Міжнародна науково-практична конференція

“Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку”

17 березня 2020 року, м. Харків

Міжнародна науково-практична конференція “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” / Збірник тез доповідей (м. Харків, 17 березня 2020 р.). – Харків. – 2020. – 212 с.

Тези доповідей опубліковано в авторській редакції, мовою оригіналу: **http://kinf.nangu.edu.ua**

Відповідальність за фактичні помилки, зміст і достовірність інформації та точність викладених фактів несуть автори.

Міністерство внутрішніх справ України
Національна академія Національної гвардії України

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Міжнародна науково-практична конференція

“Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку”

17 березня 2020 року

м. Харків

Організатори конференції:
Національна академія Національної гвардії України, м. Харків,
Харківський національний університет радіоелектроніки.

Організаційний комітет конференції:

Голова – Іохов О. Ю., доктор технічних наук, с.н.с., доцент, начальник кафедри військового зв'язку та інформатизації Національній академії Національної гвардії України (+38097-69-81-250).

Заступник голови – Малюк В. Г., кандидат технічних наук, доцент, професор кафедри військового зв'язку та інформатизації Національній академії Національної гвардії України.

Відповідальний секретар – Новикова О. О., кандидат технічних наук, доцент кафедри військового зв'язку та інформатизації Національної академії Національної гвардії України.

Члени організаційного комітету:

Соколовський С. А. – кандидат технічних наук, доцент, начальник Національної академії Національної гвардії України;

Морозов О. О. – доктор технічних наук, професор, перший заступник начальника з навчально-методичної та наукової роботи Національної академії Національної гвардії України;

Семенець В. В. – доктор технічних наук, професор, ректор Харківського національного університету радіоелектроніки;

Железко Б. О. (Железко Б. А.) – кандидат технічних наук, доцент, доцент кафедри економічної інформатики Білоруського державного економічного університету, м. Мінськ, Республіка Білорусь;

Красовський Є. (Krasowski E.) – доктор наук, професор, керівник секції відділу Польскої академії наук, м. Люблін, Польща;

Собчук Г. (Sobczuk H.) – доктор наук, професор, директор представництва Польскої академії наук, м. Київ;

Кобзєв В. Г. – кандидат технічних наук, с.н.с., доцент кафедри прикладної математики Харківського національного університету радіоелектроніки;

Козлов В. Є. – кандидат технічних наук, доцент, доцент кафедри військового зв'язку та інформатизації Національної академії Національної гвардії України.

Адреса організаційного комітету: 61001, м. Харків, майдан Захисників України, 3, Національна академія Національної гвардії України, науково-організаційний відділ.
Телефон: +38097-69-81-250.
Електронна адреса: nanguki@ukr.net.

УДК 351.741:[621.397.4+004]

Коршенко В. А.

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ – ПРИХОВАНІ ЗАГРОЗИ

Останнім часом використання інтелектуальних систем відеоспостереження в правоохоронній діяльності стало трендом. Кількість камер, які використовують як правоохоронні органи так і комерційні організації збільшується з кожним днем. Застарілі аналогові камери замінюються сучасними цифровими. Значно збільшилася кількість камер відеоспостереження на дорогах, в громадських місцях, в організаціях і закладах всіх форм власності.

Упровадження сучасних інтелектуальних системи відеоспостереження дає можливість значно підвищити ефективність роботи правоохоронних органів. МВС України, реалізуючи свої першочергові завдання із забезпечення безпеки громадян, дотримання прав людини, охорони громадського порядку, попередження терористичних актів, виступає з ініціативою облаштування автошляхів та громадських місць системами інтелектуального відеоспостереження [1].

Здавалось би від цього суспільство та держава в цілому отримає тільки вигоду. Однак ця тенденція несе дуже серйозні потенційні загрози, які потрібно вивчати та попереджувати. Основа проблеми полягає в самій технології. Кожна сучасна цифрова камера, для виконання своїх функцій повинна бути оздоблена власним процесором та пам'яттю що перетворює її на мікрокомп'ютер. З розвитком технологій ці мікрокомп'ютери стають дедалі потужнішими, обладнуються телекомунікаційними модулями, що надає їм можливість отримувати, обробляти та передавати інформацію. Це, в свою чергу, надає можливість злочинцям атакувати і компрометувати як окремі відеокамери так і інтелектуальні системи відеоспостереження в цілому. Адже бізнес-моделі багатьох виробників цифрових відеокамер не передбачають того рівню безпеки, який розповсюджується на традиційні інтернет пристрої (комп'ютери, маршрутизатори тощо). Бюджетні виробники цифрових камер взагалі не мають ані досвіду ані стимулу підтримувати достатній рівень безпеки своєї продукції. Наявність в системах відеоспостереження вразливостей та «бекдорів» підтверджений факт. Наприклад в 2016 році дослідники з компанії Sucuri виявили ботнет із 25000 пристроїв для відеоспостереження. В 2017 році експерти компанії Positive Technologies знайшли цілий ряд критичних вразливостей в системах відеоспостереження Samsung та у популярній прошивці DVR-систем, яка використовується багатьма виробниками цифрових камер і нарахували більш ніж 100000 шт. скомпрометованих відеокамер в мережі інтернет. В 2019 році тільки хробаком BASHLITE було заражено більше ніж 1 мільйон пристроїв відеоспостереження. Зловмисники сформували з них ботнети та проводили DDoS атаки [2].

Брюс Шнайер, консультант з безпеки, який досліджує так звані «дірки» в інтернеті речей та описує їх, у своїй книзі «Натисніть сюди, щоб вбити усіх» зазначає, що він не налаштований цілком песимістично, але тут складно зберігати спокій, адже економічні та технічні цілі індустрії інтернету речей, не відповідають тим заходам безпеки які необхідні для забезпечення конфіденційності суспільства. Вбудувавши комп'ютер у звичні нам речі, компанії перетворюють весь світ у суцільну загрозу [3]. І з ним не можна не погодитись, адже погана безпека несе в собі як ризики витоку даних так і можливість зміни та перетворення інформації. Отримавши незаконний доступ до цифрової відеокамери злочинець може отримати доступ до інформації про її місце знаходження, фотографій, відеозаписів, метаданих, та можливість знищення або спотворення зазначених даних. Також, використовуючи декілька скомпрометованих камер можливо створення ботнетів, проведення ними DDoS атак, незаконного видобутку криптовалюти та ін.

Значна частина цифрових відеокамер, особливо бюджетних, переважно китайського виробництва вже на етапі завантаження на них базового програмного забезпечення ма-

ють серйозні «діри» в безпеці, або містять потенційно небезпечний програмний код. Разом з тим сьогодні існує велика кількість інтернет-ресурсів для пошуку вразливих пристроїв підключених до інтернету і пошук та використання таких вразливостей набуває все більшої популярності між зловмисників які спеціалізуються на злочинах у кіберпросторі та в сфері високих технологій.

Для того щоб досягти безпеки при використанні інтелектуальних систем відеоспостереження потрібно додержуватись декількох загальних правил:

- не використовувати бюджетні камери маловідомих виробників;
- не використовувати несертифіковане програмне забезпечення;
- ізолювати доступ до систем цифрового відеоспостереження з Інтернету;
- дозволити редагувати налаштування камери тільки з визначених IP адрес (білий список);
- не використовувати стандартні логіни, використовувати складні паролі, не використовувати однакові логіни/паролі на різних камерах;
- проводити регулярне оновлення програмного забезпечення;
- проводити регулярний моніторинг журналів подій як окремих цифрових камер так і системи відеоспостереження в цілому;
- встановити глобальні програмно-технічні комплекси захисту.

Упровадження сучасних інтелектуальних системи відеоспостереження дає можливість значно підвищити ефективність роботи правоохоронних органів, однак ця тенденція несе дуже серйозні потенційні загрози, які потрібно вивчати та попереджувати.

Список використаних джерел

1. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду : методичні матеріали для працівників підрозділів поліції / [уклад. В. А. Коршенко, М. В. Мордвинцев, Ю. В. Гнусов, В. В. Чумак, В. А. Світличний]; Харків. нац. ун-т внутр. справ. – Харків, 2020. – 44 с.

2. Positive Technologies. Уязвимости систем видеонаблюдения позволяют хакерам создавать масштабные ботнеты// Хабр [Електронний ресурс]. – Режим доступу: https://habr.com/ru/company/pt/blog/310548/

3. Bryus Shnayyer. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World// September 2018 W. W. Norton & Company 288 Pages ISBN: 978-0393608885

УДК 353.9+621.32

Орлов М. М., Дятлова Г. Р.

ІНФОРМАЦІЙНА МОДЕЛЬ ЦИРКУЛЯЦІЇ ІНФОРМАЦІЇ В КОНТУРІ ВЗАЄМОДІЇ ВЛАДНИХ СТРУКТУР, ПОЛІТИЧНИХ І ГРОМАДЯНСЬКИХ ОРГАНІЗАЦІЙ

Як відомо, *інформаційна модель* – модель об’єкту, представленого у вигляді потоків інформації, які описують сутність для даного розгляду параметри і змінні величини об’єкту, зв’язок між ними, входи і виходи об’єкту і дозволяючи шляхом подачі на модель інформації про зміни вхідних величин модулювати можливі стани об’єкту (переклад авторів тез) [1]. Інформаційна модель (в широкому, загальнонауковому сенсі) – сукупність інформації, яка характеризує сутність властивостей і стану об’єкту, процесу явища, а також взаємний зв’язок зі зовнішнім світом (із зовнішнім середовищем).

У межах дослідження, розглядається інформаційна модель взаємодії декількох (трьох) організаційних структур.

Взаємодія – узгоджені за метою, завданням, місцем, часом та способом виконання завдань дії певних суб'єктів для досягнення визначеної мети. *Взаємодія* – узгоджені зусилля органів держаної влади та місцевого самоврядування між собою та з взаємодіючими органами (наприклад, органами силових відомств, політичними партіями, громадськими організаціями). Організується за завданнями, місцем і часом в інтересах найбільш ефективного застосування сил та засобів, досягнення високих результатів зазначеній діяльності або за визначеним державницьким завданням [2].

Під *системою взаємодії* владних структур, політичних і громадських організацій в Україні на регіональному рівні розуміється організаційні структури зазначених складових, інформаційні та забезбечуючі зв'язки між ними та склад надсистеми, її повноваження і можливий вплив на організацію та здійснення зазначеної взаємодії. Зазначені складові системи взаємодії мають певні зони дотику і зони впливу, де циркулює інформація різного призначення (рис. 1).

