and represents modern progress of language and his constituents trends.

Keywords: abbreviation, lexically-semantic circle, semantic value, polysemy row, political abbreviation, lexically-semantic circle, semantic value, polysemy row, political abbreviation, lexically-semantic circle, semantic value, polysemy row, political explanation

УДК 378.013.77 **Грибок А.О.** (КНУ)

СОЦІАЛЬНО-ПСИХОЛОГІЧНІ ОСОБЛИВОСТІ АДАПТАЦІЇ КУРСАНТІВ – УЧАСНИКІВ БОЙОВИХ ДІЙ В РАЙОНІ ПРОВЕДЕННЯ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ, ДО НАВЧАЛЬНОЇ ДІЯЛЬНОСТІ У ВИЩОМУ ВІЙСЬКОВОМУ НАВЧАЛЬНОМУ ЗАКЛАДІ

У статті здійснено аналіз теоретичних основ адаптації курсантів - учасників АТО до навчанні у вищому військовому навчальному закладі та виявлено особливості цього процесу.

Встановлено що процесу адаптації курсантів до навчання притаманні специфічні риси, серед яких – багатоманітність форм поведінки, що вирізняється претензіями на дорослість, особлива чутливість і уразливість, прагнення до групування, нестійкість інтересів та ін.

Розкриваються психолого-педагогічні чинники цієї адаптації, зроблено спробу розробки певних рекомендацій щодо надання курсантам даної категорії допомоги в адаптації до нових умов життєдіяльності.

Зроблено спроба розглянути процес адаптації курсантів АТО до навчання у ВНЗ через діяльність молодіжних організацій, у яких поєднуються колективна, навчальна, пізнавальна, трудова, творча, організаційна та інші види діяльності. Доведено, що існує нагальна потреба збільшення кількості просоціально спрямованих молодіжних (формальних і неформальних) організацій, їх психолого-педагогічного супроводу і суспільного визнання як повноцінного соціального інституту.

Ключові слова: адаптація, реабілітація ,навчальна діяльність, психолого-педагогічні умови, кризові ситуації, соціум,зовнішні умови, дезадаптація, діагностика, самодопомога, тренінг.

Постановка проблеми. У державних документах України з проблем освіти підкреслюється необхідність кардинальної зміни підготовки майбутніх офіцерів з орієнтацією на формування у них всебічної компетентності на основі військово-професійних, державних і національних цінностей, на європейські освітні стандарти, а також формування творчої особистості українського офіцера, здатного самоактуалізуватися та самореалізуватися у військово-професійній діяльності до діяльності в особливих умовах та умовах ризику. Зазначається, що військова освіта, коли Україна знаходиться в умовах військової агресії з боку східного «сусіда», повинна забезпечувати відтворення інтелектуального потенціалу військової галузі та сприяти зміцненню обороноздатності держави відповідно до Конституції та Законів України.

Таким чином, здійснення підготовки військових фахівців у вищих військових та цивільних навчальних закладах, відповідно до сучасних потреб українського суспільства, є важливою науковою проблемою.

Психологи, досліджуючи протягом останніх десятиліть проблему становлення особистості майбутнього фахівця в процесі професійної підготовки, дедалі більше уваги приділяють різним аспектам його психологічної адаптації до умов та вимог навчально-службової діяльності у певному типі навчальних закладів, підготовки до діяльності в особливих умовах та умовах ризику.

Аналіз останніх досліджень і публікацій. Зокрема, у системі вищої військової освіти нині здійснюється активна розробка гуманістичних, особистісно орієнтованих концепцій навчання, які б дозволили всебічно розв’язати проблему адаптації молодих людей до умов навчання у ВВНЗ. Важливим внеском в обґрунтування особистісно орієнтованих підходів до вирішення освітніх проблем у ВНЗ, у тому числі й військових, є дослідження В.А. Баранніка, В.С. Кортлова, П.П. Криворучка, Г.В. Ложкіна, О.П. Макаревича, М.І. Нещадима, В.І. Осьодла, В.В. Рибалки, О.Д. Сафіна, О.В. Симоненка, В.О. Татенка, Г.Д. Темка, В.В. Ягупова та ін. Здебільшого зазначені дослідження присвячені, насамперед, проблемам ефективного управління пізнавальною діяльністю курсантів, формування у них провідних військово-професійних якостей.

Тривають дослідження проблеми адаптації людини до діяльності в особливих та екстремальних умовах (Д.С. Байбаєв, В.І. Воронова, М.І. Дяченко, М.С. Корольчук, Г.В. Ложкін, С.А. Галкін, І.В. Малько, Д.О. Коршевнюк, Б.В. Кравченко, О.П. Макаревич, В.Є. Шевченко та ін.).

Останнім часом, у зв'язку з процесом демократизації українського суспільства, широкомасштабним реформуванням Збройних сил України, адаптацією підготовки військових фахівців до цивільних напрямів підготовки, змінюються умови їх підготовки й, відповідно, істотно змінюються етапи і зміст психологічної адаптації курсантів до умов службово-навчальної діяльності у ВНЗ.

Загалом, процес реформування системи військової освіти пов'язаний із подоланням ***суперечностей***, які мають безпосередній вплив на адаптацію майбутніх офіцерів до навчально-військового середовища. Це суперечності між:

- прагненням курсанта до самостійності та творчості у військово-соціальному середовищі та непідготовленістю до активної життєдіяльності в умовах навчально-службових відносин у цивільному ВНЗ;
- характером статутних вимог, нетиповим соціально-рольовим статусом курсанта і ступенем його підготовленості до їх засвоєння та відтворення у своїй навчально-службовій діяльності, готовності до діяльності в особливих умовах та умовах ризику;
- досвідом відносин і соціальних ролей, що раніше склалися в курсанта, та характером нових для нього взаємостосунків із викладачамиами та однокурсниками;
- закономірностями пізнавальної діяльності курсантів та організацією військово-навчального процесу у цивільному ВНЗ;
- жорсткими, нормативно-статутними вимогами науково-педагогічних працівників і командирів до курсантів та їх пізнавальними можливостями і актуальним рівнем загального, соціально-психологічного, інтелектуального та фізичного розвитку;
- двома взаємно суперечливими сферами життєдіяльності курсанта у військово-соціальному середовищі цивільного ВНЗ: 1) цивільною – навчальною діяльністю у загальному навчальному середовищі та 2) службовою у військовому підрозділі.

Зазначені суперечності зумовлюють необхідність приділення особливої уваги заходам оптимізації психологічної адаптації курсантів - учасників АТО (далі курсантів АТО), до умов навчання у цивільному ВНЗ як важливого етапу їх підготовки до діяльності в особливих умовах та умовах ризику. Подібну оптимізацію можна вважати істотною передумовою ефективної навчальної, навчально-бойової, службової та майбутньої військово-професійної діяльності курсантів, необхідною умовою досягнення ними вершин військової майстерності, особистісного розвитку без відчуття дискомфорту, напруженості та внутрішнього конфлікту з професійним і соціальним оточенням.

Формулювання цілей статті. Російська агресія на сході України поставила перед громадським суспільством та державою чимало складних питань. Одним із таких залишається проблема адаптації воїнів АТО до мирного життя. Проблема адаптації воїнів АТО до мирного життя – це виклик перед українським громадянським суспільством та державою, які виявилися в значній мірі неготовими належним чином забезпечити успішну соціальну інтеграцію бійців АТО. Учасники бойових дій після повернення додому зіштовхуються не тільки з матеріальними проблемами, але й із психологічними. Адаптація військовослужбовців до мирного життя ускладнюється чисельними соціально-психологічними проблемами, а державна система психологічної допомоги військовослужбовцям потребує вдосконалення.

Разом з тим, аналіз наукових праць, пов'язаних із проблемою адаптації майбутніх військових фахівців, показав, що проблема психологічної адаптації курсантів до умов навчально-службової діяльності у ВВНЗ найменш розроблена. Це зумовило вибір теми нашого дослідження " Соціально - психологічні особливості адаптації курсантів учасників бойових дій у районі проведення антитерористичної операції до навчальної діяльності у

вищому військовому навчальному закладі”.

Мета нашої статті – визначити особистісні та соціально-психологічні особливості адаптації курсантів – учасників АТО до навчально-службової діяльності у вищому військовому навчальному закладі, як важливого етапу їх підготовки до діяльності в особливих умовах та умовах ризику, й обґрунтувати психолого-педагогічні засади її оптимізації.

Виклад основного матеріалу. Сучасна молодь характеризуються підвищеною мобільністю, пізнавальною активністю, здатністю в короткий термін формувати в своєму середовищі різні психологічні установки, які певною мірою визначають спрямованість особистості на життя [4].

Сьогодні практика постійно вимагає конкретних досліджень, орієнтованих на адресного споживача відповідних знань, якими у нашому випадку виступають курсанти АТО, молодіжні організації, їхні лідери, викладачі, державні службовці, котрі опікуються проблемами даної категорії військовослужбовців.

Зі вступом до вищого навчального закладу курсанти АТО потрапляють у нові, незвичні для них умови, що неминуче спричиняє ламання динамічного стереотипу і пов'язаних з ним емоційних переживань.

Адаптація розуміється як процес пристосування до змін навколишнього середовища та є однією із важливих загальнотеоретичних проблем і дотепер являє собою традиційний предмет дискусій у психології [5]. Неможливість упоратись із новою життєвою ситуацією спричиняє певні труднощі у навчанні та емоційний дискомфорт.

Сьогодні термін "адаптація" використовується як наукова категорія психології, соціології, педагогіки, антропології та ін. наук.

Соціально-психологічна адаптація курсантів АТО – специфічний і комплексний процес, який представляє цілісну систему та має розглядатися у загальному контексті адаптаційних процесів живих систем, а організація ефективної соціальної адаптації курсантів до умов навчальної діяльності має реалізовуватися через діагностування та корегування їх як суб’єктів діяльності [3].

Нерідко соціально-психологічна дезадаптація породжує втрату сформованих позитивних установок і відносин курсанта АТО зі товаришами по навчанню та викладачами.

Психологічна готовність курсанта АТО до дій часто характеризується з визначеністю цілей, послідовністю, вмінням спрямувати енергію в потрібне русло, цілеспрямованістю. Ці характеристики значно відрізняють курсанта АТО від курсантів, які прийшли до ВВНЗ зі школи.

Багато курсантів повернулися із району проведення антитерористичної операції з величезним багажем психологічних переживань, зміною стилю поведінки до війни, що безпосередньо пов'язано з бойовими рефлексами, які він придбав в результаті небезпечних для життя ситуацій. Що ж тоді робити?

Успішна психологічна адаптація та реабілітація ґрунтується на трьох основних діях: спілкуванні, прийнятті героя таким, яким він є і допомозі фахівця.

Зауважимо, що «студентський вік» (16-24роки) учені розглядають як період індивідуалізації, коли хлопці й дівчата бажають виділити себе серед інших, критично ставляться до суспільних норм поведінки, більш схильні до асоціальних і навіть антисоціальних проявів. Молодь в цей період свого життя негативно реагують на різні зауваження і вимоги. Невдачі різко змінюють їх настрій, у них з’являється почуття провини, тривоги, неповноцінності, зневір’я, безсилля. У цей час вони особливо гостро відчувають будь-яку напругу чи фальш у стосунках з батьками, родичами, викладачами і, як наслідок, шукають спілкування поза звичним колом – сім’ї, університету. Виходячи "на вулицю", юнак хоче бути "своїм" у компанії ровесників або більш старших молодих людей, йому притаманне особливо гостре почуття колективізму ("ми"), тому він шукає і встановлює контакти з різними молодіжно-підлітковими групами, угрупованнями, дитячими і молодіжними організаціями та ін.

Отримуючи позитивний вплив потужного тиску різних людей і обставин на свій розвиток, та передумови для поступового адаптування до навколишньої дійсності юнак, таким чином, набуває досвід. Незаперечний є той факт, що в сучасному молодіжному середовищі відбуваються певні негативні процеси, деформації – коли невиправдано інтенсивно пропагується перевага матеріального над духовним, що призводить до послаблення морально-ціннісних орієнтирів нового покоління [6].

Теоретичний аналіз показав, що у процесі адаптації курсанта АТО до навчання у ВВНЗ необхідно враховувати: *по-перше,* специфічні риси людей, які були в екстремальних умовах пов'язаних з величезним ризиком для життя; *по-друге – те*, що сучасна молодь живе в складному за змістом і тенденціями середовищі соціалізації, він частіше від представників інших вікових груп потерпає від соціальної, економічної, моральної нестабільності й несправедливості, і на цьому тлі закладається фундамент усіх наступних етапів адаптації, що стає основою його реалізації в студентському середовищі; *по-третє – те,* що існують реальні можливості ефективної адаптації курсантів до нових умов навчання в умовах діяльності молодіжних (формальних і неформальних) організацій просоціального спрямування.

Після спроби проведення невеличкого дослідження у формі письмового опитування студентів, які навчаються за програмою підготовки офіцерів запасу, курсантів та курсантів АТО було виявлено конкретні труднощі, які пов'язані з проблемою адаптації курсантів АТО, а саме: фінансові проблеми; труднощі самоорганізації в умовах навчання у ВУЗі; проблеми із засвоєнням певного обсягу навчальної інформації; психологічна неготовність до умов мирного життя; невміння регулювати час, відведений на навчання і відпочинок; соціально-психологічні проблеми спілкування і входження в курсантський (студентський) соціум.

Проблема психологічної адаптації курсантів АТО ускладнюється негативними стереотипами в українському суспільстві щодо консультації психологів. Значна частина курсантів АТО розглядає потребу в психологічній допомозі як ознаку слабкості та вважає, що час усе вилікує. Внаслідок цього вони тримають всі проблеми в собі. Крім того не можна забувати, що психологічної допомоги можуть потребувати родини учасників бойових дій, які також знаходяться у стані постійної нервно-психологічної напруги.

Подолати наслідки психологічних травм не так просто. Військові психологи зазначають, що саму травму подолати неможливо, проте з нею треба навчитися жити.

Після війни курсантам АТО важко повернутися в русло мирного життя. Фізичне повернення додому не завжди збігається із психологічним. Участь у бойових діях може призвести до переорієнтації цінностей. У учасників АТО часто зустрічається порушення соціальної взаємодії та втрата інтересу до суспільного життя, зниження активності, прагнення до соціальної ізольованості. Внаслідок недостатньої уваги суспільства та держави до проблем даної категорії військовослужбовців у них можливе виникнення комплексу жертви та розвиток посттравматичного стресового розладу.

Повертаючись до мирного життя, перш за все повертається лише тіло. Ментально воїн ще перебуває в стані війни. Мається на увазі система цінностей. Уявіть собі, що людина, основним інстинктом якого є виживання, повертається в соціум, цінностями якого є звичайне навчання, виконання вимог військових статутів, духовний та фізичний розвиток. Для воїна це неважливо, й соціум його не сприймає. Тому воїнам АТО часто здається, що вони ненормальні. Хоча все, що з ними відбувається, – це адекватні реакції. Від цих «нестиковок» потерпають як самі воїни АТО, так і близьке оточення, якщо й ті, й інші не підготовлені до такого розвитку подій.

У світовому стандарті є поняття «соціально-психологічна адаптація», а не реабілітація. Бо реабілітація – це відновлення. Ми розуміємо, що курсант АТО таким, як був, вже не стане. І це нормально.

Ми пропонуємо впровадити в життя курсантських підрозділів програму адаптації курсантів АТО до мирного життя та навчання у ВВНЗ через розвиток ***груп самодопомоги***, які сподіваємось допоможуть нашим героям. Ця програма повинна передбачати інтеграцію

курсантів АТО в суспільство не зі штучними цінностями, а зі своїми – справжніми. Перша хвиля демобілізації відбулася у 2015 році. З'явилися ветерани з річним досвідом інтеграції в суспільство. Вони готові віддавати свій досвід тим, хто цього потребує. Між учасниками АТО високий рівень довіри один до одного. Більш, ніж до чиновників та психологів.

Сприяння адаптації курсантів АТО до мирного життя та навчання у вищі має супроводжуватися комплексом заходів, які повинні включати соціальну, економічну складову. Поєднання всіх цих аспектів допомагатиме успішній соціальній інтеграції курсантів АТО.

З метою визначення типових соціальних проблем, які мають місце у курсантському середовищі, нами було класифіковано необхідну соціальну допомогу від соціальної служби ВВНЗ: налагодження взаємодії курсантів і викладачів – 48%; надання соціально-психологічної допомоги курсантам АТО-першокурсникам – 64%; організація змістовного дозвілля – 89%; створення умов для самореалізації та саморозвитку – 48%.

Зазначене дослідження дозволило з'ясувати особливості досліджуваних адаптаційних процесів та намітити головні шляхи їх оптимізації.

Аналіз результатів опитування вказує на слабку ефективність спроб оптимізації адаптивних здібностей курсантів АТО, особливо першого року навчання, на наявні недоліки, на основі яких визначаються шляхи оптимізації.

Ключові соціально-психологічні проблеми адаптації курсантів АТО до навчання в університеті за даними дослідження:

1. Фінансові проблеми та проблеми адаптації до умов життя в незнайомому місті, гуртожитку, налагодження взаємин з товаришами по кімнаті, матеріальні та побутові проблеми.
2. Невміння регулювати час, відведений на навчання і відпочинок.
3. Низький рівень навичок самоорганізації, самоконтролю та саморегуляції поведінки під час навчального процесу в умовах великого навчального навантаження.
4. Невміння курсанта АТО (внаслідок відсутності досвіду) результативно себе презентувати на семінарських заняттях.
5. Відсутність або недостатня розвінутість навичок самостійної роботи під час підготовки до семінарських занять та іспитів.
6. Виникнення проблемних ситуацій в навчальній групі під час підготовки та проведення семінарських занять, підґрунтям чого є розподіл навчальних питань перед семінаром та боротьба за кількість балів під час його проведення, що супроводжується напруженістю стосунків у курсантському середовищі.

У результаті проведення численних діагностичних процедур (бесіда, анкетування, спостереження) було виокремлено кілька груп проблем, що виникають.

Перша група має доволі опосередковане відношення до психології, але є суттєвою і стосується великого числа курсантів. Мається на увазі відсутність у курсантів АТО - першокурсників багатьох спеціальних організаційно-навчальних навичок, необхідних у вузівському навчанні: конспектування лекцій та першоджерел, користування бібліотекою тощо. Зазвичай, подібні вміння й навички дуже швидко набуваються, але зафіксовано негативний вплив їхньої відсутності на успішність навчання і на цілісні показники адаптації курсантів АТО.