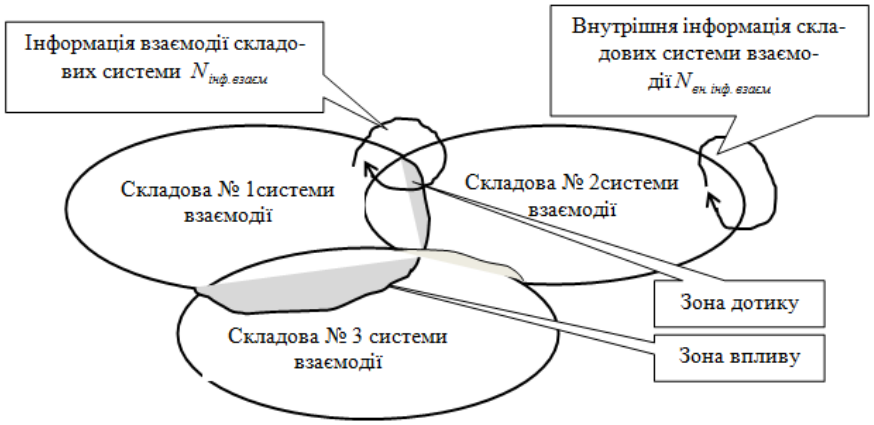


Рисунок 1 - Система взаємодії владних структур, політичних і громадських організацій

Визначення меж та змісту зазначених зон можна за допомогою: 1) теорії розпізнавання об'єктів [3]; 2) теорії імовірностей [4] – тема подальшого дослідження.

Зона дотику вказує за якими функціями суб'єкти взаємодії співпадають. *Зона впливу* вказує за якими функціями один суб'єкт взаємодії впливає на інший. Сутність функцій суб'єктів взаємодії тема окремного дослідження.

У межах зон дотику циркулює інформація взаємодії між складовими (між владними структурами, політичними і громадянськими організаціями) $N_{інф.взаєм}$. Разом з тим, в межах кожної складової циркулює внутрішня інформація $N_{вн.інф.взаєм}$. У цілому в системі взаємодії владних структур, політичних і громадянських організацій циркулює сума інформацій: внутрішньої інформації та інформації взаємодії. Визначення обсягу зазначеної інформації – завдання для управлінців та органів управління владних структур, політичних і громадянських організацій. Від обсягу інформації, що циркулює в межах системи взаємодії, залежить кількість управлінців (посадових осіб органів управління) – в цьому і є сутність інформаційно-структурного методу формування органів управління [5]. Оптимізація складу органів управління суб'єктів взаємодії (скорочення чисельності) вплине на ефективність управління за рахунок скорочення ресурсів системи управління суб'єктів взаємодії.

Список використаних джерел

1. Терехов С. А. Нейросетевые информационные модели сложных инженерных систем // Нейроинформатика / А. Н. Горбань, В. Л. Дунин-Барковский, А. Н. Кирдин и др. – Новосибирск: Наука. Сибирское предприятие РАН, 1998. – 296 с.

2. Орлов М. М. Тлумачний словник-довідник фахівця з менеджменту, маркетингу та публічного адміністрування (підготовлений до видання) / М. М. Орлов. – Х. : ХНУБА, 2019. – 323 с.

3. Дружинин В. В. Введение в теорию конфликтов / В. В. Дружинин, М. Д. Конторов. – М. : Радио и связь, 1989. – 288 с.

4. Корн Г. Справочник по математики: для научных работников и инженеров / Г. Корн, Т. Корн. – М. : Наука, 1968 – 720 с.

5. Орлов М. М. Формування системи взаємодії регіональних органів виконавчої влади у сфері охорони правопорядку (теоретико-методологічні засади) : монографія / М. М. Орлов. – Х. : ХарРІ НАДУ "Магістр", 2012. – 344 с. ISBN 978-966-390-112-1.

УДК 353.9+621.32

Орлов М. М., Резниченко В. В.

КОМПЕТЕНЦІЇ ДЕРЖАВНОГО УПРАВЛІНЦЯ У СФЕРІ ІНФОРМАЦІЙНО-КОМУНІКАТИВНИХ ТЕХНОЛОГІЙ

Державний управлінець – фахівець у таких сферах як: 1) державне управління; 2) публічне адміністрування; 3) електронне урядування; 4) система надання послуг громадянам державі як на центральному, так і на регіональному рівнях тощо. На теперішній час, будь-яка з зазначених сфер прямо або опосередковано використовує інформаційно-комунікаційні технології (ІКТ). Для використання державним управлінцем ІКТ він зобов'язаний мати такі *компетенції* як: 1) здатність розв'язувати складні спеціальні завдання та практичні проблеми у сфері державного (публічного управління та адміністрування) або у процесі навчання, що передбачає застосування теорії та наукових методів відповідної галузі (у томі числі ІКТ) і характеризується комплексністю та невизначеністю умов; 2) здатність до адаптації та дії у новій ситуації (при широкому застосуванні ІКТ); 3) здатність планувати та управляти часом та подіями з використанням сучасних інформаційних технологій; 4) здатність до пошуку, оброблення та аналізу інформації з різних джерел; 5) мати навики міжособистої взаємодії та здійснювати взаємодію з органами різних систем в державі з використанням сучасних технічних засобів оброблення інформації; 6) здатність вчитися і вчити та оволодівати сучасними знаннями, у тому числі у сфері застосування ІКТ; 7) здатність використовувати систему електронного документообігу з використанням сучасних електронних засобів оброблення інформації; 8) здатність використовувати сучасні джерела економічної, соціальної, управлінської, облікової інформації для складання службових документів та аналітичних звітів; 9) здатність поглиблено аналізувати проблеми і явища в одній або декількох професійних сферах з використанням соціально-економічних ризиків та можливих соціально-економічних наслідків тощо.

Зазначений перелік компетенцій певним чином пов'язаний з необхідністю знань державного службовця у сфері ІКТ. Слід зазначити, що такою проблемою в Національній академії державного управління при Президентові України опікаються такі вчені як Машкаров Ю. Г., Кобзев І. В, Орлов О. В. та Мордвінев М. В. [1]. Разом з тим, враховуючи, що ІКТ – уніфікована технологія, яка об'єднує інтегровану телекомунікацію (ліній та каналів різного призначення), комп'ютери, програмне забезпечення, накопичувальні та аудіовізуальні системи, які дозволяють користувачам одержувати доступ, зберігання, передавання та змінювати інформацію [2], слід погодитися, що *напрямами удосконалення компетенцій державного управління* у сфері інформаційно-комунікативних технологій слід вважати: 1) опанування знаннями та навиками щодо застосування ліній та каналів в системі ІКТ; 2) набути здатності використовувати можливості сучасних комп'ютерів та їх програмного забез-

печення; 3) мати здібності використовувати на практиці локальні обчислювальні мережі; 4) знання основ автоматизації опрацювання інформації.

Набуття зазначених компетенцій дозволить державним управлінця: 1) у повній мірі використовувати ІКТ у сфері Електронного урядування; 2) якісно (ефективно – з меншими ресурсними затратами) надавати громадянам держави послуги; 3) бути спроможними використовувати сучасні методи формування системи державного (публічного) управління та їх складових (наприклад, застосування інформаційно-структурного методу формування органів управління різних організаційних структур [3]); 4) мати здатність поглиблено аналізувати проблеми і явища в одній або декількох професійних сферах з використанням соціально-економічних ризиків та можливих соціально-економічних наслідків сучасності.

Список використаних джерел

1. Машкаров Ю. Г. Комп'ютерні мережі та телекомунікації : навч. посіб. / Ю. Г. Машкаров, І.В. Кобзев, О.В. Орлов, М. В. Мордвінев – Х.: ХарРІНАДУ, 2012 – 212 с.

2. Інформаційно-телекомунікаційні технології. Електронний ресурс. Режим доступу: https://uk.wikipedia.org/wiki.

3. Орлов М. М. Інформаційно-структурний метод формування органів державної влади / М. М. Орлов // Глобальне управління: теорія та практика. Збірник наукових праць серії "Україна-Греція". Випуск 1. – Афіни, 2015. – С. 106–114.

Орлов М. М., Літус І. Р.

ІНФОРМАЦІЙНА ОБІЗНАНІСТЬ УПРАВЛІНЦЯ ДЕРЖАВНОГО УПРАВЛІННЯ В СИСТЕМІ ПІСЛЯДИПЛОМНОЇ ОСВІТИ

Як зазначено у [1] інформаційна обізнаність будь-якого фахівця – це: 1) запорука того, що управлінець буде дотримуватися законності при виконанні власних обов'язків та вимагати від інших (у першу чергу від підлеглих); 2) його спроможність передбачити (спрогнозувати) можливості порушення законності під час підготовки та проведення різного роду заходів в регіоні (в населеному пункті); 3) здатність управлінця державного управління (ДУ) організувати взаємодію з іншими органами (наприклад, при вирішенні питань пов'язаних з охороною громадського порядку та забезпечення громадської безпеки [2]).

Безперечно, основу інформаційної обізнаності управлінець ДУ отримує при навчанні у вищому навчальному закладі. Разом з тим, слід мати на увазі, що в процесі виконання обов'язків управлінцем ДУ на практиці, здійснюються зміни у сферах законодавства, побудови організаційних структур тощо, тому питання інформаційної обізнаності управлінця державного управління в системі післядипломної освіти на теперішній час є актуальним.

На думку авторів праці, *напрямами удосконалення* інформаційної обізнаності управлінця державного управління в системі післядипломної освіти слід вважати:

1. З'ясувати сутність післядипломної освіти. *Післядипломна освіта* – в українському законодавстві визначається як спеціалізоване вдосконалення освіти та професійної підготовки особи шляхом поглиблення, розширення і оновлення її професійних знань, умінь і навичок або отримання іншої спеціальності на основі здобутого раніше освітньо-кваліфікаційного рівня та практичного досвіду [3].

Згідно з таким державним визначенням, *післядипломна освіта* створює умови для безперервності та наступності освіти і включає: 1) *перепідготовку* – отримання іншої спеціальності на основі здобутого раніше освітньо-кваліфікаційного рівня та практичного досвіду; 2) *спеціалізацію* – набуття особою здатностей виконувати окремі завдання та обов'язки, які мають особливості, в межах спеціальності; 3) *розширення профілю (підвищення кваліфікації*) – набуття особою здатностей виконувати додаткові завдання

та обов'язки в межах спеціальності; 4) *стажування* – набуття особою досвіду виконання завдань та обов'язків певної спеціальності.

Особа, яка пройшла перепідготовку і успішно пройшла державну атестацію, отримує відповідний документ про вищу освіту. Особа, яка успішно пройшла стажування або спеціалізацію чи розширила профіль (підвищила кваліфікацію), отримує відповідний *документ про післядипломну освіту.*

Післядипломна освіта є підгрунттям до руху управлінця органів публічного ДУ в Україні службовою драбиною.

2. Удосконалити організацію кадрового забезпечення органів ДУ в Україні шляхом широкого впровадження закордонного досвіду [4].

3. Чітко побудувати технологічні процедури управління кадровими процесами у відповідних органах влади. Так, М. Карпа вважає, що на будь-якому рівні реалізації кадрової політики (державному, регіональному або місцевому) відбуваються такі основні кадрові процеси як: 1) розроблення концепції державної кадрової політики (у сфері державного управління); 2) визначення засобів і способів кадрового забезпечення; 3) формування та реалізація цільових кадрових програм; 4) виконання планів роботи з кадрами і кадрових програм; 5) реалізація розроблених кадрових програм; 6) розроблення стратегії підбору кадрів; 7) відбір кадрів для заміщення посад; 8) процеси розстановки кадрів; 9) процеси прийому та звільнення персоналу; 10) професійна освіта, підготовка, можливість підвищення кваліфікації, компетентності; 11) розроблення та втілення стандартів кваліфікації працівників; 12) ідентифікація кадрового складу за показниками (стать, вік, рівень освіти, досвід роботи тощо), здійснення контролю за результатами праці (оцінка, атестація тощо); 13) стимулювання праці; 14) розроблення підходів управління з урахуванням індивідуальних якостей управлінців; 15) підготовка, перепідготовка та підвищення кваліфікації кадрів; 16) формування та ефективне використання кадрового резерву; 17) заходи щодо підвищення престижності роботи в органах публічного адміністрування; 18) оцінка ефективності роботи кадрів органів публічного адміністрування; 19) чіткий розподіл функцій, завдань та відповідальності за їх здійсненням; 20) заходи щодо запобігання корупційних дій тощо [5].

Отже, інформаційна обізнаність управлінця державного управління в системі післядипломної освіти є актуальною проблемою і вона повинна вирішуватися комплексно.

Список використаних джерел

1. Інформаційна обізнаність – запорука забезпечення правопорядку. Електронний ресурс. Режим доступу: https://f3.naiau.kiev.ua/news/informacijna-obiznanist-%E2%80%93-zaporuka-zabezpechennya-pravoporyadku.html.

2. Орлов М. М. Формування системи взаємодії регіональних органів виконавчої влади у сфері охорони правопорядку (теоретико-методологічні засади) : монографія / М. М. Орлов. – Х. : ХарРІ НАДУ "Магістр", 2012. – 344 с. ISBN 978-966-390-112-1.

3. Післядипломна освіта. [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Післядипломна_освіта.

4. Капінус М. Р. Світові тенденції розвитку державної служби / М. Р. Капінус // Державна служба України в історичному контексті: проблеми становлення та розвитку : 12 матеріали наук.-практ. конф. до 90-річчя держ. служби України (Київ, 18 листоп. 2008 р.) : у 2 т. / за заг. ред. О. Ю. Оболенського, С. В. Сьоміна. – К. : НАДУ, 2009. – Т 2 : у 3 ч. – Ч. 3. – 96 с.

5. Карпа М. Методи управління кадровими процесами у контексті становлення публічної служби в Україні // Ефективність державного управління : зб. наук. пр. ЛРІДУ НАДУ. – Вип. 37. – Львів : ЛРІ НАДУ, 2013. – 470 с.

Пастухов В. В., Вільгуш Д. В., Корнієнко О. С., Левкович П. В.

ОСНОВНІ АСПЕКТИ КІБЕРБЕЗПЕКИ У СУЧАСНОМУ СВІТІ ТА В УКРАЇНІ

У сучасному світі під час ведення бойових дій велику роль відіграють кібератаки на головні структури і підприємства держави, які тим чи іншим чином впливають на перебіг бойових дій. Кібератаки дають змогу досягти певної мети в економічній, політичній, військовій та інших галузях, а також досягти перевагу у збройному протистоянні. Такі дії зі сторони противника ще називають кібервійною.

Кібервійна – це «військові» дії, що здійснюються в електронному просторі в електронному вигляді. Зброя в кібервійні – це інформація, інструменти – комп'ютери, театр військових дій – інтернет. Сьогодні мережа інтернет є потужною зброєю, яка суттєво підсилюється технологіями штучного інтелекту.

Кіберзброя представляє собою широкий спектр технічних і програмних інструментів, які найчастіше спрямовані саме на використання вразливих місць у системах передачі даних. Механізм дії кіберзброї може бути абсолютно різним. Наприклад, вірусні програми можуть створювати перешкоди іншим програмам різними способами: відміняти команди або задавати свої, видаляти всі дані або змінювати їх. Однак у більшості випадків достатньо проникнути в чужу програму для того, аби отримати необхідні дані. Інструментами кібератак є шкідливі програми і віруси, тому для того, щоб протистояти кібератакам, необхідно використовувати високоякісний захист і, безумовно, залучати компетентних фахівців.

Відповідно до чинного законодавства України основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації, Національна поліція України, СБУ, Міністерство оборони України та Генеральний штаб ЗСУ, розвідувальні органи, Національний банк України, Державний комітет фінансового моніторингу України. Таким чином, розвиток інформаційних технологій зумовлює появу нових видів кібератак. Низка потужних та складних кібератак на комп'ютерні мережі енергетичного, банківського, транспортного секторів, галузі зв'язку, які відбулись з початку 2014 року, вкотре засвідчили, що російський агресор і надалі використовуватиме кібератаки як інструмент геополітичного впливу. Протидія цьому потребує не тільки зусиль на національному рівні, але й відпрацювання дієвих механізмів міжнародного співробітництва.

Отже, кібербезпека сьогодні як ніколи набуває значення нової галузі і призначена забезпечити національну безпеку держави. Тому своєчасне планування й реалізація заходів забезпечення кібербезпеки та інформаційного протиборства на глобальному та регіональному рівнях стає одним із пріоритетних завдань держави. Україна не просто може, а вимушена перестати концентруватись виключно на оборонних заходах. Маючи один із найкращих у світі людських потенціалів, фахівців з інформаційних технологій, здатність працювати швидко та ефективно, високу мотивацію до протистояння зовнішній агресії, держава повинна робити ставку не лише на оборонні технології, а й на наступальні, в тому числі у сфері кіберозброєння.

Корнієнко О. С., Пастухов В. В., Манелюк А. В., Ликова І. В.

РОЗВИТОК ІНФОРМАЦІЙНОЇ ВІЙНИ НА СУЧАСНОМУ ЕТАПІ

Інформаційна боротьба ведеться не тільки в ході військового конфлікту, але ж ще задовго до його початку та після завершення. На етапі підготовки до збройної боротьби заходи інформаційної боротьби проводяться, в першу чергу, на державному рівні з метою створення бажаних воєнно-політичних та економічних умов для початку агресії. Розвиток соці-

альних мереж і глобалізація світового співтовариства активно використовуються у військовій галузі не тільки з метою здійснення інформаційної боротьби, але й для ведення віртуальних бойових дій, які забезпечують реальні військові протистояння. За допомогою інформаційних технологій значна частина функцій людини перекладається на штучний інтелект і машини.

Бойові роботи – андроїди, безпілотні літальні апарати, системи наведення та корегування вогню, розвідувальні пристрої поступово переходять зі сторінок фантастичних творів і кінофільмів у реальний театр бойових дій, що дозволяє суттєво зменшити втрати серед особового складу. В цих інноваціях особливе значення відіграють інтернет-технології, як засіб передавання даних та технічне підтримання базового інформаційного процесу. Ключовим елементом у теоретичній моделі є поняття інформаційна мережецентрична війна, що визначається, як комплекс інформаційних впливів між соціальними системами (групами), що орієнтовані на отримання певних переваг у військових та громадських протистояннях.

На сьогоднішній день соціальні мережі відіграють важливу роль у процесі розповсюдження інформації, створюючи умови для над швидкого поширення інформаційних повідомлень з метою послабити моральні і матеріальні сили противника чи конкурента, та посилити власні. Вони передбачають активізацію заходів пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях. Очевидно, що інформаційна війна – складова частина ідеологічної боротьби. Вона не призводить безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою. І це породжує небезпечну безпечність у ставленні до життєво важливих благ. Тим часом, руйнування, яких завдають інформаційні війни у суспільній психології, психології особи, за масштабами і за наслідками цілком співрозмірні, а часом і перевищують наслідки бойових дій.

Слід зазначити, що сьогодні Збройні сили України забезпечені великою кількістю техніки та приладів, які призначенні для протидії інформаційному протистоянню на сучасному етапі розвитку. Такі системи є аналогами продуктів провідних країн світу, які виготовляються підприємствами вітчизняного оборонно-промислового комплексу.

Таким чином, зважаючи на проведення на Сході України операції Об’єднаних сил та, враховуючи особливості ведення сучасних бойових дій, й надалі існує необхідність проведення робіт зі створення нових та модернізації існуючих зразків для придушення інформаційної війни, які б за рівнем тактико-технічних характеристик не поступались закордонним аналогам та відповідали вимогам сьогодення.

Бокачов С. В., Федоров О. Ю., Мокоївець В. І.

ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В СИСТЕМУ ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ І ЧАСТИН ЗСУ ТА ІНШИХ СИЛОВИХ СТРУКТУР

Сучасна воєнно-політична обстановка, яка склалася навколо України, вимагає подальшого нарощування спроможностей її Збройних Сил та інших складових оборони, досягнення їх оперативної сумісності і скорішого набуття критеріїв, що потрібні для набуття членства у НАТО.

У зв’язку з насиченістю Збройних Сил й інших силових структур великою кількістю різноманітної бойової техніки і підвищенням ролі системи технічного забезпечення виникає потреба удосконалення системи управління нею, яка передбачає впровадження в її роботу сучасних алгоритмів і методів роботи технічного забезпечення, яки застосовуються при плануванні і веденні бойових та інших дій, удосконалення наявних і створення сумісних пунктів управління технічним забезпеченням, обладнаних автоматизо-

ваними робочими місцями, переоснащення та нарощування системи зв'язку та створення єдиної системи автоматизованого управління технічним забезпеченням силових структур під час виконання завдань із захисту держави.

Реальне технічне забезпечення в ході виконання любої бойової задачі визначається не стільки потенційними задачами, а тими з них, які можуть бути реалізовані, ступень же реалізації їх знаходиться у безпосередньої залежності від ефективності управління ними. Тому одним з основних напрямків подальшого удосконалення управління системою технічного забезпечення може бути автоматизація найбільш трудомістких і витратних за часом інформаційних процесів.

Автоматизація системи технічного забезпечення досягає дві мети: перша – забезпечення реалізації можливостей існуючої системи технічного забезпечення в інтересах досягнення виконання отриманих завдань на підставі вироблення і виконання своєчасних і обґрунтованих, виходячи з умов конкретної обстановки, рішень, друга – створення умов реалізації інтелекту керівників технічним забезпеченням усіх рівнів в ході їх діяльності за рахунок відповідної інформаційної підтримки.