До цієї ж групи слід віднести відсутність адекватних комунікативних навичок. Перш за все, це особливості спілкування курсантів АТО з викладачами. Відомо, що цей процес дуже відрізняється від взаємодії зі командирами та підлеглими під час знаходження в районі проведення АТО, і спроби курсантів АТО "перенести" фронтовий стиль спілкування у вузівське життя, як правило, є неефективними і досить конфліктними. Слід зазначити, що в цілому ці проблеми досить легко коригуються, але, як не дивно, часто вони зберігаються тривалий час і серйозно впливають на успішність навчання курсантів АТО.

Друга група проблем стосується функціонування вищих психічних процесів. Перш за все, це довільність та опосередкованість пізнавальних процесів та емоційної сфери. Часто виявляється, що способи зосередження уваги, запам'ятовування, вирішення навчальних

завдань, якими володіє курсантів АТО і які були цілком адекватними в умовах бойового вишколу, не "працюють" у навчанні вузівському. Те саме стосується управління увагою, розподілу активності у часі, керівництва емоційною сферою.

Третю групу становлять власне особистісні труднощі курсантів АТО. Серед них найсуттєвішою є проблема недостатнього самовизначення. З літератури відомо, що готовність до життєвого самовизначення є центральним психічним новоутворенням молоді. Основними психологічними компонентами цієї структури є: життєві плани як стійкий вияв мотивації особистості відносно визначеного напряму життєвого шляху.

Адаптація – це зміна самого себе (настанов, рис характеру, стереотипів поведінки тощо) відповідно до нових вимог діяльності, соціальних умов і нового оточення [1]. Це входження в нову соціальну позицію і нову систему взаємин. Психологічна адаптація пов'язана з прийняттям курсантом АТО нової соціальної позиції й опануванням нової соціальної ролі «студента» (студент – той, хто навчається самостійно, наполегливо опановує професію) і «майбутнього фахівця». Наявність в «Я-концепції» курсанта (студента) конструктів, які вказують на його професійно-рольову ідентифікацією («Я – студент», «Я – майбутній фахівець» тощо) позитивно позначається на процесі його професійного становлення. «Я-концепція» курсанта (студента), його самооцінка безпосередньо впливає як на його дидактичну адаптацію, так і на адаптацію до умов майбутньої професійної діяльності [6].

Чинники ефективної адаптації курсанта АТО до навчання у вищому військовому навчальному закладі:

- здатність навчатися самостійно;
- уміння контролювати й оцінювати себе;
- врахування індивідуальних особливостей власної пізнавальної діяльності;
- уміння правильно розподіляти свій час для самостійної навчальної підготовки й відпочинку;
- самодисципліна.

Психодіагностика адаптаційних можливостей курсантів АТО першого року навчання дуже важлива, тому що дезадаптація може позначитися погіршенням роботи пізнавальної сфери (зосередження уваги, пам'яті, мовлення), змінами в емоційно-почуттєвій сфері (поява тривоги, поганого настрою, невпевненості у собі, страху). Кризові ситуації студентського віку, особливо залежність курсанта АТО від матеріального та фінансового стану, уявляють загрозу всієї системі соціально-психологічної адаптації курсантів АТО до навчання у вищому навчальному закладі [12].

Дослідники вважають, що соціально-психологічна робота зі курсантами – учасниками бойових дій в сучасних умовах має свої особливості: адаптація курсанта АТО до умов функціонування вищого навчального закладу (особливо це стосується першокурсника); корекція (захист) відносин між викладацьким складом та курсантом АТО, який навчається; попередження можливих фізичних, психічних і соціокультурних зіткнень окремого індивіду і груп ризику; розвиток курсанта АТО як неповторної особистості, формування якості творчого професіонала через процес навчання, виховання, соціалізації [9].

Особливо великий виховний і соціалізуючий потенціал щодо стимулювання до суспільної активності й розвитку курсанта АТО, його особистісних якостей закладено у діяльності молодіжних організацій. Проте, сьогодні розгорнули свою діяльність не тільки суспільно корисні (просоціальні) молодіжні організації, а й такі організації (об'єднання, групи, угруповання), які мають асоціальне і антисоціальне спрямування, що зазвичай негативно впливає на процес соціалізації курсантів АТО та є серйозною соціально-педагогічною проблемою. У цьому зв'язку існує нагальна потреба педагогічного осмислення діяльності різних молодіжних організацій як соціально-педагогічного механізму соціалізації учасників бойових дій.

Практичні рекомендації командирам курсантських підрозділів та науково-педагогічним працівникам ВНЗ.

1. Приготуйтеся, що курсант АТО, який повернувся із зони бойових дій, – це вже інша людина, яка отримала унікальний досвід. Його потрібно прийняти разом з новими поглядами, знайомствами, проблемами, страхами і, можливо, проявами агресії.

2. Пам'ятайте: людина, що пройшла війну, стала набагато більш сильнішою, мудрішою і досвідченішою. Він повернувся ЖИВИМ. Повернувся саме до вас. Все інше – труднощі, які можна пережити, якщо ви націлені на те, щоб курсант АТО успішно навчався й отримав від цього задоволення.

3. Не відгороджуйтеся. В іншому випадку курсант АТО залишається сам на сам зі своїми спогадами, які часом є небезпечними для психічного здоров'я. Це призводить до внутрішнього конфлікту, який буде поступово посилюватися. У підсумку виходів з нього може виявитися багато і всі вони будуть деструктивні для особистості і соціуму.

4. Слухайте його. Це важливо. Курсант АТО повинен зрозуміти, що поруч з ним людина, яка прийме його будь-яким. Він повинен зрозуміти, що він потрібен.

5. Забороніть собі ображатися. Не можна не будувати здогади "... він зі мною не говорить, тому що ...". Не можна ставити себе в роль жертви. Людина була в ситуації, де все по-справжньому. У зоні бойових дій немає тієї дипломатії, до якої ми звикли у повсякденному житті – там щось не скажи, тут посміхнися, умовності збережи, так себе не поведи. Курсант АТО налаштований категорично, він так звик. Через це можуть виникати конфлікти.

6. Щоб курсант АТО швидше адаптувався, його потрібно залучати у повсякденне життя. Він повинен розуміти, що він потрібен підрозділу і не є тягарем. В іншому випадку, у свідомості курсантів АТО виникає розлом – там він герой, а тут не зрозуміло що. Ні в якому разі не можна жаліти людину, потрібно залучати її до абсолютно всіх питань по мірі готовності.

7. Якщо людині починають снитися кошмари – зверніться до психотерапевта або психолога. Вони допоможуть створити комфортні умови, які сприятимуть усвідомленню безпеки. Приклад: курсант АТО повернувся з війни без видимих фізичних ушкоджень. Однак, коли вимикається світло у кімнаті гуртожитку і всі лягають спати, йому здавалося, що поруч сепаратист, який може його задушити. Він починав захищатися. Ситуацію врятувала порада психолога залишати включеним нічник. Людина прокидається від кошмару, дивиться по сторонах, бачить, що вона у безпеці, життю нічого не загрожує, жодних сепаратистів немає – поруч сплять товариші, з якими він навчається.

8. Буває, що людина, яка повернулася із зони бойових дій, довго мовчить, але в якийсь момент зривається і починає трощити все навколо. У таких ситуаціях потрібно максимально намагатися прибрати всі колючо-ріжучі предмети, щоб вони не потрапили під руку.

9. При проявах агресії на словах – намагайтеся говорити з людиною спокійно. Буде дуже складно, тому що всередині все закипить, але піддаватися на цю агресію не можна. Потрібно своєю поведінкою, інтонацією і реакцією давати зрозуміти, що ви усвідомлювати, як йому важко. Або що вам складно це зрозуміти, але від того, що на вас кричать, зрозуміліше не стає.

10. Якщо ви бачите, що курсант АТО починає заводитися – постарайтеся заручитися підтримкою друзів, які знаходяться поруч, і вивести людину із зони ризику. Якщо в компанії з'являється людина, яка може спровокувати курсанта АТО на конфлікт (це завжди помітно), потрібно зробити все можливе, щоб уникнути такої ситуації.

11. Якщо прояви агресії супроводжуються зловживанням алкоголю – потрібно негайно звертатися до фахівців. Тому що спиртне гарантує непередбачуваність у будь-якому стані.

12. Якщо курсант АТО скаржиться на болі в спині пройдіть дослідження – носіння бронежилета і переміщення на бронетехніці тривалий час може стати причиною проблем з хребтом. Якщо не знайдені якісь фізичні проблеми в ході дослідження, то травма є психосоматичною. З нею теж потрібно звертатися до фахівців. Потрібні розслаблюючі масажі, фізіотерапевтичні процедури, плавання, гімнастика.

13. Якщо курсант АТО не хоче звертатися до психолога або психотерапевта, хоча ви бачите, що йому потрібна допомога, то фахівець повинен прийти до нього. Можна змоделювати

ситуацію, коли у вашому колі спілкування з'являється людина, що встановить довірчі взаємовідносини з курсантом АТО і допоможе йому усвідомити деякі моменти в його поведінці.

14. Поясніть, що психолог – це не людина-енциклопедія. Психолог – це людина яка працює зі здоровими людьми, що потрапили у складні ситуації.

15. Якщо людина не хоче йти до психолога, але готова йти на сповідь до духівника – йдіть до церкви. В окопах атеїстів немає.

Загальні поради курсантам АТО щодо адаптації до навчання у ВВНЗ

1. Не очікуйте опіки, а розраховуйте на дружню підтримку оточуючих, яка надасть Вам відчуття рівності, потрібності та незалежності.
2. Не уникайте тих, хто готовий прийти Вам на допомогу, але не допускайте зайвої опіки, намагайтесь стати самостійним.
3. Прагніть виконувати посильну і цікаву роботу, підтримуйте охайність і порядок на робочому місці.
4. Активніше добивайтесь отримання потрібної Вам інформації та нових знань.
5. Не створюйте емоційну напругу у відносинах із одногрупниками, намагайтесь завжди бути приязним і доброзичливим.
6. Змістовно проводьте свій вільний час із іншими студентами, набувайте хороших друзів.
7. Будьте оптимістом, вірте у свої можливості і пам'ятайте, що Ви потрібні іншим людям.
8. Сміливіше відповідайте на запитання, беріть участь в обговоренні - це допоможе Вам пов'язати нову інформацію з тим, що Ви вже знаєте.

Практичні рекомендації курсантам АТО першого року навчання

1. Не порушувати норм та правил поведінки.
2. Брати активну участь у заходах, які проводяться в навчальному закладі.
3. Виконувати рекомендації викладачів щодо навчання, намагатись досягти нових та корисних знань.
4. Співпрацювати з групою та завжди підтримувати один одного, поважати думку оточуючих.
5. Стримувати негативні емоції, бути впевненим у собі і своїх діях.
6. Не відмовляти у допомозі тим, хто цього потребує.
7. Бути цілеспрямованим, ставити перед собою чітку мету та досягати її.
8. Співпрацювати з викладачами та студентами, регулярно відвідувати заняття.
9. Концентрувати свою увагу на навчанні, вдосконалювати свої знання.
10. Не боятись пробувати щось нове для себе, відповідати на семінарських заняттях.
11. Радіти кожному дню, проведеному у ВВНЗ, адже цей період – неповторний!

Якщо у Вас виникли проблеми у навчанні:

Вам слід: дати викладачу можливість допомогти Вам; залучити викладача до процесу розв'язання проблеми, якщо немає конкретного способу її розв'язання без його участі; впевнено відстоювати свою точку зору, але з повагою і ввічливо ставитись до викладача; звернути увагу викладача на позитивні моменти, на те, що Ви засвоїли на його лекціях, а не жалітися на свої проблеми; зрозуміти, що викладач більше зацікавлений в успішності Вашого навчання, аніж у виставленні поганої оцінки. Ваше бажання вчитись є найкращим стимулом для отримання допомоги від викладача.

Вам не слід: публічно висловлювати свою розлюченість, різку незгоду, ні в якому разі не тисніть на викладача; благати викладача про зниження вимог; зловживати виразом: «Ви зобов'язані...»; висловлювати нерозумні або занадто обтяжливі прохання; висувати вимоги до викладача щодо додаткового використання його часу.

Висновки.

1. Аналіз наукової літератури засвідчив, що поняття "адаптація" розглядається вченими як складне багатоаспектне соціальне явище, специфіка якого відображається через різні соціальні умови та багатоманітність його змістовних і процесуальних сторін.
2. Теоретичний аналіз наукових джерел дозволяє стверджувати, що психологічна

готовність курсантів АТО до нової діяльності часто стикається з невизначеністю цілей, недостатністю життєвого досвіду, непослідовністю, невмінням направити енергію в потрібне русло. Така неузгодженість викликає багато проблем соціально-психологічного плану, а стихійна адаптація, яка є найбільш властивою, негативно впливає на розвиток і становлення першокурсника.

3. Процес адаптації курсантів АТО до навчання у ВНЗ через діяльність молодіжних організацій може бути адекватно зрозумілим тільки на основі вивчення загальносоціалізаційного процесу і притаманних студентській молоді специфічних рис, він буде більш успішним за умови залучення їх до діяльності в різних молодіжних об'єднаннях, у яких поєднуються колективна, навчальна, пізнавальна, трудова, творча, організаційна та інші види діяльності.

Зазначене дозволяє стверджувати, що існує нагальна потреба збільшення кількості просоціально спрямованих молодіжних (формальних і неформальних) організацій, їх психолого-педагогічного супроводу і суспільного визнання як повноцінного соціального інституту. На підставі означених позицій доцільно розробити психолого-педагогічні рекомендацій що підвищать ефективність процесу адаптації курсантів АТО шляхом залучення їх до діяльності молодіжних організацій.

4. Соціальна адаптація курсантів АТО першого року навчання до навчання у ВВНЗ та надання загальної, ситуативної та особистісної психологічної допомоги в сучасних умовах є одним із провідних напрямів діяльності соціальної служби вищого навчального закладу, яка на сьогодні має певні проблеми, що потребують вирішення. Аналіз результатів дослідження свідчить про слабку ефективність оптимізації адаптивних здібностей курсантів АТО першого року навчання, та виявляє недоліки, на основі яких можна визначати шляхи покращення роботи соціальної служби вищого навчального закладу.

ЛІТЕРАТУРА:

1. Андреева Д. А. О понятии адаптации // Человек и общество. – Л., 1983. – С. 64-67.

2. Адаптация организма подростков к учебной нагрузке / [Под ред. Д.В. Колесова.] – М: Педагогика, 1987. – С. 84-115.

3. Алексєєва Т.В. Психологічні фактори та прояви процесу адаптації студентів до навчання у вищому навчальному закладі: автореф. дис. на здобуття наук. ступеня канд. психол. наук / Т.В. Алексєєва. – К.: Київський національний університет імені Тараса Шевченка, 2004. – С.22.

4. Бибрих Р.Р. Мотивационные аспекты адаптации студентов к учебному процессу в вузе / Р.Р. Бибрих / [Психолого-педагогические аспекты адаптации студентов к учебному процессу в вузе]. – Кишинев: изд-во Кишинев, 1990. – С.17-27.

5. Бохонкова Ю.А. Особенности социальной адаптации студентов к условиям ВУЗа / Ю.А. Бохонкова // Психолого-педагогічні проблеми розвитку сучасних освітніх технологій. – Луганськ: Вид-во СНУ, 2004. – С. 45–48.

6. Ворожбит С.А. Вплив особливостей інтелекту на процес успішної адаптації студентів до університету / С.А. Ворожбит // Проблеми загальної та педагогічної психології. – 2006. – Т. 8. – Вип. 7. – С. 74–79.

7. Зеер Э.Ф. Кризисы профессионального становления личности / Э.Ф. Зеер, Э.Э. Сыманюк // Психологический журнал. – 1997.– С. 57–79.

8. Кокун О.М. Аналіз поняття адаптаційних можливостей людини // Проблеми загальної та педагогічної психології: Зб. наук. праць Ін-ту психології імені Г.С. Костюка АПН України / За ред. С.Д. Максименка. – К.: ГНОЗІС, 2002. – Т. IV. – Ч. 5. – С. 137-140.

9. Рудакова С. Г. Психолого-педагогическое сопровождение адаптации студентов в ВУЗе: автореф. дис..канд. пед. наук. – Биробиджан, 2005. – С. 23–32.

10. Сластьонін В. А., Подымова Л. С. Педагогика: инновационная деятельность. – М. : 1997. – С. 285–289.

11. Слободчиков И. М. Переживание одиночества к контексту проблем психологической адаптации студентов психолого-педагогических вузов // Психологическая наука и образование. 2005.– С. 281–288.

12. Семиченко В.А. Психические состояния: Модульный курс для преподавателей и

студентов. – К.: Магістр-S, 1998. – С. 207.
13. Татенко В.А. Психология в субъективном измерении. – К.: Просвіта, 1996. – С. 403.
14. Ягупов В.В. Військова й соціальна психологія: Навч. посіб. – К., 1998. – С. 400.
15. Ягупов В.В. Військова й соціальна психологія: Навч. посіб. – К., 2000. – С. 522.
16. Ягупов В.В. Військова психологія: Підручник. - К.: Тандем, 2004. – С.656.
17. Яценко Т.С. Психологічні основи групової психокорекції: Навч. посібник.– К.:Либідь,1996.–С. 264.

REFERENCES:

1. Andreeva D.A. O concept of adaptation // Man and society. - L., 1983. 64-67 p.
2. Adaptation organism for teenagers uchebnoy load / [Ed. D.V. Kolesov.] - Moscow: Pedagogika, 1987. 84-115 p.
3. Alekseeva T.V. Psychological factors and symptoms of the process of adaptation of students to training in high school: Author. Dis. on competition sciences. degree candidate. Psychology. Science / TV Alekseev. – K.: Taras Shevchenko National University of Kyiv, 2004. 22 p
4. R.R. Bybryh Motyvatsyonnыe aspects studentov for uchebnomu adaptation process in vuze / R.R. Bybryh / [Psychological-Pedagogical aspects for uchebnomu studentov adaptation process in vuze]. - Chisinau: Publishing House Chisinau, 1990.17-27 p.
5. Bohonkova Y.A. Features sotsyalnoy adaptation studentov terms for high school / YA Bohonkova // Psycho-pedagogical problems of modern educational technologies. - Lugansk: Izd Dreams, 2004. 45-48 p.
6. Vorozhbit S.A. Impact features intelligence to the process of successful adaptation to university students / S.A. Vorozhbit // Problems of general and educational psychology. - 2006 - Vol 8 - Vol. 7. 74-79 p
7. Zeer Э.F. Kryzysы PROFESSIONAL Formation of personality / Э.F. Zeer, Э.Э. Simanyuk, psychological journal. - 1997.57-79 p.
8. Kokun A.M. Analysis of the concept of adaptive human capabilities // Problems of General and Educational Psychology: Coll. Science. works Inst of Psychology behalf G.S. Kostyuk APS of Ukraine / Ed. S.D. Maksimenko. - K .: Gnosis, 2002. - T. IV. - Part 5.137-140 p.
9. Rudakova S.G. psycho-pedagogical adaptation soprovozhdenye student dentov in VUZe: Author. dys..kand. ped. Science. - Birobidzhan, 2005. 23-32 p.
10. Slastonin V.A. Podыmova L. Pedagogika: ynnovatsyonnaya activities. - M., 1997. 285-289 p.
11. Slobodchikov I.M. Perezhyvanye loneliness context for problems psyholohycheskoy adaptation studentov psycho-pedagogical high schools // Psyholohycheskaya science and education. 2005. 281-288 p.
12. Semychenko V.A. Psyhycheskye STATUS: Modulnыy Lecturer and course for students. - K .: Master-S, 1998. 207 p.
13. Tatenko V.A. Psychology in subjective measurements. - K.: Education, 1996. 403 p.
14. Yagoupov V.V. Military and Social Psychology: Training. guidances. - K., 1998. 400 p.
15. Yagoupov V.V. Military and Social Psychology: Training. guidances. - K., 2000. 522 p.
16. Yagoupov V.V. Military Psychology: Textbook. - K .: Tandem, 2004.- 656 p.
17. Yatsenko T.S. Psychological foundations of group correction: Training. manual. - K .: Lybid,1996. 264 p.

Рецензент: к.т.н., доц. Пампуха І.В., начальник відділу – заступник начальника науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка

Грибок А.А.

СОЦІАЛЬНО-ПСИХОЛОГИЧЕСКИЕ ОСОБЕННОСТИ АДАПТАЦІЇ КУРСАНТОВ – УЧАСТНИКОВ БОЕВЫХ ДЕЙСТВИЙ В РАЙОНЕ ПРОВЕДЕНИЯ АНТИТЕРОРИСТИЧЕСКОЙ ОПЕРАЦИИ, К УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ В ВИСШЕМ ВОЕННОМ УЧЕБНОМ ЗАВЕДЕНИИ

В статье проведен анализ теоретических основ адаптации курсантов - участников АТО к учебе в высшем военном учебном заведении и выявлены особенности этого процесса.

Установлено, что процесс адаптации курсантов к обучению присущи специфические черты, среди которых - многообразие форм поведения, которые отмечаются претензиями на взрослость, особую чувствительность и уязвимость, стремлением к группированию, неустойчивостью интересов и др.

Раскрываются психолого-педагогические факторы этой адаптации, сделана попытка разработки определенных рекомендаций о предоставлении курсантам данной категории помощи в адаптации к новым условиям жизнедеятельности.

Сделана попытка рассмотреть процесс адаптации курсантов АТО к обучению в ВУЗе через деятельность молодёжных организаций, в которых сочетаются коллективная, учебная, познавательная, трудовая, творческая, организационная и другие виды деятельности. Доказано, что существует насущная необходимость увеличения количества социально направленных молодежных (формальных и неформальных) организаций, их психолого-педагогического сопровождения и общественного признания в качестве полноценного социального института.

Ключевые слова: адаптация, реабилитация, учебная деятельность, психолого-педагогические условия, кризисные ситуации, социум, внешние условия, дезадаптация, диагностика, самопомощь, тренинг.

Hrybok A.A.

PECULIARITIES OF SOCIAL AND PSYCHOLOGICAL ADAPTATION OF THE CADETS-PARTICIPANTS OF THE ANTI-TERRORIST OPERATION TO LEARNING ACTIVITY AT HIGHER MILITARY EDUCATIONAL INSTITUTIONS

The article analyzes theoretical basics of adaptation of the cadets-participants of the Anti-terrorist operation (ATO) to learning activity at higher military educational institutions as well as the peculiarities of this process.

It was established that the process of cadets adaptation to learning activity is characterized by some specific features, among them – the variety of behavior types with openly demonstrated claims for adulthood, particular sensitivity and vulnerability, desire to bond or form groups, volatility of interest, etc.

The paper reveals psychoeducational factors of adaptation and proposes specific recommendations for providing such cadets with the help they need in order to adapt to the new conditions of life.

An attempt was made to consider the process of adaptation of the cadets-participants of the ATO to learning activity through multiple youth organizations, which combine collective, educational, cognitive, labor, creative, organizational and other activities. It was proved that there is an urgent need to increase the number of socially oriented (both formal and informal) youth organizations, their psychological and pedagogical support and publicly recognize them as a full-fledged social institution.

Keywords: adaptation, rehabilitation, learning activities, psychological and pedagogical conditions, critical situations, society, external conditions, disadaptation, diagnostics, self-helpō training.

УДК 024-056.26

Гуменна О.І. (Хм.СЗОШ № 15)
к.т.н., доц. **Муляр І.В.** (ХмНУ)
Ряба Л.О. (ВІКНУ)

ДОСТУПНИЙ БІБЛІОТЕЧНИЙ ПРОСТІР ДЛЯ КОРИСТУВАЧІВ З ОБМЕЖЕНИМИ МОЖЛИВОСТЯМИ

У статті розглядається потреба в створенні рівних можливостей доступу до знань, інформації і художніх творів шляхом використання ряду ресурсів і служб в рівній мірі всім членам суспільства, незалежно від ступеня працездатності, релігійних, етнічних особливостей. Фізичні дефекти, відсутність мобільності людей з обмеженими можливостями здоров'я не дають вільного доступу до інформації. Висвітлення проблем бібліотечно-інформаційного обслуговування, що допомагають людям з обмеженими фізичними можливостями отримати інформацію, щоб не бути ізольованими від соціально-культурного життя суспільства. Завдання бібліотек полягає в тому, щоб зруйнувати бар'єри і зробити інформацію найбільш доступною і повноцінною для різних груп таких категорій громадян. При всій складності вирішення завдань по соціальному захисту людей з особливими потребами слід залучити їх до книги, до бібліотеки. Це є безперечною умовою їх повноцінної соціальної реабілітації. Бібліотеки повинні робити все для того, щоб ресурси їх книгозбірень стали доступнішими для всіх категорій користувачів.

Ключові слова: бібліотечно-інформаційне обслуговування; бібліотечні послуги; люди з обмеженими можливостями.

Вступ. Ми увійшли в нове тисячоліття, яке може і повинно відрізнятися від попередніх створенням умов для повноцінного життя та розвитку усіх членів суспільства, в тому числі, людей з особливими потребами, і сучасна бібліотека повинна взяти участь у процесі інтеграції цих людей у суспільство.

Не всіх людей доля наділила здоров'ям в рівній мірі. Живуть серед нас прекрасні люди, здібні і талановиті, але з обмеженими фізичними можливостями. Їх називають інвалідами, а вони просто по-іншому дивляться на світ, у них інша шкала духовних цінностей. Вони вміють радіти кожному сонячному дню.

Понад 500 мільйонів людей у світі є інвалідами в результаті розумових, фізичних чи сенсорних розладів. Серед них – близько 3 мільйони мешканців України, серед них великий відсоток учасників АТО, які постраждали під час антитерористичної операції.

У цивілізованих країнах осіб з різними інтелектуальними та фізичними відхиленнями називають *«люди з особливими потребами»*, а не *«інваліди»* - як досі прийнято у нас.

Не секрет, що в нашому суспільстві по-різному ставляться до людей з особливими потребами. Це варіюється від розуміння, жалю, співчуття, бажання допомогти – до неприйняття і байдужості.

Толерантне ставлення до всіх соціальних груп населення у багатьох країнах визначається гаслом: *«Усі люди рівні»*.

Постановка проблеми. У цій статті йдеться про те, що люди з особливими потребами в Україні мають дуже обмежений доступ до інформації. Бібліотечна громадськість, керуючись гуманістичними прагненнями, веде пошук шляхів щодо зміни ситуації на краще.

Основна мета бібліотеки - забезпечення доступу до знань, інформації і художніх творів шляхом використання ряду ресурсів і служб в рівній мірі всім членам суспільства, незалежно від ступеня працездатності, релігійних, етнічних особливостей. Фізичні дефекти, відсутність мобільності людей з обмеженими можливостями здоров'я не дають вільного доступу до інформації. Отже, завдання бібліотек полягає в тому, щоб зруйнувати бар'єри і зробити інформацію найбільш доступною і повноцінною для різних груп таких категорій громадян.

Виклад основного матеріалу. Безперечною цінністю і показником високого рівня розвитку цивілізованого суспільства є забезпечення рівних можливостей людей. Термін "забезпечення рівних можливостей" означає процес, завдяки якому різні системи суспільства

і довкілля (як обслуговування, трудова діяльність та інформація) є доступними для всіх. Принцип рівності прав передбачає, що потреби всіх без винятку індивідуумів мають однаково важливе значення, що ці потреби повинні служити основою планування в суспільстві; кожному індивідууму потрібно забезпечити рівні можливості для участі в житті суспільства. Сьогодні понад 500 млн осіб у світі мають особливі потреби і через розумові, фізичні або сенсорні розлади. Їм потрібно забезпечити ті самі права і можливості, що й іншим людям. Досвід показує, що саме середовище значною мірою визначає вплив дефекту або інвалідності на повсякденне життя людини. Позбавлена можливостей, зазвичай доступних у суспільстві і необхідних з точки зору основних елементів життя в межах звичайних систем охорони здоров'я, освіти, зайнятості і соціальних послуг, вона відчуває дискомфорт. Однією з обов'язкових умов повноцінної інтеграції людей з особливими потребами в інформаційне суспільство є наявність ефективного бібліотечного обслуговування. Ця проблематика є предметом активних наукових досліджень з 60-х років минулого століття.

Люди з особливими потребами в Україні мають дуже обмежений доступ до інформації. Свої можливості найповніше вони можуть реалізувати у великих містах і, у поодиноких випадках, через власні комп'ютери, підключені до інтернету. Це свідчення несправедливого ставлення суспільства до інвалідів й існування бар'єру для їхньої соціальної активності. Бібліотечна громадськість, керуючись гуманістичними прагненнями, веде пошук шляхів щодо зміни ситуації на краще.

Основна місія кожної бібліотеки – забезпечення доступу до знань, інформації і художніх творів шляхом використання ряду ресурсів і служб в рівній мірі всім членам суспільства, незалежно від ступеня працездатності, релігійних, етнічних особливостей. Фізичні дефекти, відсутність мобільності людей з обмеженими можливостями здоров'я не дають вільного доступу до інформації. Отже, завдання бібліотек полягає в тому, щоб зруйнувати бар'єри і зробити інформацію найбільш доступною і повноцінною для різних груп таких категорій громадян.

Обслуговування людей з обмеженими можливостями, допомога їм у соціальному становленні і соціальній адаптації, поглиблення та розширення знань, підвищення культурного рівня, залучення до спілкування, організація їхнього дозвілля – один із пріоритетних напрямків діяльності бібліотек.

Пріоритетними напрямками роботи бібліотек з користувачами з обмеженнями на сучасному етапі мають стати: соціальний, інформаційний, психологічний, дозвіллєвий, професійно-реабілітаційний.

Ефективній роботі сприятиме координація діяльності бібліотек з органами місцевої влади, державними і громадськими організаціями, соціальними, юридичними, психологічними службами, центрами реабілітації, методичними та навчальними закладами, спортивними товариствами, молодіжними організаціями, товариством Червоного Хреста, тощо.

Проблемами бібліотечно-інформаційного обслуговування, які є причиною обмеження права людей з обмеженими фізичними можливостями на отримання інформації, їх ізоляції від соціально-культурного життя суспільства є :

- відсутність належної координації у роботі місцевих органів державної влади, місцевого самоврядування, бібліотек, громадських організацій інвалідів;
- непристосованість життєвого середовища, бібліотечних закладів для пересування та обслуговування людей з захворюваннями опорно-рухового апарату;
- відсутність спеціальної комп'ютерної техніки, спеціального обладнання для людей з вадами руху, зору, слуху;
- дефіцит у бібліотеках видань у спеціальних форматах для людей з обмеженими можливостями в отриманні інформації;

• відсутність пристосованого транспорту для інформаційно-бібліотечного обслуговування на дому, доставки людей з обмеженими фізичними можливостями до бібліотек.

Вивчення стану бібліотечно – інформаційного обслуговування людей з фізичними обмеженнями показало, що в наш час для більшості з них накопичений в країні інформаційний потенціал є недосяжним. Одна з причин цього полягає в тому, що бібліотеки орієнтовані в основному на роботу із здоровими людьми і не враховують потреб та особливостей осіб з функціональними можливостями.

При всій складності вирішення завдань по соціальному захисту людей з особливими потребами залучення до книги, до бібліотеки є безперечною умовою їх повноцінної соціальної реабілітації. Бібліотеки повинні робити все для того, щоб ресурси їх книгозбірень стали доступнішими для всіх категорій користувачів.

На бібліотекаря, який працює з такими користувачами, лягає висока моральна і психологічна відповідальність. Дуже важливо не лише принести необхідну книгу, а й підтримати бесіду, виявити не жалість, а розуміння, терпіння, адже ці люди позбавлені спілкування з ровесниками, не мають можливості проявити свій творчий потенціал та здібності.

Люди з особливими потребами навчаються все життя. І на їх шляху існують труднощі. Через свої індивідуальні особливості і фізичні вади їм складно приходити до бібліотеки. Тому будь-який вихід у бібліотеку – це вікно у світ книги. Нові враження, нові інтелектуальні можливості. Свій внесок у подоланні цих труднощів можуть зробити бібліотеки. Істина, яка підтверджується з все більшою повнотою, і складає основний сенс життя *«Хто володіє інформацією – володіє світом».*

Якщо таких людей залучати до участі у конкурсах, виставках, вікторинах, концертах, презентаціях книжкових виставок, бібліотечних вечорах, засіданнях клубів з інтересами, то можна на прикладах набути досвіду роботи з людьми з особливими потребами.

Роботу бібліотек необхідно проводити за такими напрямками:

• організація роботи щодо створення регіональної бази даних з фізичними обмеженнями, які потребують інформаційно-бібліотечного обслуговування;

• збір інформації в регіоні щодо людей з фізичними обмеженнями, шляхом опитування (анкетування) серед читачів родини, де є членами особи з обмеженнями, з'ясувати їх інформаційні потреби;

• проведення інструктажу, навчання персоналу бібліотеки;

• комплектування бібліотечного фонду виданнями у спеціальних форматах (аудіо книги, книги зі шрифтом Брайля, друк великими літерами тощо), а також електронними програмами звукового супроводу друкованої інформації;

• обладнання спеціальних комп'ютеризованих робочих місць користувачів;

• створення інформаційних куточків, тематичних виставок, полиць, прес – досьє, картотек з питань правового та соціального забезпечення людей з фізичними обмеженнями;

• здійснення інформаційно-бібліотечного обслуговування людей з обмеженням життєдіяльності поза стінами бібліотек ;

• запровадження системи віртуального бібліотечного обслуговування людей з фізичними обмеженнями (запис до бібліотеки та прийом замовлень по телефону, e-mail, віртуальна довідка, надання інформації з мережі Інтернет);

• організація заходів з розкриття талантів, захоплень людей з фізичними обмеженнями (творчі вечори, вечори-зустрічі, персональні виставки тощо);

• проведення вікторин, розвиваючих ігор, тренінгів, тестів, які сприятимуть подоланню інформаційної та психологічної самотності людей з обмеженнями;

• організація інформаційно-благодійних заходів (благодійне свято, інформаційний марафон, день спонсора тощо);

• активна участь у заходах, які проводяться місцевими громадськими організаціями інвалідів;

• вивчення та узагальнення світового та вітчизняного досвіду з інформаційно – бібліотечного обслуговування та сприяння соціально-культурній реабілітації людей з фізичними обмеженнями;

• виявити літературу для інвалідів (право, законодавство, періодика тощо); про інвалідів; написану інвалідами – "Книги, що допомагають жити" та інші.

На веб-сайтах можна створити рубрику "Турбота", яка може містити наступні лінки:

• законодавство для людей з особливими потребами;

• інтернет для людей з обмеженими фізичними можливостями (пошук інформації про новітні технології у лікуванні рідкісних захворювань);

• служба зайнятості інформує (пошук роботи для людей з обмеженими фізичними можливостями);

• творчість (підтримка талановитих людей з обмеженими можливостями, популяризація їх творчості через веб-сторінку бібліотеки).

З метою систематичного обслуговування даної категорії людей необхідно створити "Адресну картотеку", яка буде включати:

• прізвище, ім'я та по-батькові людини – інваліда;

• прізвище, ім'я та по-батькові опікунів;

• адресу, телефон;

• стать;

• вік;

• вид захворювання;

• здібності, зацікавлення;

• вид бібліотечного обслуговування (на дому, в бібліотеці).

Для обслуговування на дому варто залучати волонтерів з кола читачів бібліотеки.

При індивідуальній роботі з інвалідами необхідно використовувати традиційні форми бібліотечної роботи: книгоношення, бесіди, індивідуальне інформування, індивідуальні запрошення на масові заходи бібліотеки, складання тематичних добірок, рекомендаційних списків тощо.

Поширенню життєво необхідної інформації серед людей з обмеженими можливостями сприятимуть "зони ділової інформації", які можуть включати:

1. Інформаційні стенди, на яких представлені матеріали про:

• нові законодавчі документи з питань життєдіяльності інвалідів;

• соціальні, психологічні і педагогічні заклади, які займаються проблемами людей з вадами здоров'я;

• перелік навчальних закладів, які пропонують варіаційні форми здобуття освіти для людей з інвалідністю;

• перелік медико-реабілітаційних центрів в Україні і за кордоном;

• інформація про працевлаштування;

• повідомлення про проведення акцій, конкурсів, благодійних марафонів тощо.