Нажаль, існуючі у теперішній час у ЗСУ АСУ є локальними, які не спрягаються з системами управління інших видів і родів військ, а тим більше інших силових структур, що не відповідає вимогам міжвидової, а також внутрішньодержавної інтеграції систем управління.

З врахуванням цього існує необхідність мати систему управління технічним забезпеченням у ЗСУ на такій функціональної основі, яка б, будучи інтегрованою в систему оперативного і бойового управління, включала управління підрозділами і частинами технічного забезпечення у системі технічного забезпечення і спрягалася з системами технічного забезпечення інших силових структур.

Одною з основних вимог при створенні інтегрованої АСУ технічного забезпечення, яка забезпечує автоматизацію окремих її функцій, є здатність до модернізації, наприклад можливості передачі інформації як по вертикалі управління, так і по горизонталі між сусідніми взаємодіючими підрозділами і частинами, а також підрозділами і частинами інших силових структур .

При створенні і удосконаленні АСУ технічного забезпечення треба врахувати наступні напрямки: доступ командирів відповідних рівнів до загальної інформаційної бази для отримання необхідної інформації, а також можливості замовлення необхідного обслуговування, ремонту або отримання запасних частин; інтегрований огляд району дій, збір і аналіз інформації про стан і положення техніки і озброєння бойових підрозділів і підрозділів (органів) технічного забезпечення, засобів матеріально-технічного забезпечення всіх силових структур, яки задіяні в районі дій; взаємодія та інтеграція системи технічного забезпечення підрозділів і частин з іншими системами всебічного забезпечення, яки задіяні для забезпечення дій військ.

Наявність у командирів всіх рівнів системи АСУ технічного забезпечить надасть їм можливість отримання достатньо детальної інтегрованої і своєчасної інформації про стан техніки і озброєння та їх технічного забезпечення для прийняття ними ефективних рішень в ході виконання завдань. Ця інформація на тактичному й інших рівнях може включати як данні по технічному забезпеченню, так і пов'язані з ним дані кадрового, медичного забезпечення, переміщення засобів тилового забезпечення тощо. Маючи відповідну інформацію командири всіх рівнів можуть проводити аналіз і оцінку стану технічного забезпечення підлеглих підрозділів (частин) і приймати ефективне рішення з технічного забезпечення виходячи з можливих варіантів бою (дій).

Через АСУ технічного забезпечення здійснюється обробка, аналіз і надання інформації для визначення потреб технічного забезпечення всіх наявних в районі дій військ, а можливо й тих, що туди прибувають. Для управління технічним забезпеченням має використовуватися загальна картина району дій, розташування підрозділів (частин, органів) технічного забезпечення, шляхів евакуації і районів передачі на них техніки, яка вийшла з ладу, об'єктів тилового забезпечення, що потрібні для забезпечення системи, інформація з пунк-

тів технічного забезпечення, заявки на забезпечення, розпорядження, інформаційні повідомлення про стан технічного забезпечення військових формувань, які задіяні в районі, а також інша інформація, яка потрібна для надійного функціонування системи.

Виходячи з практичного досвіду, можна стверджувати, що командири вимушені приділяти технічному забезпеченню досить велику кількість часу, як при підготовці, так і в ході виконанні задачі. Обсяг інформації про стан технічного забезпечення, який отримується від підлеглих підрозділів, обробляється і передається до органів технічного забезпечення із затримкою по часу, що не сприяє виконанню задачі. Наявність же АСУ технічного забезпечення надасть можливість всім органам технічного забезпечення отримувати інформацію безпосередньо, самостійно планувати виконання замовлень і свої дії ще до отримання розпорядження від командира, а інколи, якщо дозволяє обстановка, і виконати їх. При такому вирішенні завдань технічного забезпечення підлеглих підрозділів командири всіх рівнів мають можливість не відволікатися і більше зосередити свою увагу на веденні бойових дій.

Вирішальним фактором такого варіанту технічного забезпечення угрупування військ, яке складається з підрозділів і частин різних силових структур, є наявність АСУ технічного забезпечення, яка інтегрована в автоматизовану систему бойового управління і спрягається з іншими автоматизованими системами, в тому числі і силових структур. Вона дозволить спостерігати за переміщенням сил і засобів у системі технічного забезпечення, оперативно відстежувати проблеми, які виникають, і своєчасно реагувати на них. При цьому частина або всі органи технічного забезпечення, які призначені і переміщуються в один з підрозділів, можуть бути при необхідності спрямовані в інший.

Виходячи з досвіду і стверджень західних воєнних експертів, створення і розгортання інтегрованої інформаційної системи технічного забезпечення у Сухопутних військах на всіх рівнях управління, яка спрягається з подібними системами інших силових структур, значно змінює процеси технічного забезпечення. Можливість спостереження за всіма силами і засобами технічного забезпечення, доповіді підлеглих підрозділів про технічний стан і замовлення щодо технічного забезпечення, автоматизація і надійний зв'язок створюють гнучку, швидку і ефективну систему підтримки бойових дій угрупувань своїх військ, а також оперативне управління силами і засобами технічного забезпечення.

Федоров О. Ю., Бокачов С. В., Мокоївець В. І.

ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Збройна агресія і порушення територіальної цілісності України (тимчасова окупація Російською Федерацією Автономної Республіки Крим, міста Севастополя та військова агресія Російської Федерації в окремих районах Донецької і Луганської областей), нарощування військової потужності Російської Федерації в безпосередній близькості до державного кордону України вимагає нарощування спроможностей Збройних Сил та інших складових сил оборони з досягненням їх оперативної і технічної сумісності зі збройними силами держав – членів НАТО, набуттям критеріїв для членства України в ЄС і НАТО.

Одним з основних напрямків набуття Збройними силами України, як основної складової сил оборони, спроможностей, необхідних для оборони держави та досягнення повної оперативної сумісності зі збройними силами держав – членів НАТО, є удосконалення системи управління, яке передбачає: послідовне переведення органів військового управління на структури штабів військ НАТО та впровадження в їх діяльність сучасних алгоритмів і методів роботи з прийняття рішення, які з**а**стосовуються під час планування операції (бойових, спеціальних дій); створення сучасних пунктів управління, які обладнані автоматизованими робочими місцями; переоснащення та нарощування системи

зв'язку та створення єдиної автоматизованої системи управління Збройних Сил, що забезпечуватиме підтримку прийняття рішення командиром (командувачем) тощо.

На сьогоднішній день за цими напрямками вже зроблені певні кроки. Так, на оперативному рівні триває плановий перехід органів військового управління Збройних Сил на структури типу «G» з розподілом між ними функцій із формування, підготовки, розвитку і забезпечення військ (сил) та функцій з управління застосуванням військами (силами) під час ведення операцій (бойових, спеціальних дій). На тактичному рівні триває перехід штабів військових частин Збройних Сил на структури типу «S».

Для підвищення ефективності системи оперативного та бойового управління військами (силами) на основі отриманого бойового досвіду та з урахуванням перспективної структури органів військового управління, за підтримки Програми уряду США з впровадження рішень на основі інформаційних технологій для Збройних Сил України, з квітня 2018 року розпочато розгортання Центру оперативного управління та контролю Головного командного центру Збройних Сил. У подальшому на його базі передбачено створення новітньої системи оповіщення на основі спеціалізованого програмного продукту, що позбавить систему управління Збройними Силами застарілих засобів оповіщення та заощадить значні кошти, які витрачалися на оренду каналів зв'язку.

У ході проведення Операції об'єднаних сил здійснено доведення мережі АСУ ЗС України "Дніпро" до тактичної ланки управління (бригада), а в окремих випадках – до взводних та ротних опорних пунктів з використанням цифрових засобів. Продовжується розгортання та удосконалення: єдиної інтеграційної платформи Збройних Сил України "Дельта", яка призначена для інтеграції інформаційних ресурсів різнотипних інформаційних та автоматизованих систем, створення єдиного геоінформаційного та інформаційно-аналітичного середовища органів військового управління, військових частин та підрозділів Збройних Сил України; інформаційної системи збору, обробки та видачі інформації про повітряну і надводну обстановку.

Продовжуються роботи з впровадження (нарощення) системи відеоспостереження за лінією розмежування. Використання цієї системи забезпечило збереження відеоконтенту з відеокамер та надало можливість Збройним Силам України вести спостереження за лінією зіткнення в режимі он-лайн, реагувати на випадки застосування зброї, здійснювати ідентифікацію об'єктів противника, засікати точки ведення вогню противником у будь-який час доби та значно зменшити втрати особового складу і техніки Збройних Сил України.

Здійснюється розроблення ескізного проекту та макетування автоматизованої системи управління логістичним забезпеченням Збройних Сил, тривають роботи з впровадження у війська автоматизованої системи управління тактичної ланки управління.

Враховуючи прагнення України до членства в НАТО, в основу діяльності командирів та штабів з планування бою (дій) закладаються алгоритми, що використовуються у штабах військ НАТО. Так, у військових організаційних структурах Збройних сил України типу відділення - взвод - рота пропонується використовувати алгоритм роботи командира під назвою TLP (troop leading procedures), а від батальйону до бригади - військовий процес прийняття рішення (ВППР), як аналог MDMP (military decision making process), що застосовується в збройних силах країн – членів НАТО. Зазначений алгоритм роботи вже закладено у проекти новітніх Бойових статутів механізованих і танкових військ (частина ІІ), які розроблялися у Національній академії сухопутних військ імені гетьмана Петра Сагайдачного.

Військовий процес прийняття рішення – уніфікований аналітичний процес, який застосовується командиром та штабом для вироблення замислу бою (дій). Він складається з сімох послідовних та взаємопов'язаних етапів: отримання завдання; аналіз завдання; розробка варіантів дій; аналіз варіантів дій; порівняння варіантів дій; затвердження варіантів дій; розробка бойового наказу. Кожен з етапів містить певні кроки, кількість та зміст яких залежать від умов обстановки, наявного часу, організаційно-штатної структури штабу, укомплектованості особовим складом та рівнем його фахової підго-

товки, оснащеністю робочих місць засобами автоматизації тощо. На кожному із зазначених етапів передбачається проведення командиром та службовими особами штабу певних тактичних розрахунків, при цьому вихідними даними для їх проведення мають бути дані поточної обстановки, яка змінюється швидкоплинно та статистичні дані, які залишаються незмінними тривалий час. Безумовно, інтенсифікація проведення цих розрахунків та процесів управління сприятиме досягненню переваги над противником у виробленні рішення та в діях. Але це потребує розробки сучасних засобів бойового управління та зв'язку, інтегрованих у єдиний інформаційний простір, удосконалення системи моделювання бою (дій), суттєвого підвищення рівню автоматизації процесів збору та аналізу інформації про обстановку, планування бою (дій) за рахунок упровадження єдиної автоматизованої системи управління військами і зброєю.