2. Тематичні папки: «Законодавство України», «Пільги інвалідам», «Освіта», «Медицина», «Про статус ветеранів війни».

3. Папки – досьє, які вміщують фактографічну інформацію про :

• навчальні заклади;

• адреси, реквізити, телефони;

• графіки роботи приймальних комісій, правила прийому документів;

• форми та терміни навчання, факультети, спеціалізації;

• перелік екзаменів та терміни їх здачі;

• наявність підготовчих курсів;

• сума оплати за навчання, пільги інвалідам;

- медичні та реабілітаційні заклади, протезно-ортопедичні підприємства;
- адреси, реквізити закладів;
- графіки роботи, правила прийому інвалідів;
- перелік захворювань, за якими здійснюється лікування;
- наявність спеціалізованого обладнання та протезування;
- прейскурант цін на послуги, пільги інвалідам;
- служби побуту, які обслуговують людей з обмеженими можливостями та пільги, що їм надаються;
- розклад руху та маршрути громадського транспорту;
- магазини.

Основним напрямком роботи має стати інформаційний.

З метою надання кваліфікованої інформації з питань правового, соціального, психологічного захисту населення, рекомендуємо організувати на базі бібліотеки консультаційний пункт юриста, психолога, соціального працівника, з чітко визначеними графіками роботи. В такі дні в бібліотеці доцільно проводити Дні інформації, присвячені заздалегідь визначеній темі, що стосується життєдіяльності людей з певними вадами здоров'я:

- "Працевлаштування";
- "Соціальні гарантії людям з обмеженими можливостями";
- "Пільги інвалідам";
- "Подолання стресу після травми";
- "Мої страхи";
- "Психологічне розвантаження".

Особливе значення для людей з інвалідністю має забезпечення вільного доступу до інформаційних ресурсів Інтернет. Він збільшує межі спілкування, яке для людей з обмеженими можливостями має життєво важливий, в якійсь мірі реабілітаційний характер.

Велику роль в цьому відіграє консультант, який буде проводити навчання даної категорії людей. А тому насамперед на базі бібліотеки необхідно створити інтернет – клас, відвідувати який будуть групи попередньо сформовані за різними ознаками (віковою, рівнем освіти, видами хвороби, характером трудової діяльності).

Перший етап навчання з людьми, які мають вади здоров’я необхідно розпочати з найпростішого:

- бесіди на теми "Я і комп’ютер", "Що таке світова мережа інтернет",
- Сучасні інформаційні технології";
- книжкові виставки, які допоможуть початківцям ближче познайомитися з комп’ютерними технологіями;
- показ фільмів на DVD - R.

Другим етапом з такими людьми буде навчання елементарними навиками роботи на комп’ютері:

- малювання;
- навчальні ігри з комп’ютерної грамотності;
- текстовий набір;
- пошук інформації в мережі "Інтернет".

Незважаючи на актуальність проблеми обслуговування людей з особливими потребами в бібліотеках, вона не досить висвітлюється. Ні в теорії ні в практиці. Це зумовлено об’єктивними причинами: непристосованість приміщень, відсутність обладнання, повільне оновлення фондів, тощо.

У інших країнах (зокрема в США), кожна бібліотека пристосована для відвідування такими людьми. Це під’їзд для машини і візка, зручні підходи до читацького місця, до місця за комп’ютером, спец ліфти і тд.

Враховуючи досвід зарубіжних країн, є сенс організувати обслуговування людей з особливими потребами не тільки у спеціальних бібліотеках, а й у публічних. Це підвищить статус бібліотеки, полегшить життя цим людям.

Висновки. Сьогодні є очевидною потреба в розвитку структури, яка стала б провідником і транслятором норм і правил поведінки у даному напрямку. І саме бібліотеки володіють можливостями стати центрами поширення інформаційної та поведінкової культури, набуття якої веде до розуміння і толерантності. Звичайно, бібліотекарі не є професіоналами і досвіду роботи з особливими людьми у нас немає, але на те ми і бібліотекарі, щоб враховувати інтереси різних категорій читачів і нести світло книги і знання будь-якому читачеві, незалежно від здібностей, статусу, звичок, характеру.

Часто бібліотекарі вважають, що обслуговування людей з особливими потребами займає багато часу, а тому не стимулюють їхню появу в бібліотеці. Насправді, давно настав час здолати ці стереотипи і перетворити бібліотеку в гостинний дім для всіх. Адже, правильно підібрана книга, що викликає позитивні емоції, не менш важлива, ніж уміло підібрані ліки.

ЛІТЕРАТУРА:

1. Литвин А.В. Розвиток спеціалізованих бібліотек для людей з особливими потребами // Бібліотечна планета. – 2004. – № 2. – С. 36-39.

2. Ашаренкова Н. Обслуговування користувачів з особливими потребами в публічних бібліотеках. Послуги, що стають реальністю для України [Текст] / Н. Ашаренкова // Бібл. планета. – 2006. – № 1. – С. 7–11 ; 2005. – № 4. – С. 7–11.

3. Васильченко С. Бібліотечно-інформаційне обслуговування людей з обмеженими можливостями [Текст] /С. Васильченко, Н. Солонська, О. Воскобойнікова-Гузєва // Бібл. вісн. – 2002. – № 1. – С. 37–41.

4. Кунанець Н. Інформаційні ресурси бібліотек для людей з особливими потребами: стан та перспективи / Н. Кунанець, О. Лозицький, В. Пасічник // Вісн. кн. палати. –2011. – № 10. – С. 1 – 4 .

5. Мартюшова О. Інформаційно-ресурсний центр для людей з обмеженими можливостями в публічній бібліотеці /О. Мартюшова // Бібл. планета. – 2011. – № 2. – С. 24 – 25.

6. Пашкова В.С. Рівноправний доступ, рівні можливості: еволюція бібліотечного обслуговування громадян із особливими потребами [Текст] / В.С. Пашкова // Бібліотекознавство. Документознавство. Інформологія. – 2006. –№ 3. – С. 26–34.

REFERENCES:

1. Litvin A.V. Rozvitok spetsIalIzovanih bIblIotek dlya lyudey z osoblivimi potrebami // BIblIotechna planeta. – 2004. – № 2. – C. 36-39.

2. Asharenkova N. Obslugovuvannya koristuvachIv z osoblivimi potrebami v publIchnih bIblIotekah. Poslugi, scho stayut realnIstyu dlya UkraYini [Tekst] / N. Asharenkova // BIbl. planeta. – 2006. – № 1. – S. 7–11 ; 2005. – № 4. – S. 7–11.

3. Vasilchenko S. BIblIotechno-InformatsIyne obslugovuvannya lyudey z obmezhenimi mozhlivostyami [Tekst] /S. Vasilchenko, N. Solonska, O. VoskoboynIkova-GuzEva // BIbl. vIsn. – 2002. – № 1. – S. 37–41.

4. Kunanets N. InformatsIynI resursi bIblIotek dlya lyudey z osoblivimi potrebami: stan ta perspektivi / N. Kunanets, O. Lozitskiy, V. PasIchnik // VIsn. kn. palati. –2011. – № 10. – S. 1 – 4 .

5. Martyushova O. InformatsIyno-resursniy tsentr dlya lyudey z obmezhenimi mozhlivostyami v publIchnIy bIblIotetsI /O. Martyushova // BIbl. planeta. – 2011. – № 2. – S. 24 – 25.

6. Pashkova V.S. RIvnopravniy dostup, rIvnI mozhlivostI: evolyutsIya bIblIotechnogo obslugovuvannya gromadyan Iz osoblivimi potrebami [Tekst] / V.S. Pashkova // BIblIotekoznavstvo. Dokumentoznavstvo. InformologIya. – 2006. – № 3. – S. 26–34.

Рецензент: к.т.н., с.н.с. Лоза В.М., старший науковий співробітник науково-дослідного центру, Військовий інститут, Київський національний університет імені Тараса Шевченка

Гуменная Е.И., к.т.н Муляр И.В., Ряба Л.А.

ДОСТУПНОЕ БИБЛИОТЕЧНОЕ ПРОСТРАНСТВО ДЛЯ ПОЛЬЗОВАТЕЛЕЙ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

В статье рассматривается необходимость создания равных возможностей для доступа к знаниям, информации и художественных произведений путем использования различных ресурсов и услуг одинаково для всех членов общества, независимо от степени трудоспособности, религиозных, этнических особенностей. Физические дефекты, отсутствие мобильности людей с ограниченными возможностями здоровья не обеспечивает свободный доступ к информации. Выделение проблем библиотечно-информационных услуг, которые помогают людям с ограниченными возможностями получить информацию, чтобы не быть изолироваными от социальной и культурной жизни общества. Задача библиотек заключается в том, чтобы сломать барьеры и сделать информацию в наиболее доступной и полноценной для различных групп граждан. При всей сложности задачи по социальной защите людей с ограниченными возможностями следует привлечь их к книге, к библиотеке. Это абсолютное условие их полной социальной реабилитации. Библиотеки должны сделать все, чтоб их ресурсы стали доступными для всех категорий пользователей .

Ключевые слова: библиотечно-информационое обслуживание; библиотечные услуги; люди с ограниченными возможностями.

Humenna E.I., Ph.D. Mulyar I.V., Ryaba L.A.

THE LIBRARY IS AVAILABLE FOR USERS WITH DISABILITIES

The article discusses the need for creating equal opportunities of access to knowledge, information and artistic works through the use of a range of resources and services equally to all members of society, regardless of the degree of disability, religious, ethnic characteristics. Physical defects, the lack of mobility of people with disabilities health does not provide free access to information. Highlighting the problems of library-information services that help people with disabilities get information to not be isolated from social and cultural life of society. The task of the libraries is to break down barriers and make the information in the most accessible and complete the following categories for different groups of citizens. For all the complexity of the tasks on the social protection of people with disabilities want to attract them to the book to the library. This is the absolute condition of their full social rehabilitation. Libraries should do everything in order for the resource.

Keywords: library and information services; library services; persons with disabilities.

УДК 504(477):323
к.пед.н., доц. **Дячук А.О.** (ХмНУ)

ВИДИ ТА ХАРАКТЕРИСТИКА ПОЖЕЖ В ЕКОСИСТЕМАХ І ЇХ ВПЛИВ НА ЗАГАЛЬНИЙ СТАН ЕКОЛОГІЧНОЇ БЕЗПЕКИ ХМЕЛЬНИЦЬКОЇ ОБЛАСТІ

На сьогодні у багатьох регіонах нашої країни постає проблема виникнення та перебігу пожеж у природних екосистемах. Особливо, критичною ситуація стає у літні місяці року, в регіонах з малою кількістю річних опадів, на територіях відпочинку населення та в об'єктах природно-заповідного фонду держави. У статті розглянуто актуальну проблему, що стосується причин виникнення, характеристику лісових пожеж, їх вплив на стан екологічної безпеки Хмельницької області.

Їх небезпека полягає у непередбачуваності, різних походженнях джерел загоряння, швидкості розповсюдження та інших факторах.

Пожежі в екосистемах виникають, головним чином, завдяки антропогенному впливу та внаслідок дії деяких природних чинників (влучання блискавки, високої температури навколишнього середовища, вулканічної діяльності), чим спричиняють різке погіршення стану екологічної безпеки регіону, а також здатні спричинити людські жертви та значні матеріальні втрати.

У результаті досліджень було встановлено, що найбільш ураженими в плані екологічної безпеки є території Хмельницької області розташовані у підпорядкуванні Ізяславського, Славутського та Шепетівського лісових господарств. Аналіз отриманих даних вказує на те, що виникнення та розвиток пожеж у природних екосистемах залежить від природно-кліматичних, метеорологічних умов та антропогенного впливу.

Постановка задачі. Одним із найбільш небезпечних явищ, що загрожують екологічній безпеці та вражають екосистеми є пожежі. Їх небезпека полягає у непередбачуваності, різних походженнях джерел загоряння, швидкості розповсюдження та інших факторах.

На сьогодні у багатьох регіонах нашої країни постає проблема виникнення та перебігу пожеж у природних екосистемах. Особливо, критичною ситуація стає у літні місяці року, в регіонах з малою кількістю річних опадів, на територіях відпочинку населення та в об'єктах природно-заповідного фонду держави. З огляду на це актуальним є проведення аналізу видів та головних причин виникнення пожеж, а також встановлення небезпечних територій у досліджуваній області.

Мета роботи. Провести аналіз видів та дати характеристику пожеж, що виникають на території області, встановити найбільш небезпечні райони поширення пожеж, а також вивчити їх вплив на стан екологічної безпеки регіону.

Викладення матеріалів дослідження. Згідно літературних джерел пожежа – це неконтрольований процес горіння, що стихійно виникає і розповсюджується в навколишньому середовищі і супроводжується інтенсивним виділенням тепла, диму та світловим випромінюванням, що створює небезпеку для людей і завдає шкоду об'єктам господарської діяльності та навколишньому середовищу [3].

Лісова пожежа – це некерований багатостадійний процес горіння лісових матеріалів у відкритому просторі на покритій лісом площі [3, 5].

Лісові пожежі, за Мелеховим І.С. (1947), виникають при наявності горючих матеріалів, умов, сприятливих загоранню цих матеріалів, тобто кисню, та джерела вогню.

Тоф'яна пожежа – це неконтрольований процес димного горіння торфу внаслідок природного або штучного загоряння [5].

З природних екосистем ліси і торфовища займають понад 10 млн. га території України, тому лісові й торфові пожежі є найбільш поширеними. 31 % лісів розташовано в північному регіоні, 17 % – у східному, 10 % – у південному, 8 % – в південно-західному і 32 % – в західному регіоні.

Найвищі показники ймовірності виникнення лісових пожеж та збитків від них характерні для хвойних молодняків та середньовікових насаджень Півдня, Сходу та Полісся

України. Загальна площа таких насаджень по Держкомлісгоспу становить понад 2 млн. га [2].

Лісові пожежі виникають, головним чином, завдяки антропогенному впливу та внаслідок дії деяких природних чинників (влучання блискавки, високої температури навколишнього середовища, вулканічної діяльності). Вогонь може швидко розростися і, підхоплений вітром, стати вогненним валом, що знищує на своєму шляху все живе і перетворює ліси в нежиттєздатні пустелі. При цьому, виникає реальна загроза для населених пунктів, життя людей, домашніх тварин, матеріальних цінностей. Найбільш небезпечними, з точки зору виникнення, бувають жаркі та сухі літні дні з відносною вологістю повітря – до 40 %.

Залежно від джерел виникнення та того, в яких елементах лісу поширюється вогонь, лісові пожежі поділяються на низові, верхові, ґрунтові, а за швидкістю поширення і висотою полум'я – на слабкі, середні й сильні (рис. 1).



Рис. 1. Класифікація пожеж, що виникають у природних екосистемах

Детальну класифікацію склав Мелехов І.С. (1944), він поділив лісові пожежі на:

− низові: підстилочно-гумусові; надґрунтові; підлісно-чагарникові і підлісно-деревні; сушнякові; пенькові;

− верхові: вершинні; повальні; стовбурні;

− підземні: торф'яні [5].

Найбільш розповсюдженими та цікавими для нас є низові пожежі, частка яких складає близько 80 % з усіх випадків можливих пожеж.

Низові (низинні) пожежі виникають у результаті згоряння хвойного підліску, живого надґрунтового покриву (моху, лишайника, трав'янистих рослин, напівчагарників і чагарників) та мертвого покриву або підстилки (опалого листя, хвої, кори, сушняку, хмизу, бурелому, гнилих пнів), тобто рослин та рослинних залишків, розташованих безпосередньо на ґрунті або на невеликій висоті (1,5 – 2 м). Полум'я має висоту до 50 см (рідше може підійматись до 1 м), швидкість розповсюдження вогню при цьому невелика – від 100 м/год. до200 м/год., а при сильному вітрі – до 1км у рівнинній місцевості та від 1 км до 3 км на схилах [11].

Згідно [3, 5] низові пожежі бувають швидкі й суцільні. Швидкі пожежі характеризуються тим, що кромка полум'я швидко рухається, а дим світло-сірого кольору. Згорають надґрунтовий покрив, опале листя, підлісок. Просування таких пожеж проходить

нерівномірно. Швидкі пожежі характерні для весни, коли на ґрунті підсохне лише тонкий шар дрібного матеріалу, який може горіти.

Суцільні пожежі повністю спалюють надґрунтовий покрив, висота полум'я вища, ніж у швидких, і досягає 2 м, але швидкість вогню невелика − не перевищує кількох сотень метрів за годину. Суцільні низові пожежі виникають, як правило, влітку, коли просохнуть сушняк і підстилка. Вони розвиваються переважно з щільним моховим покриттям, у чорничниках, у сосняках і брусничниках, світлохвойних лісах, на підвищених сухих місцях.

Верхові лісові пожежі виникають із низових і відмінність їх у тому, що згоряє не тільки надґрунтовий покрив, але й нижні яруси дерев та крони жердняків. Однак, можуть бути ще й вершинні пожежі, коли вогнем знищуються лише крони дерев. Але без супроводу низинної пожежі, вони довго продовжуватися не можуть.

Під час верхових пожеж виділяється багато тепла. Висота полум’я при цьому становить 100 м і більше. В таких випадках вогонь перекидається на значні відстані, іноді на декілька сотень кілометрів з утворенням завихрень, а швидкість пожежі зростає до 8 км/год. – 25 км/год.

Верхові пожежі, як і низові, поділяються на швидкі й суцільні.

При швидких верхових пожежах вогонь поширюється стрибками зі швидкістю 0,2-0,6 км/год., а при сильному повітрі − до 525 км/год., дим темного кольору.

Суцільні верхові пожежі характерні тим, що вогонь рухається суцільною стіною від надґрунтового покриву до крон дерев. Дим при такій пожежі темно-сірого кольору.

Торф’яні пожежі – це загоряння висушеного торфовища внаслідок природних чинників або викликане штучно. Вони часто охоплюють величезні простори і дуже важко піддаються гасінню. Небезпека їх у тому, що горіння виникає під землею, утворюючи пусті місця у торфі, який уже згорів. У ці пустоти можуть провалюватися люди і техніка. Такі пожежі виникають частіше наприкінці літа, як продовження низових або верхових лісових пожеж і розповсюджуються по тому що знаходиться в землі торф'яному шару на глибину до 50 см і більше. Горіння йде повільно, майже без доступу повітря, зі швидкістю 0,1-0,5 м/хв з виділенням великої кількості диму і освітою вигорілих порожнин (прогарів). Тому підходити до осередку підземної пожежі треба з великою обережністю, постійно промацуючи щупом [5].

Заглиблення низової пожежі починається біля стовбурів дерев, потім поширюється у боки зі швидкістю від кількох сантиметрів до кількох метрів на добу. Дерева при цьому повністю гинуть внаслідок оголення і обгорання коріння. Такі пожежі можуть виникати на ділянках з торф'янистими ґрунтами і ділянках із шаром підстилки 20 см і більше.

Торфові пожежі також можуть виникати незалежно від лісових: у районах торфорозробок і оліготрофних боліт. Горіння проникає у більш глибокі шари торфу і цьому сприяє наявність у ґрунті коріння.

Вогню на поверхні ґрунту при підземних пожежах немає, лише інколи він пробивається з-під землі, але скоро зникає, виділяється тільки дим, який стелиться. На такі пожежі не впливають ні вітер, ні добові зміни погоди. Вони можуть тягнутися місяцями і в дощ, і в сніг.

Торф містить до 25 % бітумів. Під час пожежі вони зосереджуються біля поверхні, що горить, і при її охолодженні водою цементують частинки вугілля. Як наслідок, виникає водонепроникний шар, під яким залишається тління, що можливе при невисокому вмісті кисню в повітрі. Це явище утруднює гасіння торфових пожеж, оскільки вода не може проникнути до осередку пожежі [5].

Всі види цього лиха супроводжуються такими вражаючими факторами, як висока температура в зоні вогню, задимлення великих районів, що подразнююче діє на людей і значно ускладнює боротьбу з пожежею, обмеження видимості, негативний психологічний вплив на населення прилеглих поселень.

Не стала виключенням по виникненню пожеж у природних екосистемах та, відповідно, погіршенню стану екологічної безпеки і Хмельницька область. Так згідно досліджень Г.О.

Обихода та оцінки зони можливих пожеж на території області рівна 230,0 тис. га (з них сильних верхових і низових 70 тис. га, слабких низових – 169 тис. га). Лісистість території області становить близько 13 % від загальної площі, також тут розташовані болота та торфовища, які за певних умов є пожежо-небезпечними. Згідно даних отриманих в обласному Управлінні лісового та мисливського господарства за 2011-2015 роки на території області виникло 58 пожеж (по об'єктах Держкомлісгоспу) загальною площею ураження 411 га. Розподіл пожеж по лісових господарства області представлено на рис. 2.

Серед найбільш уражених є і території природно-заповідних об'єктів області розташованих у підпорядкуванні Ізяславського, Славутського та Шепетівського лісових господарств. Під час виникнення та розвитку пожеж тут постраждали лісові угіддя, унікальні оліго- та мезотрофні болота, тваринний світ. Великі площі потенційних слабких низових пожеж вказують на те, що виникають можливості втрати первинного стану об'єктів (зокрема, боліт, торфовищ), відбувається трансформація природних екосистем із втратою цінності об'єктів природно-заповідного фонду.

Аналіз отриманих даних вказує на те, що виникнення та розвиток пожеж у природних екосистемах залежить від природно-кліматичних. метеорологічних умов та антропогенного впливу.

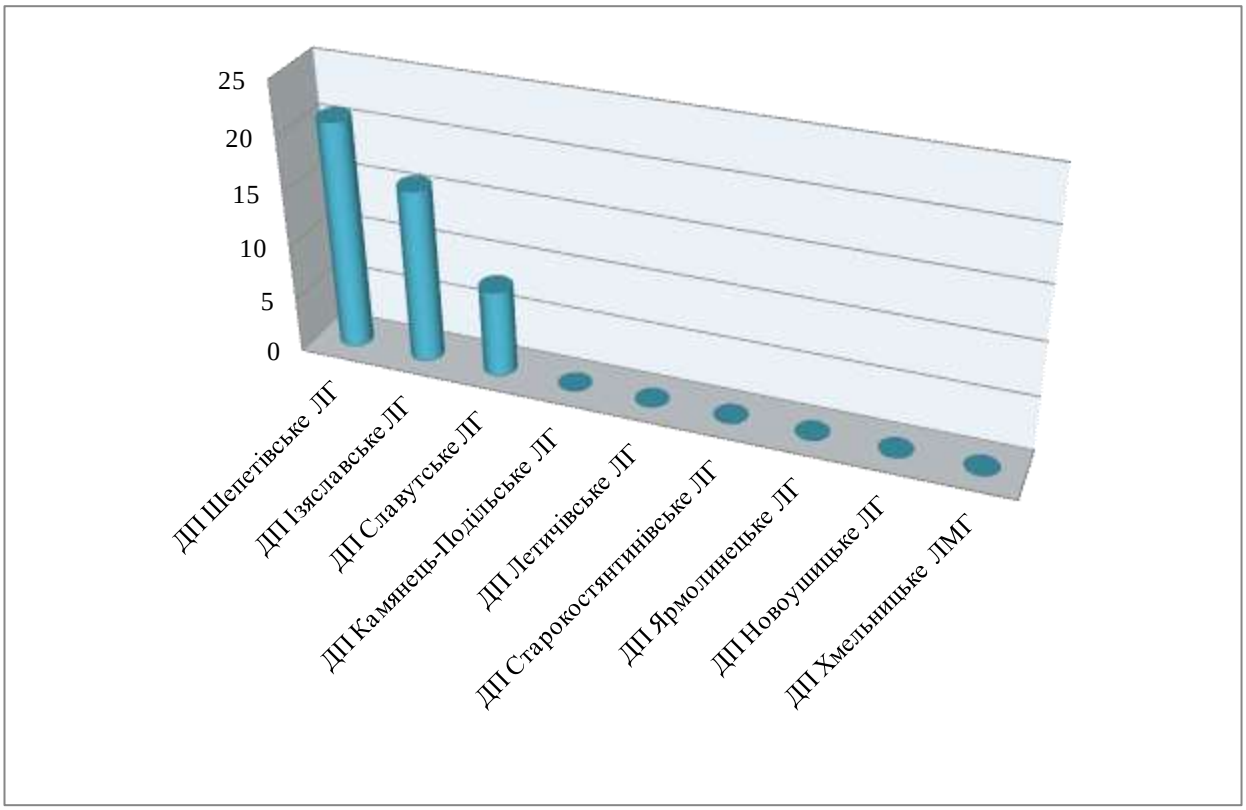


Рис. 2. Розподіл пожеж по лісових господарствах, що знаходяться на території Хмельницької області (2015 рік)

Так на рис. 3 відображено кількість пожеж по трьох найбільш «вразливих» лісових господарствах області, і стає очевидним, що 2015 рік став критичним. Лише протягом одного року на об'єктах підпорядкованих ОУЛМГ виникло 45 пожеж загальною площею ураження 409,57 га. Визначальну роль у такому розподілі внесли погодні умови – аномально посушливе літо, відсутність опадів, а також людський фактор (більшість пожеж виникала внаслідок порушення правил поводження із вогнем, сільськогосподарських підпалів та недбалості).

Характерною особливістю є сконцентрованість пожеж – це переважно період з липня по вересень місяць, коли на більшій території України тривалий час домінувала надзвичайно спекотлива та суха погода [2, 4, 5].

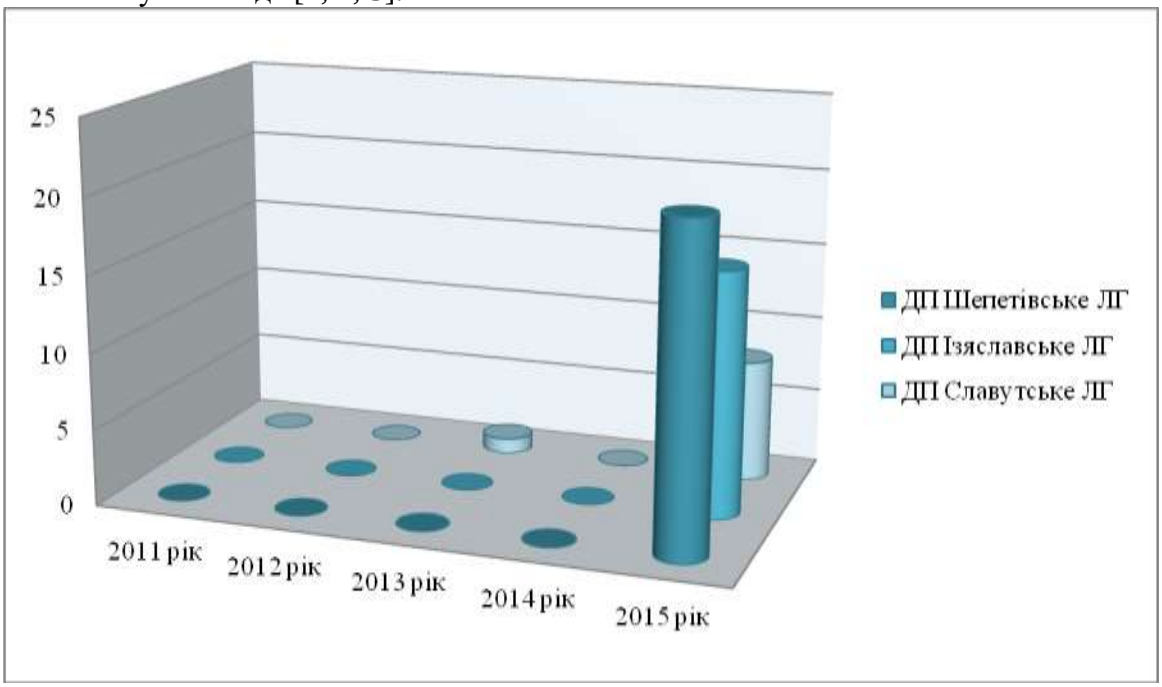


Рис. 3. Кількість пожеж на об’єктах підпорядкованих ОУЛМГ
у Хмельницькій області протягом 2011-2015 років

Високий рівень виникнення пожеж саме на територіях Ізяславського, Славутського та Шепетівського лісових господарств може бути і високий вміст смоли у хвойних деревах [4] порівняно із листяними породами, оскільки на згаданих територіях переважно хвойні ліси. Також А.Д. Кузик стверджує, що неперегнилі сухі рештки за умов низької вологості та високої температури здатні до займання та горіння навіть при не надто потужному джерелі запалювання. Зважаючи, на високий вміст хвої та смоловмісних решток, сухих мохів та трав’яного покриву ліси північної частини Хмельниччини є надзвичайно пожежо-небезпечними при наступних посушливих періодах.

Висновки. За останні роки екологічна безпека багатьох регіонів України зазнає впливу від пожеж, що виникають у природних екосистемах (зокрема: лісі, болоті, торфовищах). Згідно розглянутої класифікації ці пожежі поділяються: за причинами виникнення (на природні та антропогенні); за локалізацією по об’єктах екосистеми (на верхові, низові та грунтові); за швидкістю поширення полум’я (на сильні,середні та слабкі). Найбільш часто виникають низові пожежі, які в подальшому переростають у верхові.

Основними природними причинами виникнення пожеж є блискавки та самозаймання у посушливу погоду, антропогенними – підпали, сільгосппідпали, з вини населення (необережне поводження з вогнем, нехтування правил пожежної безпеки), та з вини організацій, що здійснюють промислову діяльність. Виникненню пожеж на територіях лісів, боліт та торфовищ сприяє висока температура повітря, мала кількість опадів, а також низька вологість.

Так наочним прикладом є Хмельницька область на території якої протягом 2015 року виникло 45 пожеж загальною площею ураження 409,57 га. Характерною рисою є концентрація пожеж на території області, яка пов’язана із високим ступенем заліснення Ізяславського, Славутьського, Шепетівського лісових господарств − територія національного природного парку «Мале Полісся», який створено в 2013 році.

Тому з метою дотримання належного стану екологічної безпеки на території області необхідно запроваджувати профілактичні, організаційні, попереджувальні, обмежувальні, освітні (підвищення кваліфікації персоналу), лісівничі заходи.

ЛІТЕРАТУРА:

1 Безпека регіонів України і стратегія її гарантування у 2-х т.: Т1. Природно - техногенна (екологічна) безпека / [Б.М. Данилишин, А. В. Степаненко, О. М. Ральчук та ін.]. − К. : Науково-виробниче підприємство Видавництво «Наукова Думка» НАН України, 2008. − 392 с.

2 Валендик Э.Н. Крупные лесные пожары / Э.Н. Валендик, П.М. Матвеев, М.А. Софронов. – М. : Наука, 1979. – 196 с.

3 Свириденко В. Є., Бабіч О. Г., Швиденко А. Й. Лісова пірологія. – К.: Агропром-видав України, 1999. – 172 с.

4 Кузик А. Д. Про залежність пожежної безпеки лісів України від типів лісових насаджень // Пожежна безпека. – Львів: ЛІПБ. – 2006, №9. – С. 34-37.

5 Нікітін, Ю. А. Попередження і гасіння пожеж у лісах і на торфовищах / Ю. А. Нікітін, В. Ф. Рубцов. − М.: Россельхозиздат, 1989. - 96 с.

6 Правила пожежної безпеки в лісах України. – Наказ Держлісгоспу України № 278 від 27.12.2004 р.

7 Дячук А.О. Аналіз об’єктів підвищеної екологічної небезпеки, розташованих на території Хмельницької області. // «Питання біоіндикації та екології». − Період. наук. видання. Вип. № 18. − Запоріжжя: Вид-во ЗНУ, 2013. − С. 3-11.

REFERENCES:

1 Danilishin B.M., Stepanenko A.V., Ral'chuk O. M. ta in.(2008) «Bezpeka regioniv Ukraïni i strategiya її garantuvannya u 2-h t.» : T1. Prirodno - tekhnogenna (ekologichna) bezpeka − K. : Naukovo-virobniche pidprієmstvo Vidavnictvo «Naukova Dumka» NAN Ukraïni, − 392 s.

2 Valendik EH.N. Krupnye lesnye pozhary (1979) – M. : Nauka – 196 s.

3 Sviridenko V.Є., Babich O.G., Shvidenko A.J. (1999) Lisova pirologiya. – K.: Agroprom-vidav Ukraïni – 172 s.

4 Kuzik A.D. (2006) Pro zalezhnist' pozhezhnoї bezpeki lisiv Ukraïni vid tipiv lisovih nasadzhen'. Pozhezhna bezpeka. – L'viv: LIPB. – №9. – S. 34-37.

5 Nikitin, Y.A., Rubcov V. F. (1989) Poperedzhennya i gasinnya pozhezh u lisah i na torfovishchah. − M.: Rossel'hozizdat, − 96 s.

6 Pravila pozhezhnoї bezpeki v lisah Ukraïni (27.12.2004) – Nakaz Derzhlisgospu Ukraïni № 278 vid 27.12.2004 y.

7 Diachuk A.O. (2013) Analiz ob’єktiv pidvishchenoї ekologichnoї nebezpeki, roztashovanih na teritoriї Hmel'nic'koї oblasti. «Pitannya bioindikaciї ta ekologiї». − Period. nauk. vidannya. Vip. № 18. − Zaporizhzhya: Vid-vo ZNU − S. 3-11.

Рецензент: д.т.н., проф. Сбітнєв А.І.

к.пед.н. Дячук А.А.

ВИДЫ И ХАРАКТЕРИСТИКА ПОЖАРОВ В ЭКОСИСТЕМАХ И ИХ ВЛИЯНИЕ НА ОБЩЕЕ СОСТОЯНИЕ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТ И ХМЕЛЬНИЦКОЙ ОБЛАСТИ

На этот день во многих регионах нашей страны встает проблема возникновения и течения пожаров в природных экосистемах. Особенно, критической ситуация становится в летние месяцы года, в регионах с малым количеством годовых осадков, на территориях отдыха населения и в объектах природно-заповедного фонда государства. В статье рассмотрено актуальную проблему, касающуюся причин возникновения, характеристику лесных пожаров, их влияние на состояние экологической безопасности Хмельницкой области.

Их опасность заключается в непредсказуемости, различного происхождения источников возгорания, скорости распространения и других факторах.

Пожары в экосистемах возникают, главным образом, благодаря антропогенному воздействию и в результате действия некоторых природных факторов (попадание молнии, высокой температуры окружающей среды, вулканической деятельности), чем вызывают резкое ухудшение состояния экологической безопасности региона, а также могут повлечь человеческие жертвы и значительные материальные потери.

В результате исследования было установлено, что наиболее пораженными в плане экологической безопасности являются территории Хмельницкой области, которые расположены в подчинении Изяславского, Славутского и Шепетовского лесных хозяйств. Анализ полученных данных указывает на то, что возникновение и развитие пожаров в природных экосистемах зависит от природно-климатических, метеорологических условий и антропогенного воздействия.

Ph.D. Diachuk A.A.

THE KIND AND TYPE OF FIRES IN THE ECOSYSTEM AND THEIR EFFECTS ON ECOLOGICAL SAFETY OF KHMELNYTSKY'S REGION

In our days many regions of the country face the problem of the origin and course of fire in natural ecosystems.

Especially, the situation is getting critical during the summer months of the year, in regions with low annual precipitation, in recreation areas and objects of natural reserve fund of the state. This article discusses the actual problem of appearance and characteristics of forest fires and their impact on the environmental safety of Khmelnitsky region.

They are dangerous because of their unpredictability, of different origin sources of ignition, how fast they spread around and other factors.

Fires in ecosystems occur mainly due to anthropogenic influence and as a result of some natural factors (lightning, high ambient temperature, volcanic activity). Those factors make a significant influence on the ecological safety of the region, causing major financial losses and sometimes even a human sacrifices.

The studies found that Iziaslav, Slavuta and Shepetivka forest preserve from Khmelnytsky region are the most affected in terms of environmental safety. Analysis of the data indicates that the emergence and development of fire in natural ecosystems depends on climatic, weather conditions and human impact.