Впровадження запропонованого процесу прийняття рішення суттєво підвищить ефективність роботи штабу, а широке застосування інформаційних технологій у ході його проведення забезпечить своєчасне і якісне планування бою (дій) та покращить сумісність із відповідними штабами збройних силах країн – членів НАТО.

Запровадження єдиних поглядів та підходів на застосування інформаційних технологій серед складових сектору безпеки та оборони, які би відповідали євроатлантичним стандартам та критеріям сприятиме підвищенню спроможностей сил оборони щодо виконання завдань оборони держави, захисту її суверенітету, територіальної цілісності і недоторканності.

Мокоївець В. І., Бокачов С. В., Федоров О. Ю.

АВТОМАТИЗАЦІЯ ПРОЦЕСУ УПРАВЛІННЯ ЯК ШЛЯХ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ ВІЙСЬКОВОГО ШТАБУ

Одним з головних завдань управлінської діяльності військового штабу є організація ефективного застосування військової частини та підрозділів. При цьому трудовитрати на основних етапах його роботи, як під час підготовки бою (дій), так і в ході його ведення, суттєво залежать від кількості і підготовленості посадових осіб, які залучаються до роботи, та, в значній мірі, від рівня забезпеченості органу управління засобами автоматизації управління (ЗАУ).

Використання ЗАУ в роботі військового штабу повинне підвищувати оперативність його роботи та реалізувати такі основні вимоги: оперативність і плановість підготовки підрозділів до виконання завдань; прихованість проведення заходів підготовки до бою (дій); обґрунтованість і своєчасність прийняття рішення щодо застосування підрозділів; своєчасність та якість розробки плануючих бойових документів; ефективний контроль готовності військової частини і підрозділів до виконання завдань та надання допомоги у їх підготовці.

Офіцери штабу готують та вводять у систему довідки, розрахунки та необхідні для командира й інших службових осіб органу управління і підрозділів дані. Застосування ЗАУ поряд зі звичайними методами інформаційного обміну може забезпечити паралельний або зустрічно-паралельний метод обміну даними, при якому необхідна інформація надається на автоматизовані робочі місця (АРМ) командира, начальника штабу й інших службових осіб, не очікуючи відповідних запитів. Такий порядок роботи виключає необхідність в орієнтуванні всіх посадовців та надає можливість всім підрозділам органу управління та командирам підрозділів, які залучаються до роботи з планування бою (дій), приймати участь в роботі одночасно з командиром і начальником штабу.

Як показує практичний досвід, під час підготовки бою (дій) найбільшим розрахунковим навантаженням характеризується етап вироблення замислу. Трудовитрати оперативного складу, залежно від ступеня забезпеченості ЗАУ, можуть бути знижені на 60–70 %. Крім того, проведення тактичних розрахунків з системним обміном даними під час вироблення замислу дозволяє враховувати вплив різноманітних факторів на веден-

ня бою (дій), а також визначити найдоцільніші способи виконання тактичних завдань.

Працюючи паралельно з командиром, офіцери штабу під час вироблення замислу повинні бути готовими своєчасно надати командиру та начальнику штабу необхідні довідкові дані та розрахунки на їх АРМ або завчасного ввести їх у базу даних, що є найбільш ефективним. Такий порядок роботи штабу з одного боку, забезпечує найбільш повну участь службових осіб у виробленні командиром замислу бою (дій), а з іншого – дозволяє більш цілеспрямовано та ефективно проводити необхідні тактичні розрахунки.

На етапі формулювання рішення на ведення бою (дій) засоби автоматизації забезпечують своєчасне введення у базу даних ЗАУ необхідної інформації та підготовку відповідні запитів.

Інтенсивне впровадження інформаційних технологій у діяльність військових органів управління значно збільшує можливості щодо збору, зберігання, аналізу й графічної візуалізації просторових даних і пов'язаної з ними інформації про об'єкти, розташовані на місцевості. Разом з цим, на початку антитерористичної операції (АТО) основним та майже єдиним джерелом інформації для командирів та штабів усіх ланок управління о топографічних елементах місцевості були топографічні карти, при цьому окремі з них настільки застаріли, що їх використання призводило до втрат серед наших військ та зриву виконання бойових завдань.

Використання в органах управління, військових частинах та підрозділах аерофотознімків, цифрових та електронних карт суттєво покращує питання з планування і застосування сил та засобів, а подальше застосування в діяльності військ сучасних навігаційних засобів стало значним кроком вперед. На сьогоднішній день на озброєнні у військових частинах та підрозділах знаходиться апаратура споживачів супутникових навігаційних систем ГЛОНАСС і GPS NAVSTAR, яка дозволяє командирам вирішувати широкий спектр завдань.

Після завершення прийняття рішення та доповіді його командиру бойові завдання підрозділам доводяться у повному обсязі із введенням їх у базу даних як окремих документів.

Під час відпрацювання широкого кола питань взаємодії різнорідних сил і засобів, які можуть брати участь у сучасному загальновійськовому бою, технічні засоби автоматизації управління дозволяють командиру і штабу організовувати її методом моделювання бойових епізодів, при якому до службових осіб пункту управління на їх АРМ доводиться обстановка, а потім послідовно ввідні, за якими вони доповідають свої рішення. Ці відомості уводяться у базу даних ЗАУ, звідки вони можуть бути отримані службовими особами за запитом. Це дозволяє скоротити час виконання конкретного заходу у 1,5–2 рази.

Отже, оптимізація процесу управління військами шляхом запровадження сучасних засобів автоматизації та програмного забезпечення їх роботи може суттєво підвищити оперативність бойової діяльності військового органу управління і скоротити час на організацію бою (дій) у 2,5–3 рази, тому використання ЗАУ є необхідною умовою ефективної роботи органу управління як під час підготовки підпорядкованої військової частини та її підрозділів до бою (дій), так і в ході управління їх діями під час виконання бойового завдання.

Заболотнюк В. І., Баган В. Р., Федоров О. Ю.

ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У ЗБРОЙНИХ СИЛАХ КРАЇН-ЧЛЕНІВ НАТО

Прорив у сфері інформаційних технологій та поява сучасних геоінформаційних систем викликали формування нових тенденцій в області управління військами (силами) та спонукали військово-політичне керівництво передових країн-членів НАТО переосмислити та переглянути загальні положення щодо ролі і місця автоматизованих систем управління у ході ведення збройної боротьби. Враховуючи, що перевагу в операціях XXI визначає вже

не стільки кількість танків та ракет, що знаходяться на озброєнні, скільки обізнаність службових особі штабів ситуації у бойовому просторі, єдине її розумінням усіма учасниками операції, бою (дій), оперативність та обґрунтованість рішень, що приймаються командиром тощо. Більшість цих завдань покладається на систему управління, що функціонує у єдиному інформаційному просторі та використовує передові інформаційні технології підтримки прийняття рішень. Враховуючи зазначене з 2002 року НАТО розпочинає розробку концепції "Комплексні мережеві можливості НАТО". До роботи залучаються провідні фахівці країн-членів НАТО, а фінансування здійснюється з військових бюджетів 12 країн альянсу. На думку її авторів вона дозволить перейти до нових, більш ефективних форм ведення операцій, бою (дій) та забезпечить:

- інформаційну перевагу над противником, покращить своєчасність і достовірність інформації, що надходить у штаби, надасть більш глибоке розуміння посадовим особам даних обстановки;
- оперативність управління та скорочення і оптимізацію циклу бойового управління;
- синхронізацію та підвищення інтенсивності і ефективності застосування в операції, бою (діях) усіх військових організаційних структур та їх систем управління;
- створення єдиного багатовимірного бойового простору коли в ході ведення операції, бою (дій) війська, сили та засоби територіально розосереджені, а лінія зіткнення сторін фактично відсутня;
- акцентування зусиль на масуванні результатів, а не на масуванні сил за рахунок об'єднання в єдину інформаційну мережу територіально рознесених систем;
- комплексне використання та підвищення ефективності застосування систем розвідувально-інформаційного забезпечення оперативно-тактичної та стратегічної ланок управління.

Значний прогрес в області інформаційних технологій на сьогоднішній день дозволяє технічно реалізувати можливості по створенню систем управління, автоматизованого прийняття рішення, управління просторовими даними. При цьому такі системи будуть відповідати вимогам по забезпеченню взаємної узгодженості як між собою так і з системами збору і обробки розвідувальних даних, датчиками (сенсорами) систем озброєння і визначення місцезнаходження будь яких об'єктів на місцевості, створення єдиного інформаційно-комунікаційного простору в якому усі елементи бойового прядку, включаючи окремого військовослужбовця, матимуть можливість здійснювати обмін інформаційний потоком в реальному масштабі часу.

Вивчення та використання досвіду країн-членів НАТО щодо впровадження інформаційних технологій підтримки прийняття рішення у діяльність органів управління є дуже актуальним питанням. Його глибокий аналіз та впровадження у Збройних Силах України дозолить суттєво покращити оперативність управління військами (силами) та організацію взаємодії, сприятиме випередженню противника у прийнятті обґрунтованих рішень та діях військ (сил), підвищить живучість військ.

УДК 621.3 (075. 8)

Давіденко С. В., Бойчук Б. М.

ПЕРСПЕКТИВИ МОДЕРНІЗАЦІЇ ТРАНСПОРТНИХ МЕРЕЖ

Сучасні тенденції розвитку систем управління силовими підрозділами полягають у створенні єдиного інформаційного і комунікаційного простору на базі локально обчислювальних мереж і характеризуються зростанням попиту на телекомунікаційні послуги де чітко відстежується швидке зростання об'ємів трафіку даних. Поступово трафік даних стає домінуючим, що вимагає створення телекомунікаційних мереж з високою пропускною здатністю на базі комутації пакетів. Збільшується кількість користувачів,

як в повсякденній, так і в професійній діяльності, разом з традиційними послугами зв'язку, яким потрібні послуги передачі даних і доступу в Інтернет. Зростає мультимедійниий трафік у телекомунікаційних мережах на основі IP технологій [1].

Задачі модернізації транспортних мереж можна розділити на два напрями. Перший напрям пов'язаний з оптимізацією структури міської телефонної мережі при цьому здійснюється пошук оптимального місця розміщення комутаційних вузлів [2, 3]. Другий напрямок приводить до якісних змін в устаткуванні передачі і комутації із збільшенням пропускної здатності транспортної мережі [4].

Аналізуючи динаміку зростання пропускної здатності транспортних мереж спостерігається “вирівнювання” пропускної здатності і продуктивності окремих ділянок мережі [5], тобто спостерігається тенденція використання однотипних технологій у всіх рівнях транспортних мереж [6, 7]. Транспортні оптичні мережі найбільш придатні, як однотипні технології для об’єднання різнорідних мереж, тобто для конвергенції мереж.