УДК 519.242.5

д.т.н., проф. **Кошевой Н.Д.** (НАКУ “ХАИ”)
Стадник А.С. (НАКУ “ХАИ”)

ОПТИМАЛЬНОЕ ПЛАНИРОВАНИЕ ЭКСПЕРИМЕНТА В УСЛОВИЯХ ОГРАНИЧЕНЫХ РЕСУРСОВ

Исследованы свойства комбинаторных планов многофакторного эксперимента. Разработаны алгоритм оптимизации по стоимостным (временным) затратам многофакторных планов эксперимента с использованием метода вложенных разбиений и реализующее его программное обеспечение, основанные на перестановке столбцов матрицы планирования эксперимента. Показана его эффективность в сравнении с методами анализа перестановок, случайного поиска, классического и ячеистого генетических алгоритмов. Эффективность использования данного алгоритма показана на примерах технологических процессов оптимизации параметров неравномерности покрытия проводников гальваническими осадками и точности устройства для контроля качества диэлектрических материалов. Работоспособность алгоритма на основе метода вложенных разбиений подтверждается приближением оптимальных планов, полученных этим методом и методом перестановки строк матрицы планирования.

Ключевые слова: метод вложенных разбиений, планирование эксперимента, оптимальный план, быстродействие.

Постановка задачи. Рост эффективности производственных процессов непосредственно связан с построениями адекватных математических моделей. В дальнейшем модели используют для поиска оптимальных режимов обработки, способных обеспечить необходимое качество продукции. Особо остро вопрос повышения эффективности исследований стоит для дорогостоящих и длительных технологических процессов. Для решения задачи оптимизации применяют различные способы повышения результативности экспериментальных методов исследования.

Изменение порядка проведения опытов существенно влияет на затраты по проведению эксперимента. Увеличение количества рассматриваемых вариантов усложняет поиск плана. Основная трудность состоит в быстром росте количества вариантов перестановок в зависимости от количества факторов и количества их уровней. При современном уровне развития вычислительной техники точно решить задачу не представляется возможным. В связи с этим становится актуальным разработка и исследование приближенных алгоритмов.

Анализ последних исследований и литературных источников. Известны примеры построения оптимальных многофакторных планов, основанные на использовании следующих методов оптимизации: анализ перестановок [1], случайный поиск [1], классический (КГА) и ячеистый (ЯГА) генетические алгоритмы [2], жадный алгоритм [3], имитации отжига [4]. Эти приближенные методы позволяют находить близкий к оптимальному план эксперимента.

Эффективность их применения доказана при исследовании ряда различных объектов: технологических процессов, приборов, систем. Но при большом количестве факторов для перебора всех возможных вариантов необходимо много времени.

Ввиду этого целесообразно для сравнения результатов применить метод вложенных разбиений. На сегодняшний день актуальной также остается задача использования метода поиска оптимального плана эксперимента, обладающего более высокими показателями быстродействия.

Цель статьи. Анализ процессов оптимизации различных технологических процессов по стоимости реализации и времени поиска оптимального плана эксперимента с использованием метода вложенных разбиений.

Основные результаты. Разработаны алгоритм и программное обеспечение оптимизации планов многофакторного эксперимента по стоимостным затратам с использованием алгоритма вложенных разбиений (рис. 1).

Сущность применения алгоритма заключается в следующем.

Шаг 1. В начале работы алгоритма производится ввод количества факторов X.

Шаг 2. Затем производится ввод количество переходов.

Шаг 3. Вводятся стоимости переходов между уровнями для каждого из факторов.

Шаг 4. В зависимости от выбранного количества факторов строится матрица планирования эксперимента.

Шаг 5. Вычисляются стоимостные затраты для начального плана эксперимента.

Шаг 6. Выполняется проверка, если число оставшихся операций больше 1, то выполняется следующий шаг. Если нет, то осуществляется переход к шагу 23.

Шаг 7. Происходит вычисление затрат S_1 при переходе от *i*-ого перехода к (*i*+1)-ому.

Шаг 8. Выполняется проверка на наличие количества оставшихся нерассмотренных вариантов переходов. Если это количество больше 1, то выполняем переход к шагу 9. В противном случае – переход к шагу 11.

Шаг 9. Происходит вычисление затрат S_2 при переходе от *i*-ого перехода к (*i*+2)-ому.

Шаг 10. Выполняется сравнение затрат S_1 и S_2, получаемых на шагах 6 и 8, соответственно. Если S_2 больше S_1, то переход к шагу 11, если нет, то к шагу 20.

Шаг 11. Присвоение переменной min_1 значение S_1.

Шаг 12. Происходит вычисление затрат S_3 при переходе от *i*-ого перехода к (*i*+3)-ому.

Шаг 13. Выполняется проверка на наличие количества оставшихся нерассмотренных вариантов переходов. Если это количество больше 1, то переход к шагу 14, в противном случае – переход к шагу 16.

Шаг 14. Происходит вычисление затрат S_4 при переходе от *i*-ого перехода к (*i*+4)-ому.

Шаг 15. Выполняется сравнение затрат S_3 и S_4, получаемых на шагах 12 и 14, соответственно. Если S_4 больше S_3, то переход к шагу 16, если нет, то к шагу 21.

Шаг 16. Присвоение переменной min_2 значение S_3.

Шаг 17. Выполняется сравнение полученных минимальных затрат при переходах. Если min_2 больше min_1, то переход к шагу 18, в противном случае - к шагу 22.

Шаг 18. Переходу, которому соответствует значение min_1, присваивается первая позиция в оптимизированном плане.

Шаг 19. Запись первого пункта в оптимальный план и исключение этого перехода из списка записей.

Шаг 20. Присвоение переменной min_1 значения S_2.

Шаг 21. Присвоение переменной min_2 значения S_4.

Шаг 22. Переходу, которому соответствует значение min_1, присваивается вторая позиция в оптимизированном плане.

Шаг 23. Запись последнего перехода.

Проверка работоспособности разработанного алгоритма и программного обеспечения для оптимизации многофакторных планов эксперимента осуществлялась на следующих технологических процессах:

1) оптимизации параметров неравномерности покрытия проводников гальваническими осадками [5];
2) точности устройства для контроля качества диэлектрических материалов [6].

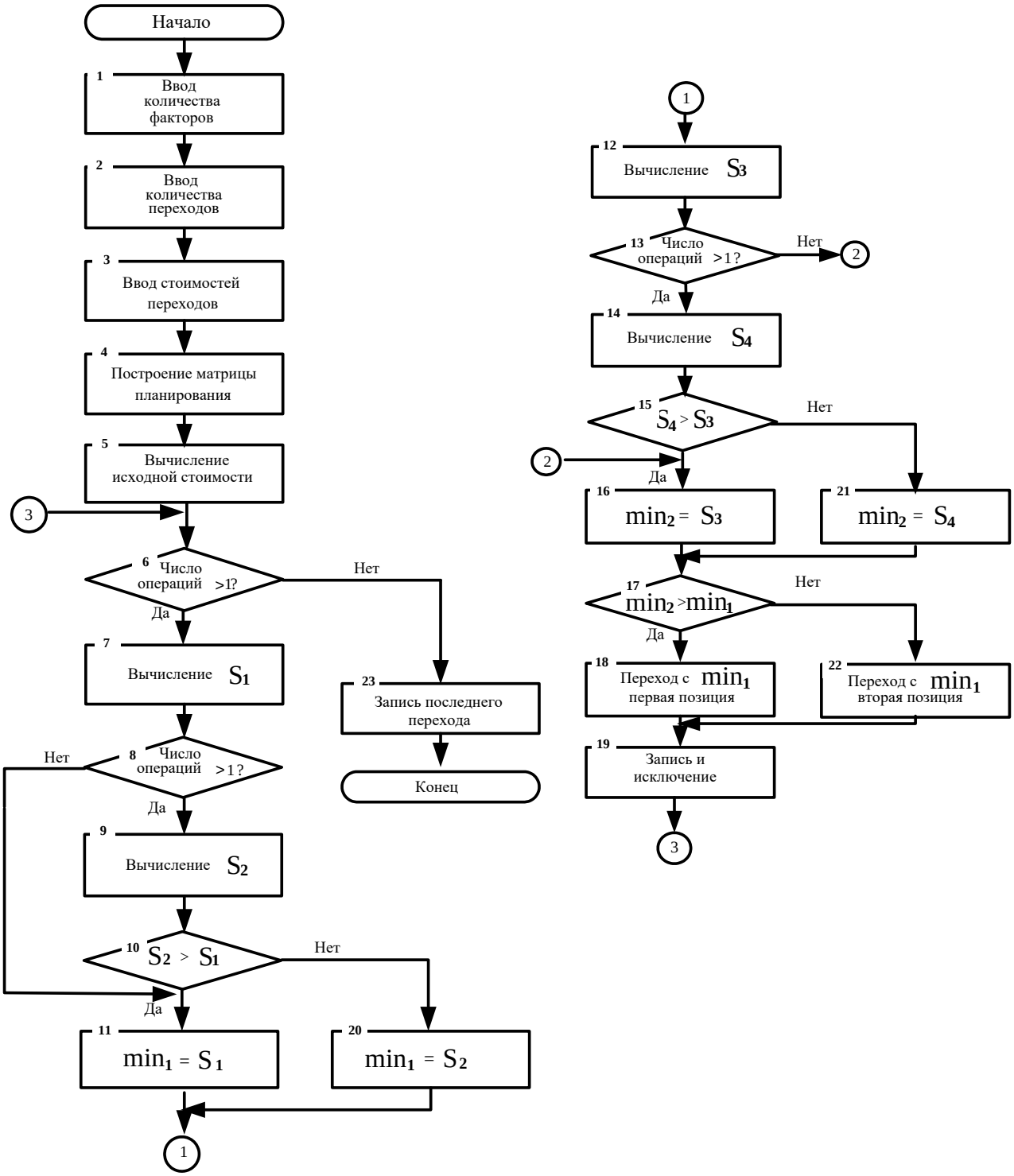


Рис. 1. Схема алгоритма, реализующая оптимизацию по стоимостным затратам планов многофакторного эксперимента по методу вложенных разбиений

Эти задачи были решены методами анализа перестановок, случайным поиском, КГА, ЯГА. Сравнение результатов представлено в табл. 1.

Таблица 1

Сравнение по критерию стоимости результатов оптимизации планов экспериментов различными методами

Технологический процесс	Стоимость начального плана, у.е.	Методы									
		Анализ перестановок		Случайный поиск		КГА		ЯГА		Вложенных разбиений	
		Стоимость, у.е.	Выигрыш, раз	Стоимость, у.е.	Выигрыш, раз	Стоимость, у.е.	Выигрыш, раз.	Стоимость, у.е.	Выигрыш, раз.	Стоимость, у.е.	Выигрыш, раз.
1	24,7	19,1	1,3	23,4	1,06	16,1	1,5	16,1	1,5	16,1	1,5
2	72,2	30,5	2,4	41,8	1,7	25,8	2,8	25,8	2,8	25,8	2,8

При поиске оптимальных комбинаторных планов эксперимента методом вложенных разбиений было затрачено менее 0,1 с. для исследования устройства для контроля качества диэлектрических материалов и менее 0,1 с. для оптимизации параметров, характеризующих неравномерность покрытия проводников гальваническими осадками (табл. 2).

Таблица 2

Сравнение по времени счета результатов оптимизации планов экспериментов различными методами

Метод	Время счета для ТП, с.	
	гальваническое меднения печатных плат	контроль качества диэлектрических материалов
Анализ перестановок	527	494
Случайный поиск	491	501
Классический ГА	2,4	1,4
Ячеистый ГА	3,2	3,5
Вложенных разбиений	0,1	0,1

Выводы. Разработан алгоритм и программное обеспечение, реализующие оптимизацию многофакторных планов экспериментов с применением метода вложенных разбиений. Доказана работоспособность и эффективность метода при исследовании технологических процессов.

Показано, что разработанное программное обеспечение позволяет без полного перебора всех вариантов перестановок получить оптимальные или близкие к оптимальным по стоимости реализации многоуровневые планы многофакторного эксперимента за время счета менее 0,1 сек.

Недостатком применения данного алгоритма является, то что при одних и тех же данных результаты оптимизации могут быть разными. Несмотря на это, его использование будет эффективным, так как при большом быстродействии программа выдаст результат,

приближенный к оптимальному плану, а при количестве факторов $n \leq 3$ результат будет оптимальным.

ЛИТЕРАТУРА:

1. Кошевой Н.Д. Оптимальное по стоимостным и временным затратам планирование эксперимента / Н.Д. Кошевой, Е.М. Костенко. – Полтава: издатель Шевченко Р.В., 2013. – 317 с.
2. Кошевой Н.Д. Оптимальное планирование эксперимента с использованием генетических алгоритмов / Н.Д. Кошевой, Е.А. Сухобрус // Математичне моделювання. – 2013. – № 2(29). – С. 36-40.
3. Кошевой Н. Д. Применение жадного алгоритма для оптимизации многофакторных экспериментов /Н.Д. Кошевой, А.В. Бельмега // Збірник наукових праць Військового інституту Київського національного університету ім. Тараса Шевченка. –К.: ВІКНУ, 2014. – № 47. – С. 29-37.
4. Кошевой Н. Д. Применение алгоритма имитации отжига для оптимизации многофакторных планов эксперимента /Н. Д. Кошевой, А. В. Бельмега // Системи обробки інформації. – 2015. – № 6(131). – С. 103-106.
5. Экспериментальное исследование, моделирование и оптимизация процесса гальванического меднения печатних плат / Н.Д. Кошевой, С.Г. Бестань, Г.К. Кожевников, О.Н. Кошевой, Н.В. Доценко // Математическое моделирование. – 2001 г. – № 1. – С. 28–30.
6. Кошевой Н.Д. Оптимальное планирование эксперимента при исследовании устройства для контроля качества диэлектрических материалов / Н.Д. Кошевой, Е.М. Костенко, А.В. Заболотный // Автоматизированные системы управления и приборы автоматики. - 2009. – № 147. – С. 38 – 42.

REFERENCES:

1. Koshevoy N.D. Optimal'noye po stoimostnym i vremennym zatratam planirovaniye eksperimenta / N.D. Koshevoy, Ye.M. Kostenko. – Poltava: izdatel' Shevchenko R.V., 2013. – 317 s.
2. Koshevoy N.D. Optimal'noye planirovaniye eksperimenta s ispol'zovaniyem geneticheskikh algoritmov /N. D. Koshevoy, Ye. A. Sukhobrus//Matematichne modelyuvannya. – 2013. – № 2(29). – S. 36-40.
3. Koshevoy N.D. Primeneniye zhadnogo algoritma dlya optimizatsii mnogofaktornykh eksperimentov / N.D. Koshevoy, A.V. Bel'mega // Zbírnik naukovikh prats' Víys'kovogo ínstitutu Kiívs'kogo natsíonal'nogo uníversitetu ím. Tarasa Shevchenka. – 2014. – № 47. – S. 29-37.
4. Koshevoy N.D. Primeneniye algoritma imitatsii otzhiga dlya optimizatsii mnogofaktornykh planov eksperimenta / ND. Koshevoy, A.V. Bel'mega //Sistemi obrobki ínformatsíí. – 2015. – № 6(131). – S. 103-106.
5. Eksperimental'noye issledovaniye, modelirovaniye i optimizatsiya protsessa gal'vanicheskogo medneniya pechatnikh plat / N.D. Koshevoy, S.G. Bestan', G.K. Kozhevnikov, O.N. Koshevoy, N.V. Dotsenko // Matematicheskoye modelirovaniye, 2001 g. – № 1. – S. 28–30.
6. Koshevoy N.D. Optimal'noye planirovaniye eksperimenta pri issledovanii ustroystva dlya kontrolya kachestva dielektricheskikh materialov / N.D. Koshevoy, Ye. M. Kostenko, A.V. Zabolotnyy // Avtomatizirovannyye sistemy upravleniya i pribory avtomatiki, 2009. – № 147. – S. 38-42.

Рецензент: д.т.н., проф. Угрюмов М. Л., профессор кафедры информатики Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ»

д.т.н., проф. Кошовий М.Д., Стадник А.С.

ОПТИМАЛЬНЕ ПЛАНУВАННЯ ЕКСПЕРИМЕНТУ В УМОВАХ ОБМЕЖЕНИХ РЕСУРСІВ

Досліджено властивості комбінаторних планів багатофакторного експерименту. Розроблено алгоритм оптимізації за вартісними (часовими) витратами багатофакторних планів експерименту з використанням методу вкладених розбиттів і програмне забезпечення для його реалізації, що базуються на перестановці стовпців матриці планування експерименту. Показана його ефективність в порівнянні з методами аналізу перестановок, випадкового пошуку, класичного і клітинного генетичних алгоритмів. Ефективність використання даного алгоритму показана на прикладах технологічних процесів оптимізації параметрів нерівномірності покриття провідників гальванічним осадом і точності пристрою для контроля

якості діелектричних матеріалів. Працездатність алгоритму на основі методу вкладених розбиттів підтверджується наближенням оптимальних планів, отриманих цим методом і методом перестановки рядків матриці планування.

Ключові слова: метод вкладених розбиттів, планування експерименту, оптимальний план, швидкодія.

prof. Koshevoy N.D., Stadnik A.S.

OPTIMAL PLANNING EXPERIMENTS IN CONDITIONS OF LIMITED RESOURCES

Properties of experiment combinatorial plans are investigated. The methods and program optimization multifactor experimental in cost (timing) designs by means method of embedded partitions are developed and software for its implementation, based on the permutation matrix column experiment planning. Its effectiveness in comparison with the methods of analysis permutations, random search of classic and cellular genetic algorithms of optimization for multifactor experimental designs is shown. The effectiveness of this method is demonstrated on the examples the optimization of the parameters of the uneven coating of conductors by galvanic precipitates and precision of the device to control the quality of dielectric materials. The efficiency of the algorithm of embedded partitions approach confirmed plans obtained by this method and and the method of row permutation of planning matrix.

Keywords: method of embedded partitions, experimental design, optimal plan time spent, speed.

УДК 004.056.5

к.військ.н. **Нікіфоров М.М.** (ВІКНУ)
к. політ.н. **Турченко Ю.В.** (ВІКНУ)

ЗАХИСТ ВІД ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ ЯК СКЛАДОВА ЧАСТИНА МОРАЛЬНО-ПСИХОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ В ЗОНІ АТО

У статті визначені основні чинники, які негативно впливають на військовослужбовців Збройних Сил України під час виконання бойових завдань в зоні Антитерористичної операції (АТО). Розглянуто основні заходи протидії інформаційній агресії під час виконання бойових завдань. Визначено, що ефективність вирішення завдань щодо захисту особового складу від інформаційно-психологічної впливу супротивника повністю залежить від особливостей психологічних операцій супротивника; закономірностей сприйняття військовослужбовцями інформації; існуючого морально-психологічного стану військ. Визначено групи чинників, що впливають на ефективність виконання службово-бойових завдань в зоні АТО.