Повністю оптичні мережі маючи достатньо велику пропускну здатність можуть забезпечувати крім конвергенції мереж, конвергенцію послуг. Існуючі транспортні системи поступово будуть модернізуватись в технологію повністю оптичних мереж [8].

Із зростанням мультисервісного трафіку і впровадженням нових видів послуг змінюються вимоги до міських телефонних мереж. Поряд з вимогою збільшення пропускної здатності ставиться питання мінімізації часів передачі із збільшенням продуктивності магістральних комутаторів. Використання технології DWDM і повністю оптичних комутаторів утворює набір віртуальних каналів, які представляються топологією тороїдальних структур. Нові види сервісу будуть базуватись на основі транспортних протоколів з гарантованим часом доставки і джитером.

Конвергентна мережа NGN - це багаторівнева мережа, рівні якої, відрізняються від рівнів семирівневої еталонної моделі взаємодії відкритих систем [4]. Суть переходу від існуючих телефонних мереж до мереж NGN – це створення на основі перспективних технологій єдиного транспортного середовища і інфраструктури для надання користувачам нових послуг, одночасно з підтримкою сучасних послуг [9]. Існуюча телефонна мережа буде конвергуватись у транспортну площинну NGN мереж. При цьому топологія міської телефонної мережі, як правило змінюватись не буде, але функціональне призначення вузлів змінюється.

Згідно концепції “не руйнуючого” переходу до NGN [10] здійснюється перехід окремих сегментів на нові технології без кардинальної зміни всієї структури мережі і тому актуальним є дослідження шляхів модернізації мережі.

Згідно [11], перехід до конвергентних мереж від мереж з комутацією каналів відбуватиметься поетапно: до мереж з комутацією пакетів на базі програмного комутатора, а потім до мереж на основі архітектури IMS.

В [11] запропоновано перехід до конвергентних мереж з використанням МАК і транзитних комутаторів на основі IP-платформи. Кожен концентратор включається в опорний комутатор двома трактами, що проходять по незалежних шляхах. Завдання транзитних комутаторів полягає в надійній передачі IP-пакетів в відповідності із заздалегідь вибраним маршрутом.

В [12] показано також включення трьох відомчих автоматичних телефонних станцій по технології IP. Процес формування IP-мережі з підтримкою показників QoS здійснюється за допомогою транзитних комутаторів і забезпечується транзит трафіку у формі IP-пакетів в міські телефонні станції і в транспортні мережі. Доцільно скористатися можливістю напівпостійної комутації у вузлах транспортної мережі [12].

На другому етапі модернізації транспортної мережі з вузлами двох типів відбувається розширення IP- мережі і одночасне скорочення чисельності комутаційних станцій, що використовують технологію "комутація каналів".

У кожному вузловому районі залишаються вузли вихідних з’єднань та вузли вхідних з’єднань, що обслуговують одну АТС. На третьому етапі, замінюються всі вузли вихід-

ного з'єднання та вузли вхідного з'єднання, тобто технологія "комутація каналів" в мережі оператора міської телекомунікаційної системи більше не використовується.

Важлива особливість іншого варіанту полягає в можливості заміни АТС протягом тривалого періоду і з мінімальними витратами. Вказаний варіант можливий за умови створення мережі IP з підтримкою показників QoS. Термінали всіх абонентів, під'єднуються до концентраторів, які підтримують обслуговування класу "Triple Play Services".

Таким чином перехід окремих сегментів на нові технології без кардинальної зміни всієї структури мережі повинен іти за рахунок модернізації мережі шляхом оптимізації структури телефонної мережі пошуком оптимального місця розміщення комутаційних вузлів та розширення IP-мереж з одночасним скороченням чисельності комутаційних станцій, що використовують технологію "комутація каналів".

Список використаних джерел

1. Гольдштейн Б. С. IP-телефония / Гольдштейн Б. С., Пинчук А. В., Суховицкий А. Л. – М: Радио и связь, 2001. – 336с.

2. Sokolov N. A. Some aspects of russian telecommunications / Sokolov N. A. // IEEE Communications Magazine. – 2006. – January. – P.23 – 26.

3. Пинчук А. В. Мультисервисные абонентские концентраторы для функциональных возможностей "Triple-Play Services"/ Пинчук А. В., Соколов Н. А. // Вестник связи. – 2005. – № 6. – С.42-48.

4. Пинчук А. В. Модернизация ГТС без узлов / Пинчук А. В., Соколов Н. А. // Вестник связи. – 2005. – № 12. – С.64-68.

5. Шварц М. Сети связи: протоколы, моделирование и анализ: [в 2 ч] / Шварц М.; пер. с англ. – М.: Наука, 1992. – Ч. 1. – 336с.

6. Гаранин М. В. Системы и сети передачи информации: учеб. пособие для вузов / Гаранин М. В., Журавлев В.И., Кунегин С. В. – М.: Радио и связь, 2001. – 336 с.

7. Лазарев В. Г. Динамическое управление потоками информации в сетях связи / Лазарев В. Г., Лазарев Ю. В. – М.: Радио и связь, 1983. – 216с.

8. Хмелёв К. Основы фотонного транспорта / Хмелёв К. – К.: Техніка, 2008. – 680 с.

9. Соколов Н. А. Телекоммуникационные сети. Т.3 / Соколов Н. А. – М.: Альварес Паблишинг. – 2004. – 192с.

10. Сети следующего поколения NGN / [Росляков А. В., Ваняшин С. В., Самсоно М. Ю. и др.]; под ред. Рослякова А. В. –М.: Эко-Тендз, 2008. – 424 с.

12. Пинчук А. В. Модернизация ГТС с узлами входящего сообщения / Пинчук А. В., Соколов Н. А. / Вестник связи. – 2006. – № 1. – С.50-53.

13. Сергеев Р. Оборудование ADSL для пользователей и операторов/ Сергеев Р. // Компьютерная неделя. – 2004. – №2. http://www.pcweek.ru/themes/detail.php?ID=66480

УДК 004.942

Д'яков А. В., Кириллова Н. В.

МОДЕЛЮВАННЯ ЯК ПЕРСПЕКТИВНИЙ НАПРЯМ У СИСТЕМІ ПІДГОТОВКИ ВІЙСЬК

В умовах сучасності все більше розповсюдження набувають обчислювальні експерименти з використанням різного роду математичних моделей та моделюючих комплексів, за допомогою яких можна спрогнозувати характер, форми та види збройних конфліктів, апробувати нове озброєння, нові технології організації і ведення військових дій, ефективно здійснювати підготовку військ.

Мінімізація затрат на бойову підготовку та навчальний процес, зменшення потенціальних втрат серед особового складу, збереження інфраструктури, матеріальних засобів та максимізація ефективності навчання військових фахівців є вагомим аргументом для зміни методів традиційного навчання на нові підходи до навчання з використанням засобів імітаційного моделювання.

Застосування ІТ-технологій суттєво знижують умовність дій за рахунок створення віртуального бойового середовища, де усі сили і засоби діють на реальній місцевості та як в реальній бойовій обстановці.

Засоби імітаційного моделювання у підготовці військових фахівців дозволяють моделювати оперативно-тактичну обстановку, різні бойові ситуації, а також проводити розрахунки та готувати дані для прийняття рішення та планування бойових дій. Реалії такого віртуального бою надають можливість відповідним командирам приймати рішення на бій і вести підготовку до бою як в реальних бойових умовах, управляти підрозділами та вогнем.

За допомогою моделей операцій (бойових дій) можна представити та завчасно програти військову операцію (бій та ін.) з будь-яким ступенем точності, в цьому випадку тільки технічні засоби виступають тут обмежувальним фактором. Це дозволяє відпрацьовувати різноманітні варіанти застосування військ в інтересах широкого спектра задач (бойових, миротворчих, спеціальних).

Відмінністю від традиційних форм бойової підготовки є забезпечення відпрацювання слухачами всебічно обґрунтованих рішень на застосування військ (сил) та управління при виконанні поставлених задач за рахунок проведення оперативно-тактичних розрахунків і математичного моделювання бойових дій в інформаційно-моделюючому середовище, забезпечення автоматизованої розробки навчально-методичних документів та розіграшу імітації бойових дій.

Слід зауважити, що органи управління , відповідальні за підготовку та проведення заходів оперативної підготовки, отримують можливість шляхом математичного моделювання здійснювати об’єктивний прогноз розвитку обстановки у відповідності із рішенням конфліктуючих сторін, при цьому враховується значно більша кількість факторів у порівнянні із методами абстрактно-логічного прогнозування.

Одним з перспективних напрямків розвитку моделювання є застосування так званої JLVC (Joint Virtual, Live, Constructive)-технології для поєднання усіх видів моделювання у єдиний інформаційний простір. Головною метою впровадження JLVC-технології є створення більш реалістичної обстановки для комплексної підготовки максимально розосереджених різнорідних угруповань сил і засобів різного базування (наземного, повітряного та морського) на принципах адекватності, скритності та ефективності (економії ресурсів).

В свою чергу, проведення бойової підготовки у відповідності до JLVC-технології передбачається на всіх рівнях – тактичному, оперативно-тактичному, стратегічному та при індивідуальній підготовці військовослужбовця. Розуміння того, як проводити підготовку на кожному з тактичних рівнів, вироблення відповідних методик навчання та тренінгу створює умови для успішної підготовки особового складу та підрозділів до виконання завдань за призначенням.

Головним напрямком підвищення ефективності використання засобів імітаційного моделювання у навчальному процесі є створення системи моделювання, яка повинна включати програмне забезпечення для різних тактичних рівнів та їх інтеграцію в єдине інформаційно-моделюючу середовище. Таке середовище повинно включати в себе сукупність сертифікованих окремих моделей і об’єктів та будуватися на основі уніфікованих програмно-технічних елементів, а саме це передбачає створення:

- уніфікованого захищеного програмного забезпечення;
- єдиної системи тримірної візуалізації віртуального бойового середовища;
- єдиного формату цифрових карт і моделей місцевості;
- єдиної системи імітації динамічних навантажень на слухачів;

- єдиного робочого місця інструкторів;
- максимально можлива уніфікація конструкторсько-технологічних рішень;
- модульність побудови для забезпечення багатоваріантності виконання тренажерів;
- можливість поєднання екіпажних та інших тренажерів в єдину систему для підготовки підрозділів і органів управління.

Основними проблемними питаннями реалізації даного підходу є:

- забезпечення високого ступеню адекватності роботи обладнання, систем та засобів зразків озброєння та військової техніки та органів управління;
- забезпечення належного ступеню адекватності бойової обстановки (наземної, повітряної, морської);
- забезпечення єдиної бойової обстановки (наземної, повітряної, морської), що імітується для всіх засобів озброєння та військової техніки і військових підрозділів;
- спряження територіально-рознесених тренувальних засобів та комплексів в системи більш високого рівня для проведення багатоступеневих тренувань органів управління;
- синхронізація за часом роботи територіально-рознесених тренажерів та тренажерних комплексів для проведення тренувань різного виду у складі тренажерних систем;
- забезпечення об’єктивності оцінювання бойових розрахунків та органів управління за результатами документування їх діяльності у процесі підготовки.