Ключові слова: інформаційно-психологічний вплив, чинники, АТО, особовий склад, психологічна операція, інформаційна війна.

Вступ та постановка задач. Сучасна війна стає війною на ураження та руйнування свідомості супротивника, та консолідацію свідомості власного народу. Як

вказують американські військові експерти, інформаційна війна складається з дій, які здійснюються з метою досягнення інформаційної переваги у забезпеченні національної військової стратегії шляхом впливу на інформацію та інформаційні системи супротивника з одночасним зміцненням і захистом власної інформації, інформаційних систем та інфраструктури.

Нині у багатьох арміях зарубіжних держав склалися і успішно розвиваються потужні структури інформаційно-психологічної дії, основним принципом діяльності яких є девіз: "Деморалізований ворог кращий за вбитого" [6]. Вважається, що в результаті ретельно підготовленої та ефективно проведеної спеціальної інформаційно-психологічної операції, солдат супротивника не лише не здатний вчинити належного опору, він втрачає будь-яку мотивацію до битви, потрапляючи в стан безнадійності, відчаю, апатії, паніки та повної недієздатності, тим самим негативно впливаючи на військовий колектив [6, 7].

Аналіз літератури. Інформаційним війнам присвячено дослідження Мартіна Лібікі. Однією із форм інформаційної війни він називає психологічну. Завдання інформаційної війни, на погляд науковця, – це знищення не фізичної сили, а соціуму [2]. На думку Г. Почепцова, інформаційна цивілізація не сприймає дій у фізичному просторі, перемогу вона вбачає в інформаційному і віртуальному просторах [3].

Під інформаційною війною в контексті публікації розуміється форма протиборства між суб'єктами інформаційної боротьби (державами, блоками тощо) з використанням засобів масової інформації, комп'ютерних мереж тощо, метою якої є інформаційне психологічний вплив (ІПВ) на населення, органи державної влади та складові сектора безпеки та оборони для формування відповідної суспільної думки, підриву морального духу як усього суспільства, так і окремих його інституцій [6].

Незважаючи на досить велику кількість досліджень та публікацій на тему щодо визначення заходів захисту від інформаційно-психологічного впливу супротивника ефективність вирішення завдань щодо захисту особового складу ЗСУ залежить від закономірностей сприйняття військовослужбовцями інформації; реального морально-психологічного стану військ тощо.

Сучасна війна дедалі більшою мірою стає війною на ураження та руйнування свідомості противника та консолідацію свідомості власного народу. На жаль, Україна стала об'єктом організованого інформаційного впливу з боку Російської Федерації. Отже, саме зараз актуальним є питання виявлення та протидії інформаційно-психологічного впливу. Аналіз ведення локальних війн і збройних конфліктів останнього десятиліття наглядно демонструє, що протиборство у військовій сфері дедалі частіше переміщується у віртуальний простір – тобто, інформаційний [6, 7, 8].

Інформаційна війна реалізує асиметричні рішення та передбачає проведення заходів, спрямованих проти систем управління, комп'ютерних та інформаційних мереж і систем. Деструктивний вплив на системи управління досягається також шляхом проведення інформаційно-психологічних операцій (ІПО), які спрямовані проти персоналу та осіб, котрі приймають рішення, і впливають на їхню моральну стійкість, емоції та мотиви прийняття рішень, виконання заходів з оперативної безпеки, дезінформації та фізичного руйнування об'єктів інфраструктури.

Метою статті є визначення основних заходи протидії інформаційній агресії під час виконання службово-бойових завдань в зоні АТО.

Виклад основного матеріалу. На сьогодні можна впевнено стверджувати, що під інформаційно-психологічний вплив підпадає більша частина населення України, яке поділяється на тих, хто стає безпосереднім суб'єктом комбінованого ІПВ та має власний негативний досвід (бійці АТО, члени родин бійців, родичі загиблих бійців, військовополонені, заручники та їх родичі, тимчасово переміщені особи, родичі біженців, що їх приймають, населення, що проживає на територіях бойових дій, медичні працівники, що

надають допомогу пораненим, волонтери), та усіх інших - суб'єктів класичного ІПВ через опосередковані інформаційні потоки [1].

Слід зазначити, що до кола найбільш актуальних проблем інформаційно-психологічного протидії належить захист військ (сил) від інформаційно-психологічної дії супротивника, який включає:

- виховання у особового складу пильності, неприйнятності до ворожої ідеології;
- протидія поширенню та сприйняття особовим складом підривної інформації;
- захист систем зв'язку, комунікацій і управління; перекриття каналів проникнення супротивника в інформаційні мережі, ресурси;
- викриття і роз'яснення воїнам підступних задумів агресорів, цілей і завдань, способів і прийомів ведення їм інформаційно-психологічної боротьби;
- припинення неправдивих чуток, панічних настроїв і профілактика різних фобій серед особового складу частин і підрозділів, що беруть участь у АТО.

Захист військ (сил) від інформаційно-психологічної дії супротивника є комплексом погоджених по завданнях, місцю та часу заходів, що проводяться в мирний та військовий час командирами, штабами і органами виховної роботи по відвертанню, зриву, нейтралізації (послабленню) і усуненню наслідків негативної інформаційно-психологічної дії на військовослужбовців та населення країни [2].

Основними цілями захисту військ (сил) від інформаційно-психологічного впливу супротивника є зниження небезпеки негативного інформаційного і психологічного впливу на командирів (начальників) і особовий склад; забезпечення ефективного управління частинами і підрозділами; зміцнення морально-психологічного стану особового складу військ (сил). Іншими словами мета захисту полягає в зриві цілей і заходів інформаційно-психологічної боротьби, що ведеться силами і засобами супротивника, відвертанні деморалізації і підтримка морально-психологічної стійкості особового складу військ (сил) у бойових умовах [2].

Зважаючи на викладені вище проблеми забезпечення інформаційної протидії, захист від негативного інформаційно-психологічного впливу передбачає виконання завдань, щодо зниження схильності військовослужбовців до дії супротивника

На даний час є актуальним питання виявлення інформаційно-психологічного впливу та протидії йому. Об'єктами ІПВ на військовослужбовців, що перебивають в зоні АТО є:

1. Населення, що мешкає в зоні АТО;
2. Особовий склад військ (сил), залучених до проведення АТО;
3. Незаконні збройні формування та особовий склад Збройних сил Російської Федерації, які перебувають у зоні АТО.

Інформаційно-психологічний вплив на особовий склад військ (сил), який готується до участі в АТО, має здійснюватися за напрямами морально-психологічного забезпечення бойових дій. При цьому основна увага повинна приділятися психологічній готовності до участі в бойових діях.

Українські дослідники вважають, що на особовий склад Збройних Сил України під час виконання службових завдань в зоні АТО діють наступні групи чинників:

1. Соціологічні або "зовнішні": довготривалі (соціально-економічні, політичні та ін. умови в суспільстві) і ситуативні (привід, час, місце, кількість присутніх тощо).
2. Соціально-психологічні або "проміжні" (соціально-психологічні механізми залучення, емоційного зараження, навіювання, наслідування, групової псевдо творчості, групової могутності та ідентифікації, які опосередковують вплив "зовнішніх" чинників на поведінку індивідів і поступово приводять до трансформації в психічному стані кожного з них).
3. Індивідуально-психологічні або "внутрішні" (особливості, що підвищують сприйняття до впливу в оточенні подібних до себе: недостатня пластичність процесів

мислення, підвищена емоційна збудливість, імпульсивність, нестача соціального досвіду, тощо).

4. Інформаційні (надання упередженої інформації за допомогою засобів масової інформації.)

5. Психологічні (вплив на складові психіки військовослужбовців).

6. Психогенними чинниками, що впливають на ефективність службової діяльності військовослужбовців є: висока невизначеність оперативної ситуації, що змушує бути готовим до швидкої зміни наявного алгоритму діяльності; афективні реакції військовослужбовців на будь-які негативні прояви з боку громадян у ході службово-бойової діяльності; дефіцит часу; раптовість; швидкий темп дій; небезпека[10].

Тобто, зазначені інформаційно-психологічні чинники, суттєво погіршують якість виконання службових завдань в зоні АТО. Нейтралізація їх неможлива без уточнення класифікації форм та методів впливу, викриття замислу, змісту та цілей інформаційно-психологічної дії на ЗС України.

Важлива особливість інформаційно-психологічних впливів на індивідуальну свідомість полягає у тому, що вони, як загрози, можуть не бути усвідомлені самою людиною.

Деякі фахівці у сфері інформаційної протидії стверджують, що ІПВ на індивідуальну свідомість можуть призвести до двох видів взаємозалежних змін: [3].

По-перше, це зміни психіки, психічного здоров'я людини. Оскільки в разі інформаційних впливів важко говорити про межі норми та патології. Показником змін може бути втрата адекватності відображення світу у свідомості, а отже і зміна у ставленні до світу.

По-друге, це зрушення в цінностях, життєвих позиціях, орієнтирах, світогляді особистості. Такі зміни обумовлюють прояви девіантної антисоціальної поведінки та становлять небезпеку вже для суспільства і держави.

У сучасних умовах інформаційно-психологічного протиборства протидія засобам інформаційно-психологічної війни повинна здійснюватися постійно і безперервно. З метою підвищення ефективності захисту особового складу підрозділу (частини) від інформаційно-психологічної дії супротивника необхідно застосовувати системний, комплексний підхід. Він передбачає:

По-перше, на основі постійного аналізу військово-політичної, соціально-економічної і інформаційно-психологічної обстановки, що складається, в районі дислокації військ, прогнозувати характер, рівень і динаміку зміни зовнішніх і внутрішніх загроз інформаційно-психологічної безпеки.

По-друге, організовувати повсякденну життєдіяльність особового складу підрозділів і частин, по можливості з максимальним пригніченням джерел негативної інформації, небезпечних з точки зору деструктивного впливу на свідомість і поведінку військовослужбовців (чи зниження їх впливу до мінімуму).

По-третє, вживати енергійні заходи контрпропагандистського характеру з метою активної протидії негативному інформаційно-психологічному впливу супротивника.

По-четверте, важливим інструментом захисту особового складу від негативного інформаційне-психологічного впливу є організація тісної взаємодії органів військового управління із засобами масової інформації, громадськими, міжетнічними, релігійними організаціями та об'єднаннями [8].

Зважаючи на прийняту у світі інформаційну практику роботи, що дозволяє підтримувати престиж армії і захищати її інтереси, слід наголосити, що, система організації захисту особового складу підрозділу (частини) від інформаційно-психологічної дії супротивника включає наступні основні напрями діяльності [8]:

1. Прогнозування інформаційно-психологічної дії супротивника на особовий склад підрозділу (частини);

2. Попередження (профілактика) щодо інформаційно-психологічного впливу супротивника;

3. Зрив інформаційно-психологічної дії супротивника на особовий склад підрозділу (частини);

4. Ліквідація наслідків інформаційно-психологічної дії супротивника.

Таким чином, від кваліфікованої та цілеспрямованої діяльності командирів, штабів, органів по роботі з особовим складом і інших посадовців по захисту військ від інформаційно-психологічної дії супротивника значною мірою залежить хід та результат бойових дій та вирішення наступних завдань:

1. Збір і узагальнення даних про джерела негативної інформаційно-психологічної дії на особовий склад з виробленням конкретних заходів по їх нейтралізації;

2. Нейтралізація інформаційно-психологічної дії супротивника, недопущення деморалізації, морально-психологічного пригнічення військ;

3. Підтримка морально-психологічного стану особового складу на рівні, необхідному для успішного ведення операцій (бойових дій);

4. Проведення інформаційно-психологічних заходів, спрямованих на свої війська і місцеве населення з метою захисту від негативної інформаційно-психологічної дії супротивника;

5. Профілактика поширення неправдивих чуток серед особового складу, попередження масових негативних психічних реакцій;

6. Припинення чуток, тривожних висловлювань, протиправних дій і недопущення деморалізації, дезінформації і зниження морально-психологічного стану військ.

Тобто, робота щодо протидії психологічним диверсіям супротивника у залежатиме від того, наскільки буде можливим реалізувати принцип попередження, та емоційної насиченості заходів, що проводяться. Тобто результати протидії визначатимуться тим, якою мірою командири, помічники по роботі з особовим складом, психологи врахують закономірності функціонування психіки воїна у бойовій ситуації.

Для вирішення зазначених завдань використовується алгоритм дій, який складається з наступних етапів:

1. Негайна доповідь вищому командуванню про наявність інформаційно-психологічної впливу супротивника на особовий склад.

2. Оцінка психологичної та інформаційної ситуації в районі дії частин (підрозділів).

3. Проведення розрахунку сил та засобів.

4. Оцінка обстановки та визначення джерела впливу на особовий склад та місцеве населення;

5. На підставі визначеної сутуації, проведеного розрахунку сил та засобів, сформулювати основні заходи щодо зриву та ліквідації наслідків інформаційно-психологічної впливу супротивника на особовий склад.

6. Проаналізувати причини інформаційно-психологічного зараження особового складу підрозділу.

7. Доповісти старшому начальнику про виконання заходів щодо зриву та ліквідації наслідків інформаційно-психологічної впливу супротивника.

Ефективність цих дій посадових осіб підрозділів (частин) щодо захисту особового складу від інформаційно-психологічної впливу супротивника багато в чому визначатиметься системністю, усебічною узгодженістю і безперервністю проведення заходів. Успіх цієї роботи залежатиме від прогнозування, планування та здійснення з урахуванням особливостей психологічних операцій супротивника, реального морально-психологічного стану військ і військово-політичної, соціально-економічної і інформаційно-психологічної обстановки, що складається в зоні АТО.

При роботі з особовим складом Збройних Сил України надзвичайно дієвим методом у системі інформаційне-психологічної протидії визнається інформування та критичне ставлення до інформації [4]. Звісно, про користь здатності критичного сприйняття

інформації, як засобу протидії ІПВ, зазначав Й. Геббельс, який наголошував, що “найгірший ворог будь-якої пропаганди — інтелектуалізм” [5].

Таким чином, ефективність рішення завдань по захисту особового складу від інформаційно-психологічної впливу супротивника залежить від складу особливостей психологічних операцій супротивника і закономірностей сприйняття військовослужбовцями інформації; реального морально-психологічного стану військ та ситуації в зоні АТО. Використання нових інформаційно-психологічних технологій впливу на індивідуальну та масову свідомість в сучасній війні дозволяє визначити необхідні і ефективні заходи протидії інформаційно-психологічним заходам супротивника, спрямованих на підрив морально-психологічного стану військ, дезінформацію і деморалізацію особового складу, дезорганізацію його бойової діяльності.

Отже, протидія інформаційно-психологічному впливу є системою погоджених і взаємозв'язаних по цілям, завданням, об'єктам та часу інформаційно-психологічних і оперативно-профілактичних заходів.

Таким чином, забезпечення інформаційної безпеки органів і військ в зоні АТО, захист особового складу від психологічних операцій супротивника є важливою складовою частиною морально-психологічного забезпечення службової діяльності в зоні АТО.

Ефективність роботи по захисту особового складу підрозділів (частин) від інформаційно-психологічної дії супротивника залежатиме від того, наскільки вдасться командуванню реалізувати принципи попередження, дохідливості і емоційної насиченості заходів, що проводяться.

З метою підвищення якості захищеності особового складу від інформаційно-психологічних дії супротивника необхідно враховувати закономірності функціонування психіки військовослужбовця, особливості її прояву у бойовій ситуації. Отже, особливу увагу слід приділяти своєчасному роз'ясненню особовому складу підрозділів (частин) справжніх цілей і завдань, змісту тематики і її спрямованості, методів, прийомів і технічних засобів, часу і місця можливого здійснення інформаційно-психологічних акцій супротивником.

Висновки

1. Таким чином, захист від інформаційно-психологічної впливу супротивника повинен здійснюватися постійно як в зоні АТО, так і на всій території країни. Слід зазначити, що безпека морального духу військ в XXI столітті багато в чому залежатиме від безпеки інформаційно-психологічного середовища суспільства, психологічної безпеки військовослужбовців.

2. Визначено групи чинників, що впливають на ефективність службової діяльності військовослужбовців це: соціологічні, соціально-психологічні або “проміжні”, індивідуально-психологічні або “внутрішні”, інформаційні (надання упередженої інформації за допомогою засобів масової інформації), психологічні, психогенні чинники.

3. Ефективність вирішення завдань щодо захисту особового складу від інформаційно-психологічної впливу супротивника повністю залежить від складу особливостей психологічних операцій супротивника та закономірностей сприйняття військовослужбовцями інформації; реального морально-психологічного стану військ та ситуації в зоні АТО.

ЛІТЕРАТУРА:

1. Діагностика, терапія та профілактика медико-психологічних наслідків бойових дій в сучасних умовах: методичні рекомендації (147.14/258.14) / П.В. Волошин, Н.О. Марута, Л.Ф. Шестопалова [та ін.]. − Х., 2014. − 79 с.

2. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / В. Г. Крысько [под общ. ред. А. Е. Тараса]. − Мн.: Харвест, 1999. − 448 с.

3. Зелинский С. А. Информационно-психологическое воздействие на массовое сознание / С.А. Зелинский. – СПб.: Издательско-Торговый Дом «СКИФИЯ», 2008

4. Методичні матеріали з воєнно-ідеологічної підготовки особового складу Збройних Сил України на 2015 навчальний рік [Електронний ресурс]. − Режим доступу : mil.univ.kiev.ua/ files/67_1074163600.doc − Назва з екрана.

5. Остроухов В.В. Інформаційне протиборство в історії людства / В. В. Остроухов / В кн. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: навч. посібн. /В. М. Петрик, О. А. Штоквиш, В. В. Кальниш [та ін.]. − К.: Росава, 2006. − С. 7 −20.

6. Дубина А.М. Інформаційно-психологічні війни і їх вплив на масову свідомість / А. М. Дубина. − К.: НТУУ «КПІ», 2011. − 57 с.

7. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу / В. Горбулін // Дзеркало тижня − Україна. − 2015. − № 2 (24 січня). − С. 3.

8. Шевчук П. Інформаційно-психологічна війна Росії протии України: як їй протидіяти / П. Шевчук // Науковий вісник «Демократичнее самоврядування». − 2014. − Вип. 13. − С. 1 −11.

REFERENCES

1. Diahnostyka, terapiya ta profilaktyka medyko-psykholohichnykh naslidkiv boyovykh diy v suchasnykh umovakh : metodychni rekomendatsiyi (147.14/258.14. − Kh., 2014, 79 p. (In Ukrainian).

2. Krыs'ko V. H. (1999). Sekretы psykholohycheskoy voynы (tsely, zadachy, metodы, formы, opыt). − Mn.: Kharvest, 1999, 448 p. (In Belarus).

3. Zelynskyy S. A. (2008). Ynformatsyonno-psykholohycheskoe vozdeystvye na massovoe soznanye / S.A. Zelynskyy. – SPb.: Yzdatel'sko-Torhovыy Dom «SKYFYYa», 2008(In Russian).

4. Metodychni materialy z voyenno-ideolohichnoyi pidhotovky osobovoho skladu Zbroynykh Syl Ukrayiny na 2015 navchal'nyy rik [Elektronnyy resurs]. − Rezhym dostupu : mil.univ.kiev.ua/ files/67_1074163600.doc − Nazva z ekrana. (In Ukrainian).

5. Ostroukhov V.V. (2006). Informatsiyne protyborstvo v istoriyi lyudstva. − K.: Rosava, 2006, 7-20p. (In Ukrainian).

6. Dubyna A. M. (2011). Informatsiyno-psykholohichni viyny i yikh vplyv na masovu svidomist'. − K.: NTUU «KPI», 2011, 57 p. (In Ukrainian).

7. Horbulin V. (2015). «Hibrydna viyna» yak klyuchovyy instrument rosiys'koyi heostratehiyi revanshu.: Ukrayina, 2015, 3 p. (In Ukrainian).

8. Shevchuk P. (2014). Informatsiyno-psykholohichna viyna Rosiyi protyy Ukrayiny: yak yiy protydiyaty, 2014, 1−11 p. (In Ukrainian).

Рецензент: к.т.н., доц. Пампуха І.В., начальник відділу – заступник начальника науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка

к.воен.н. Никифоров Н.Н., к. полит.н.Турченко Ю.В.

ЗАЩИТА ОТ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ КАК СОСТАВЛЯЮЩАЯ ЧАСТЬ МОРАЛЬНО-ПСИХОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ СЛУЖЕБНО-БОЕВЫХ ЗАДАЧ В ЗОНЕ АТО

В статье определены основные факторы, которые негативно влияют на военнослужащих Вооруженных Сил Украины во время выполнения боевых задач в зоне Антитеррористической операции (АТО). Рассмотрены основные меры противодействия информационной агрессии во время выполнения боевых задач. Определено, что эффективность решения задач по защите личного состава от информационно-психологического влияния противника полностью зависит от особенностей психологических операций противника; закономерностей восприятия военнослужащими информации; существующего морально-психологического состояния войск. Определены группы факторов, влияющих на эффективность выполнения служебно-боевых задач в зоне АТО.

Ключевые слова: информационно-психологическое воздействие, факторы, АТО, личный состав, психологическая операция, информационная война.

Ph.D. Nikiforov M.M., Ph.D. Turchenko Yu.V.

INFORMATION AND PSYCHOLOGICAL EFFECTS PROTECTION AS PART OF THE PSYCHOLOGICAL AND MORAL SUPPORT OF THE SERVICE AND COMBAT MISSION IN THE ATO AREA

Authors have defined the main factors negatively affecting the Armed Forces of Ukraine personnel in the course of combat missions in the anti-terrorist operation (ATO) area. The main information aggression countermeasures in the course of combat missions have been considered. It has been determined that the efficiency of solving problems as to the personnel protection against adversary's information and psychological effects is absolutely dependent on the characteristics of the adversary's psychological operations as well as on the regularities of information perception by servicemen and actual moral and psychological condition of troops. The groups of factors affecting the service and combat mission efficiency in the ATO area have been defined.

Keywords: information and psychological effect, factors, anti-terrorist operation (ATO), personnel, psychological operation, information warfare.

ДАНІ ПРО АВТОРІВ

Апатова Наталія Володимирівна, доктор педагогічних наук, доктор економічних наук, професор, професор кафедри бізнес-інформатики та математичного моделювання Таврійського національного університету імені В.І. Вернадського (м. Сімферополь)

Бабій Ігор Миколайович магістр кафедри комп'ютерних систем та мереж, Хмельницький національний університет (м. Хмельницький)

Бабій Юлія Олександрівна, кандидат технічних наук, викладач кафедри зв'язку, автоматизації та захисту інформації. Національна академія Державної прикордонної служби України імені Богдана Хмельницького Хмельницького (м. Хмельницький)

Бадрук Оксана Олександрівна, науковий співробітник науково-організаційного відділення, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Балицький Ігор Іванович, кандидат технічних наук, доцент, начальник факультету інженерно-технічного забезпечення та технічних засобів охорони кордону, Національна Академія Державної прикордонної служби України імені Богдана Хмельницького Хмельницького (м. Хмельницький)

Білик Олег Михайлович, магістр кафедри кібербезпеки та комп'ютерних систем і мереж, Хмельницький національний університет (м. Хмельницький)

Бойченко Олег Валерійович, доктор технічних наук, професор, професор кафедри бізнес-інформатики та математичного моделювання Таврійського національного університету імені В.І. Вернадського (м. Сімферополь)

Бойчук Вадим Олександрович, кандидат технічних наук, доцент кафедри комп'ютерних систем та мереж, Хмельницький національний університет (м. Хмельницький)

Бригадир Сергій Петрович, ад'юнкт науково організаційного відділу, Військовий інститут телекомунікацій та інформатизацій (м. Київ)

Вавасова О.С., працівник Збройних Сил України, науковий співробітник науково-дослідного відділу наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації (м. Київ)

Василенко Сергій Вікторович, аспірант Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ» (м. Київ)

Горбачевський С.А., науковий співробітник Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України (м. Київ)

Горячева Кіра Сергіївна, кандидат економічних наук, доцент**,** провідний науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Гостєв Володимир Володимирович, кандидат технічних наук, старший науковий співробітник**,** Київський національний університет імені Тараса Шевченка (м. Київ)

Грибок Андрій Олександрович, студент, Київського національного університету імені Тараса Шевченка (м. Київ)

Гришин Сергій Павлович, кандидат технічних наук, начальник науково-методичного відділу (психологічного вивчення особового складу) Науково-методичного центру кадрової політики Міністерства оборони України (м. Київ)

Гуменна Олена Іванівна, завідуюча бібліотекою Хмельницької спеціалізованої загальноосвітньої школи І-ІІІ ступенів №15 імені Олександра Співачука (м. Хмельницький)

Гунченко Юрій Олександрович, доктор технічних наук, доцент, професор кафедри математичного забезпечення комп'ютерних систем, Одеський національний університет імені І.І. Мечникова (м. Одеса)

Гусляков Гліб Володимирович, магістр кафедри кібербезпеки та комп'ютерних систем і мереж, Хмельницький національний університет (м. Хмельницький)

Джулій Володимир Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж, Хмельницький національний університет (м. Хмельницький)

Дячук Андрій Олександрович, кандидат педагогічних наук, доцент, доцент кафедри екології, Хмельницький національний університет (м. Хмельницький)

Жиров Генадій Борисович, кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Коваленко І.Г., кандидат технічних наук, провідний науковий співробітник науково-дослідного відділу наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації (м. Київ)

Козак Іван Віталійович, магістр кафедри кібербезпеки та комп'ютерних систем і мереж, Хмельницький національний університет (м. Хмельницький)

Кольцов Руслан Юрійович, кандидат технічних нук, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Костенко Олена Михайлівна, доктор технічних наук, доцент, доцент кафедри «Процеси, машини та обладнання агропромислового виробництва» Полтавської державної аграрної академії (м. Полтава)

Кошова Ірина Іванівна, аспірант кафедри авіаційних приладів і вимірювань Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» (м. Харків)

Кошовий Микола Дмитрович, доктор технічних наук, професор, завідувач кафедри авіаційних приладів і вимірювань Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» (м. Харків)

Кубявка Микола Богданович, ад'юнкт Військового інституту Київського національного університету імені Тараса Шевченка (м. Київ)

Лєнков Євген Сергійович, кандидат технічних наук, старший науковий співробітник, Військовий інститут телекомунікацій і інформатизації (м. Київ)

Лєнков Сергій Васильович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, начальник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Лисий Микола Іванович, доктор технічних наук, доцент, професор кафедри інженерного забезпечення та технічних засобів охорони кордону, Національна Академія Державної прикордонної служби України імені Богдана Хмельницького (м. Хмельницький)

Лоза Віталій Миколайович, кандидат технічних наук, старший науковий співробітник науково-дослідного центру, Військовий інститут, Київський національний університет імені Тараса Шевченка (м. Київ)

Любарець А.А., кандидат технічних наук, начальник відділу експлуатації, надійності і випробувань державного підприємства "Державне київське конструкторське бюро "Луч", (м. Київ)

Міночкін Дмитро Анатолійович, кандидат технічних наук, старший науковий співробітник, доцент кафедри, Інститут телекомунікаційних систем НТУУ «КПІ» (м. Київ)

Мірошніченко Олег Вікторович, кандидат технічних наук, старший науковий співробітник, начальник відділу наукових методологічних розробок та високих технологій начальника науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка (м. Київ)

Міщенко А.О., провідний науковий співробітник науково-дослідного відділу наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації (м. Київ)

Муляр Ігор Володимирович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж, Хмельницький національний університет (м. Хмельницький)

Мясіщев Олександр Анатолійович, доктор технічних наук, професор, професор кафедри кібербезпеки та комп'ютерних систем і мереж, Хмельницький національний університет (м. Хмельницький)

Нікіфоров Микола Миколайович, кандидат військових наук, старший науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Огнєвий Олександр Вікторович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерних систем і мереж, Хмельницький національний університет (м. Хмельницький)

Осипа Володимир Олександрович, кандидат військовий наук, доцент, старший науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Охрамович Михайло Миколайович, кандидат технічних наук, старший науковий співробітник, старший науковий співробітник науково-дослідного центру, Військовий інститут, Київський національний університет імені Тараса Шевченка (м. Київ)

Пампуха Ігор Володимирович, кандидат технічних наук, доцент, начальник відділу – заступник начальника науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Поліщук Віктор Вікторович, ад'юнкт, Національна Академія Державної прикордонної служби України імені Богдана Хмельницького (м. Хмельницький)

Прокопчук Сергій Олексійович, магістр кафедри кібербезпеки та комп'ютерних систем і мереж, Хмельницький національний університет (м. Хмельницький)

Проценко Ярослав Миколайович, ад'юнкт Військового інституту Київського національного університету імені Тараса Шевченка (м. Київ)

Радзівілов Григорій Данилович, кандидат технічних наук, доцент, начальник кафедри технічного та метрологічного забезпечення факультету інформаційних технологій, Військового інституту телекомунікацій та інформатизацій (м. Київ)

Рома Олександр Миколайович, доктор технічних наук, старший науковий співробітник, професор Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ» (м. Київ)

Романенко Вадим Петрович, кандидат технічних наук, доцент, начальник кафедри теоретичних основ експлуатації засобів спеціального зв'язку, Інститут спеціального зв'язку та захисту інформації, Національного технічного університету України «КПІ» імені І.Сікорського (м. Київ)

Романовська Ірина, магістр кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету (м. Хмельницький)

Ряба Людмила Олександрівна, науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Савков Павло Анатолійович, кандидат технічних наук, доцент, начальник кафедри топогеодезичного забезпечення, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Савкова Валентина Павлівна, кандидат технічних наук, Київський національний університет імені Тараса Шевченка (м. Київ)

Селюков Олександр Васильович, доктор технічних наук, старший науковий співробітник, директор ТОВ «Укрспецконсалтинг» (м. Київ)

Солодєєва Людмила Василівна, науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Киев)

Стадник Анастасія Сергіївна, магістр кафедри «Авіаційні прилади й вимірювання», Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ» (м. Харків)

Тупота Олена Сергіївна, бакалавр кафедри бізнес-інформатики та математичного моделювання Таврійського національного університету імені В.І. Вернадського (м. Сімферополь)

Турченко Юлія Вікторівна, кандидат політичних наук, старший науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Хірх-Ялан Вікторія Ігорівна, кандидат технічних наук, науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Чешун Віктор Миколайович, кандидат технічних наук, доцент кафедри кібербезпеки та комп'ютерних систем і мереж, Хмельницький національний університет (м. Хмельницький)

Шатров А.М., кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник Державного науково-дослідного інституту авіації (м. Київ)

Шевченко Валерій Віталійович, науковий співробітник, науково-дослідний центр, Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ)

Шишанов М.О., доктор технічних наук, професор, провідний науковий співробітник Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України (м. Київ)

Юмашов Вадим Станіславович, магістр кафедри комп'ютерних систем та мереж, Хмельницький національний університет (м. Хмельницький)

АЛФАФІТНИЙ ПОКАЖЧИК

Апатова Н.В. 182
Бабій І.М. 149
Бабій Ю.О. 40
Бадрук О.О. 7
Балицький І.І. 40
Білик О.М. 143
Бойченко О.В. 191
Бойчук В.О. 99
Бригадир С.П. 63
Вавасова О.С. 22
Василенко С.В. 71
Горбачевський С.А. 88
Горячева К.С. 199
Гостєв В.В. 166
Грибок А.О. 205
Гришин С.П. 7
Гуменна О.І. 216
Гунченко Ю.О. 99
Гусляков Г.В. 134
Джулій В.М. 120
Дячук А.О. 223
Жиров Г.Б. 16, 55
Коваленко І.Г. 22
Козак І.В. 107
Кольцов Р.Ю. 114
Костенко Е.М. 33
Кошова І.І. 33
Кошовий Н.Д. 33,230
Кубявка М.Б. 174
Лєнков Є.С. 143
Лєнков С.В. 79,120
Лисий М.І. 40
Лоза В.Н. 50
Любарець А.А. 88
Міночкін Д.А. 128
Мірошніченко О.В. 7
Міщенко А.О. 22
Муляр І.В. 134,216
Мясіщев О.А. 143
Нікіфоров М.М. 55,235
Огнєвий О.В. 107,149
Осипа В.О. 149
Охрамович М.М. 79
Пампуха І.В. 55,166
Поліщук В.В. 38
Прокопчук С.О. 79
Проценко Я.М. 94
Радзівілов Г.Д. 63
Рома О.М. 71
Романенко В.П. 63
Романовська І.А. 120
Ряба Л.О. 216
Савков П.А. 166
Савкова В.П. 166
Селюков О.В. 149
Солодєєва Л.В. 134
Стадник А.С. 230
Тупота Е.С. 191
Турченко Ю.В. 235
Хірх-Ялан В.І. 157
Чешун В.М. 79
Шатров А.М. 88
Шевченко В.В. 79
Шишанов М.О. 88
Юмашов В.С. 99

Шановні автори!

Хочемо повідомити, що наш «Збірник наукових праць ВІКНУ» пройшов переатестацію (Наказ МОН України від 16.05.2016 № 515) і його відновлено у переліку наукових фахових видань із технічних наук, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук. Також «Збірнику…» присвоєно ISSN.

Для представлення «Збірника…» в науко-метричних базах даних Web of Science (Thomson Reuters), Scopus (Elsevier), Гугл Академія (Google Scholar) необхідно дотримуватись ряду додаткових вимог в оформленні статей, продиктованих обов'язковими вимогами світових реферативних баз даних.

1. РОЗШИРЕНА АНОТАЦІЯ трьома мовами: українською, російською, англійською (***обсяг 800-1000 знаків без урахування пробілів***).

При перекладі анотації на російську та англійську мови заборонено використовувати онлайн-перекладач в Інтернеті.

2. ЛІТЕРАТУРА:

Список літератури оформлюється в суворій відповідності з міждержавним стандартом ДСТУ ГОСТ 7.1:2006.

3. REFERENCES

Список літератури (References) для наукометричних БД наводиться повністю окремим блоком, повторюючи список літератури до україно-, російськомовної частини, незалежно від того, є чи немає в ньому іноземні джерела. Якщо в списку є посилання на іноземні публікації, вони повністю повторюються в списку і оформляється таким чином:

всі автори (транслітерацією), переклад назви статті на англійській мові, назва джерела (транслітерацією, якщо джерело не має адекватної англійської назви), вихідні дані з позначеннями на англійській мові, або тільки цифрові. Наприклад:

Zagurenko, A.G., Korotovskikh, V.A., Kolesnikov, A.A., Timonov, A.V., Kardymon, D.V. (2008). Technical and economic optimization of hydrofracturing design. Neftyanoe khozyaistvo [Oil Industry], no. 11, pp. 54-57 (In Russian).

Для транслітерації латиницею російськомовних і україномовних текстів можна скористатися програмою на сайті: http://translit.net/ua та http://ukraine.velesava.com/?p=255.

Транслітерувати інформацію потрібно згідно постанові КМУ від 27.01.2010 №55 (http://zakon2.rada.gov.ua/laws/show/55-2010-%D0%BF).

ЗРАЗОК



ЗРАЗОК

1. Hubers'kyj, L., Kamins'kyj, Y., Makarenko, Y. (2007). Informatsijna polityka Ukrainy: Yevropejs'kyj kontekst.[Information Policy of Ukraine: European context], Kyiv, Lybid', 358 p. (In Ukrainian).

2. Kvietnyj, R., Kompanets', M., Kryvohubchenko, S., Kulyk, A. (2002). Osnovy tekhniky peredavannia informatsii. [Fundamentals of technology information transfer], Vinnytsia, UNIVERSUM, 157p.

4. ФОРМУЛИ. Для коректної верстки статей, будь ласка, набирайте формули в редакторі формул. Інтеграція формул в текст статті як графічний об'єкт не припустима!

Офіційна веб-сторінка журналу: http://miljournals.knu.ua/

Наукове видання

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Військового інституту

Київського національного університету імені Тараса Шевченка

Випуск № 54

(Усі матеріали надруковані в авторській редакції)

Підписано до друку 16.12.16 р.
Авт. друк. Арк. 18. Формат 60х90/8
Безкоштовно. Замовлення № 10-2012

Надруковано у навчальному картографічному комплексі ВІКНУ

03680, Київ, вул. Ломоносова 81

т. 521-32-89