УДК 355.244.2

Гончар Р. О.

ЦІЛІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ В СЛУЖБОВО-БОЙОВІЙ ДІЯЛЬНОСТІ ОРГАНІВ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

В контексті розвитку та якісної трансформації органів управління Національної гвардії України (НГУ) актуальним є питання розвитку та впровадження у роботу органів управління інформаційно-аналітичної складової. Інформаційно-аналітична робота – діяльність органів управління НГУ, спрямована на пошук, отримання, систематизацію, оцінку і аналіз даних про стан оперативної обстановки в районах виконання службово-бойових завдань (СБЗ), результатах їх виконання, виявлення та прогнозування тенденцій і відхилень, вироблення на цій основі своєчасних, обґрунтованих і оптимальних управлінських рішень, спрямованих на ефективне виконання функцій Національної гвардії України і виконанні поставлених СБЗ.

Суб'єкти інформаційно-аналітичної роботи – командири частин та з’єднань, штаби та структурні підрозділи НГУ, які здійснюють організаційно-методичні та інформаційно-аналітичні функції, посадові особи гвардії, діяльність яких пов'язана з обробкою, узагальненням і аналізом інформації.

Цілі інформаційно-аналітичної роботи в службово-бойовій діяльності Національної гвардії України:

- визначення фактичного стану об’єктів протидії в районі виконання СБЗ;
- оцінка стану забезпечення громадської безпеки на території, яка аналізується та об’єктах за визначений період;
- виявлення проблем і недоліків в організації службово-бойової діяльності підрозділів частин та з’єднань НГУ, вивчення причин і умов їх виникнення, вироблення заходів щодо їх усунення;
- аналітичне забезпечення розробки планів, розпоряджень та інших управлінських рішень органів управління НГУ, конкретних пропозицій щодо вирішення найбільш актуальних проблем які виникають в ході виконання службово-бойових завдань;

- оцінка і прогнозування оперативної обстановки, визначення пріоритетних напрямків діяльності органів управління щодо попередження кризових ситуацій і виникаючих ризиків, варіантів оптимального використання наявних сил і засобів підрозділів та частин;
- своєчасне інформування взаємодіючих органів складових сектору безпеки і оборони, органів місцевого самоврядування про стан громадської безпеки в районах виконання завдань, підготовка конкретних пропозицій щодо усунення причин і умов, що сприяють скоєнню правопорушень;
- використання результатів досліджень громадської думки про діяльність Національної гвардії при виробленні управлінських рішень;
- вивчення позитивного досвіду виконання службово-бойових завдань підрозділами, частинами та з'єднаннями Національної гвардії України, в тому числі щодо попередження, припинення протиправних дій при забезпеченні громадської безпеки.

Комплексне впровадження інформаційно-аналітичної роботи в службово-бойовій діяльності органів управління Національної гвардії України є складним питанням, яке потребує ґрунтовного наукового дослідження та використання досвіду провідних правоохоронних формувань світу.

Кобзєв В. Г., Козлов В. Є., Козлов Ю. В., Мощенко І. О., Новикова О. О.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ РЕАЛІЗАЦІЇ КОМПЕТЕНТНІСНОГО МЕТОДУ ОЦІНЮВАННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ СПЕЦІАЛІСТА

Послідовне і поступове розповсюдження на Заході поняття "competence" у практиці післядипломного навчання, підвищення кваліфікації та перепідготовки кадрів, професійної школи призвело до появи в системі освіти концепції так званого компетентнісного підходу. Спираючись на цю концепцію, Міжнародна асоціація праці вводить поняття "ключові компетенції", що включають предметні й соціальні компоненти, у кваліфікаційні вимоги до спеціалістів.

Накопичений досвід втілення компетентнісного підходу в системі освіти показав наявність низки проблем, обумовлених складністю оцінювання процесу і результату професійної діяльності спеціалістів. Ця проблема викликала потік публікацій, різних за видом, обсягом і змістом, за авторством від маститих і титулованих вчених до вчителів молодших класів середньої школи, кількість посилань на які в Інтернеті налічує мільйони. Наявність безлічі публікацій спонукає до пошуку шляхів вирішення проблеми з застосуванням методів кваліметрії та інформаційної технології.

Запропоновано до практичного застосування інформаційну технологію вирішення завдань оцінювання професійної діяльності спеціаліста, засновану на компетентнісному підході. Сутність методу: група експертів складає інформаційну модель (професіограму) робітника – переліки (тезаурус і абетковий покажчик) оцінюваних ознак – кола повноважень (компетенції), а також знань, умінь та особистісних ознак (компетентності); кожен об'єкт оцінювання (ОО) експерти порівнюють за кожною із ознак і приписують бал за чотирибальною шкалою порядку, що характеризує ступінь відповідності ОО конкретній ознаці; отримані сукупності оцінок (персонограми) обробляють відповідним чином; результат оброблення (ранжированый список) подається особі, що приймає рішення.

В якості приклада застосування методу розглянуто процедуру оцінювання професійної діяльності групи викладачів-початківців закладу вищої освіти.

Куценко Є. Є., Пастушенко М. С.

ОЦІНКА ЧАСТОТИ ОСНОВНОГО ТОНУ ГОЛОСОВОГО СИГНАЛУ КОРИСТУВАЧА СИСТЕМИ АУТЕНТИФІКАЦІЇ

Більшість сучасних організацій і підприємств здійснюють свою діяльність за допомогою інформаційних і телекомунікаційних систем. При цьому системи доступу до фінансових, інформаційних і обчислюваних ресурсів на сучасному етапі потребують удосконалення, оскільки використовується ненадійний парольний захист. Підтвердженням сказаного є дані про фінансові розкрадання з карток в Україні за 2019 рік, які зросли на 47,3% і досягли 361,99 млн. грн.

Першим бар'єром в забезпеченні безпеки комп'ютерних та інформаційних мереж, систем доступу різного призначення є процедури аутентифікації користувачів. Головним напрямком удосконалення сучасних систем аутентифікації– використання біометричних ознак користувача, і в першу чергу, його динамічних (поведінкових) ознак, а саме, систем голосової аутентифікації (СГА). За критерієм ефективність/вартість СГА найбільш перспективні системи. Разом з тим, СГА мають якісні показники, які не відповідають зростаючим сучасним вимогам до їх характеристик.

У СГА при формуванні ознак шаблону знайшли застосування наступні ознаки голосового сигналу користувача, які витягуються з амплітудно-частотного спектру: частота основного тону, формантна інформація, спектральні і кепстральні коефіцієнти. Серед цих ознак важливе місце займає частота основного тону.

У доповіді розглядається задача підвищення точності оцінки частоти основного тону голосового сигналу користувача системи аутентифікації. Поряд з відомими методами спектральної оцінки частоти основного тону в роботі досліджується вплив фазових даних голосового сигналу, а також кепстральних коефіцієнтів на точність одержуваних оцінок.

Наводяться результати модельного експерименту та формуються напрямки подальших досліджень.

УДК 519.8

Душкін В. Д., Мельник В. М.

ВИКОРИСТАННЯ МЕТОДУ ДЕЛЬФІ ДЛЯ ПРОГНОЗУВАННЯ ПЕРСПЕКТИВ РОЗВИТКУ ОЗБРОЄННЯ, ТЕХНІКИ ТА ЗВ’ЯЗКУ

Ера технологічних революцій, що призвела до виникнення нових матеріалів, засобів і принципів зв'язку, способів зберігання інформації підвищує важливість правильного прогнозування тактико технічних характеристик нових видів озброєння і техніки. Прийняття рішень, що ґрунтуються лише на досвіді минулого, буде призводити до систематичного відставання від потреб «майбутнього дня», який вже «завтра» стане сучасним.

На думку фахівців, рішення, вироблені під час нарад, використання «мозкового штурму» мають суттєві недоліки завдяки конформізму учасників процесу. Принцип єдиноначальності, що призводить до небажання учасників нарад висловлювати та відстоювати ідеї, що відрізняються від ідей вищого керівництва.

Одним з методів, який позбавлений від вищезазначених недоліків, є метод Дельфі. Підкреслимо, що він був розроблений корпорацією RAND у США для прогнозування впливу майбутніх наукових розробок на методи ведення війни. Він виключає пряме спілкування учасників експертної групи, що дає можливість позбавитись відкритих зіткнень між представниками антагоністичних поглядів. До того ж він дозволяє не збирати фахівців одноча-

сно у певному місці та залучати до роботи експертів та стейкхолдерів з усієї України. Збір думок можна реалізувати за допомогою листування електронною поштою.

Метод Дельфі реалізується за допомогою декількох послідовних кроків опитувань експертів. Після кожного кроку опитування відбувається доведення до учасників кожного етапу опитування. Думки експертів обробляються за допомогою статистичних методів. Члени творчої групи повторно розглядають свої судження з урахуванням групової думки. У більшості випадків він веде до вироблення узгодженої думки за декілька турів.

Особливою рисою цього методу є необхідність вираження думок експертів у кількісній (числовій) формі. Ця особливість призводить до настороженості фахівців у бажанні використовувати цей метод, не зважаючи на вищезазначені переваги дельфійського методу. Тому важливою приділити увагу процедурі переведення думок експертів у кількісну форму та ознайомлення усіх учасників процесу з думками експертів, оцінки яких не входять у центральні квартилі оцінок.

Успіх використання дельфійського методу залежить від правильного складання листа для опитування. У класичному варіанті методу Дельфі початкова анкета містить лише загальне формулювання задачі. Експерти визначають основні фактори, що характеризують процес на основі яких формується структура анкети наступних етапів. Інший підхід передбачає, що замовник самостійно складає опитувальну анкету, або робить це за допомогою інших фахівців. Ми вважаємо, що має сенс паралельно скласти анкети замовників дослідження та кількісною обробкою результатів.

Метод Дельфі, як і усі методи прийняття рішень, має свої переваги та недоліки. Тому його результати можна використовувати лише як одну з рекомендацій для прийняття остаточного рішення.

УДК 355.233:5.001

Зуб О. В., Алфімова Л. Д.

ФУНДАМЕНТАЛЬНА ПРИРОДНИЧО-НАУКОВА ПІДГОТОВКА МАЙБУТНІХ ОФІЦЕРІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Сучасний стан системи військової освіти в умовах усебічного вдосконалення потребує пошуку нових підходів до організації навчального процесу у військовому виші, здатних створити умови для підготовки кваліфікованих офіцерських кадрів. В останній час у військах Національної гвардії України відбувається переозброєння на нову техніку та прилади, дія яких заснована перш за все на фізичних принципах, однак у педагогіці вищої військової школи недостатньо розкриті можливості організації педагогічного процесу, які б забезпечували підготовку майбутніх офіцерів Національної гвардії до використання знань природничо-наукових дисциплін в професійній діяльності.

Нами зроблено гіпотетичне припущення, що підготовка майбутніх офіцерів Національної гвардії України до використання знань природничого циклу у професійній діяльності буде забезпечена, якщо:

- у змісті навчальних дисциплін природничо-наукового циклу виділяться елементи, пов'язані з професійною діяльністю офіцерів Національної гвардії України;
- у процесі навчання будуть сформовані мотиви застосування знань поставлених завдань у військах Національної гвардії, причому одним з бажаних моментів є використання інтерактивних методів навчання;
- забезпечиться варіативність використання педагогічних засобів, що сприятиме підготовці курсантів до застосування знань природничого циклу в майбутній професійній діяльності.

Для досягнення поставлених цілей можуть застосовуватись різноманітні методи: теоретичний аналіз проблеми і предмета дослідження, системний аналіз, цілісний та інтегральний підходи до дослідження педагогічних явищ і виявлення тенденцій їх розвитку.

Вивчення курсантами значної кількості навчальних предметів природничо-наукового циклу не тільки закладає фундамент для засвоєння дисциплін професійної і практичної підготовки, але й формує науковий світогляд, його алгоритмічну культуру, уміння встановлювати причинно-наслідкові зв’язки, обґрунтовувати ствердження, моделювати ситуації. Крім того, цей факт стимулює мислення майбутнього фахівця сукупністю характерних для природознавства методологічних підходів до розгляду будь-яких процесів і явищ, створює передумови до більш широкої освіченості.

Викладачам курсу математично-природничих дисциплін бажано тісно співпрацювати зі своїми колегами зі спеціальних кафедр з метою обговорення та коригування робочої програми з дисципліни. В свою чергу вона повинна містити здебільшого ті розділи, що безпосередньо будуть використовуватись у практичній професійній діяльності або є необхідними при засвоєнні дисциплін професійної і практичної підготовки.

УДК 62-614; 004.942

Шамшин О. П.

ЦІЛОЧИСЕЛЬНА ЛІНІЙНА ЗАДАЧА ПОШУКУ ФІЗИКО-ХІМІЧНОГО СКЛАДУ ПММ З УРАХУВАННЯМ ВЛАСТИВОСТЕЙ СКЛАДОВИХ

Комп'ютерна розробка хімічних продуктів дозволяє уникнути рутинного вибору, сортування й синтезу з величезного числа хімічних речовин і сполук, звузивши поле пошуку до конкретних груп з’єднань, що володіють перспективними властивостями для одержання кінцевого продукту з заданими характеристиками. Отримання необхідних значень фізико-хімічних властивостей як рідких, так і газових паливно-мастильних матеріалів, що мають високе октанове (цетанове) число, протидетонаційний індекс, тиск насичених і сухих пар, оптимальний фракційний склад, щільність, плинність, в'язкість, молекулярну масу, необхідні експлуатаційні параметри оксигенатів, анілінів, ароматичних вуглеводнів, присадок, що підвищують октанове число, значення теплоти згоряння, швидкості горіння, меж займистості і т. і. можливо при комп'ютерній обробці молекулярної структури оксигеновмісного органічного палива.

Оскільки практично всі паливні суміші є складними хімічними комплексами, то розробка кінцевого продукту включає проведення таких видів аналізу: молекулярного, суміші, взаємодії властивостей палива й фізико-механічних характеристик двигуна внутрішнього згоряння.

Молекулярний аналіз дозволяє безпосередньо визначити первинні параметри компонентів і вторинні параметри сполук, виходячи з хімічного складу. На другому кроці робиться аналіз залежностей функціональних властивостей чистих і змішаних компонентів від зовнішніх параметрів (температури, тиску, концентрації). Третій крок розробки – аналіз властивостей суміші в різних термодинамічних процесах і вимагає розв'язку рівнянь стану, зв'язку, теплового балансу, побудови феноменологічної моделі.

Комплексна методологія комп'ютерного проектування паливних сумішей і одержання змішаних продуктів бензиноподібних і дизельних палив формулюється як нелінійна програма інгредієнтів, що змішуються, розв'язувана розкладанням на ряд підпрограм (підзадач), тобто за допомогою послідовної редукції по кандидатах на змішування. Така редукція спрощує первісне завдання й дозволяє знайти оптимальні компоненти суміші, приймаючи в якості основного інгредієнта граничні, негранічні, нафтенові вуглеводні, включаючи ароматичні. Однак, останнім часом для розробки паливних сумішей з необхідними фізико-

хімічними властивостями й відповідним ним хімічним складом використовується автоматичний генератор реакцій, що базується на аналізі потоку мережі реакцій. Оптимізаційна задача пошуку необхідної сполуки вирішується як цілочисельна лінійна задача (ЦЛЗ).

У роботі в рамках ЦЛЗ проведений композиційний аналіз бензинових сумішей з метою одержання максимальних характеристик ефективності фракційної сполуки, що впливають на експлуатаційні характеристики ДВС – повнота згоряння, час прогріву, надійність пуску, зносостійкість деталей, економічність і т. і.

УДК 614.846.6, 623.4.01

Толкачов А. М., Сидоренко І. І.

ПЕРСПЕКТИВНІ ПАРАМЕТРИ ВОДЯНОЇ ГАРМАТИ WG РУЙНУЮЧОЇ ДІЇ

Розглядаються додаткові можливості запропонованою раніше авторами водяної гармати (WG) із використанням дрібномасштабної турбулентної течії. Розробка WG мала мету збільшення дальності прицільного метання води, яка була недосяжною для струминних водометів не дуже великої потужності.

Одночасно з основною метою природно виникає можливість використання руйнівної потужності снаряда WG. Існує достатньо обставин, коли доцільно замість вибухової дії снаряду використати тільки його кінетичну енергію, наприклад, для руйнування старих будівель чи усунення заторів на річках під час льодоходу або повіні. Досить прості рішення запровадження ударних технологій демонструють приклади використання у якості снарядів контейнерів з водою і навіть бляшанок з напоями. Однак необхідність виготовлення контейнера дискредитує саму технологію.

У разі використання водяного снаряда без оболонки необхідно враховувати незвичайність його як ударного засобу. При великій швидкості деформації вода веде себе як нестисливе тіло, однак досягнення такого стану рідини стає можливим лише при великій швидкості снаряда під час зіткнення з перепоною. У даному випадку удар слід розглядати як дію з рівномірним тиском на перепону на протязі часу Δt, впродовж якої снаряд втрачає свій імпульс $\Delta p = p$. Середнє значення зусилля за цей час подається виразом $F = \Delta p / \Delta t$.

Подальший аналіз руйнівної дії снаряду WG потрібує реальних значень параметрів елементів пристрою. Вони будуть виявлені лише в результаті дослідження конструкції WG на практиці. Наразі використаємо припустимі, на думку авторів, значення: швидкості снаряду – $\upsilon = 100$ м/с, його маси – $m = 2$ кг і відповідного об'єму – $V = 2 \cdot 10^3$ см^3 або 2 літра. Слід зазначити, що вибір значення перерізу S снаряду суттєво і суперечливо впливає на його аеродинаміку польоту та на протяжність часу Δt, тому було обране найменше з ймовірних значень S = 10 см^2, що відповідає діаметру снаряда d = 3.56 см. При заданому об'ємі V це дає довжину водяного снаряду $L = 2$ м.

Використання обраних значень параметрів дозволяє обчислити $\Delta p = m\,\upsilon = 200$ кг·м/с, $\Delta t = L / \upsilon = 2 \cdot 10^{-2}$с = 20 млс (мілісекунд), а також руйнівну силу снаряду $F = \Delta p / \Delta t = 1 \cdot 10^4$Н. Дія сили поширюється на площу контакту снаряду з перепоною S = 10 см^2 і створює на неї тиск 1000 Н/см^2 (застосовувати системну одиницю тиску Паскаль у даному разі незручно).

Порівняємо одержане значення тиску з міцністю, наприклад, цегляної кладки. Таке завдання не зовсім визначене через велику кількість будівельних матеріалів та засобів їх застосування. В галузі будівництва для кладки із цегли М100 на цементному розчині користуються граничним значенням міцності до удару R = 13 кг/см^2 (мається на увазі кілограм-сила), що відповідає значенню 130 Н/см^2. Таким чином руйнівна дія водяного снаряда WG

з обраними параметрами у 7,7 разів перевищує міцність цегляної кладки. Це дуже обнадійливий результат. Між іншим, енергія водяного снаряда становить $1 \cdot 10^4$ Дж.

Можна очікувати менше значення сили удару через втрату швидкості снаряду в польоті а також не перпендикулярний напрямок удару до об'єкта. Однак втрату імпульсу можна корегувати збільшенням маси снаряда через збільшення його діаметру. Таким чином не виникає сумнівів щодо можливості використання водяної гармати WG у руйнівних завданнях.

УДК 378

Сидоренко І. І., Нефедов О. П.

ТЕСТИ MULTIPLE CHOICE ЯК АЛЬТЕРНАТИВА ЕКЗАМЕНАЦІЙНИМ БІЛЕТАМ З ВИЩОЇ МАТЕМАТИКИ

Традиційно склалося так, що підсумковий контроль з вищої математики проходить у вигляді класичного екзамену, у рамках якого курсант відповідає на два практичних питання та одне теоретичне питання, взяте зі списку, що був виданий курсанту заздалегідь. Умови такого підсумкового контролю зазначені у силабусі навчальної дисципліни. Однак практика показує, що с кожним роком число курсантів, що успішно складають такий іспит, знижується та є усі підстави вважати, що така тенденція буде зберігатися у наступні роки.

На таку статистику впливає низка факторів, а саме: недостатня шкільна підготовка, звичка працювати з репетитором (для абітурієнтів, що поступають у ВНЗ відразу після школи), відсутність звички систематичного виконання завдань на самопідготовку і, як наслідок, недостатньо сформована навичка працювати самостійно.

Однак, на думку авторів на успішність підсумкових атестацій також впливає невідповідність формату семестрових іспитів до формату тестів ЗНО, що усталено сформувалися у освітній системі за останні 15 років. Особливо це стосується фундаментальних дисциплін, зокрема вищої математики, семестрові екзамени проводяться за традиційною системою, що збереглася ще з радянських часів.

З огляду на вищесказане, авторами розроблена та апробована тестова система семестрового екзамену Multiple Choice з курсу математично-природничих дисциплін, яка була створена у рамках звичного курсантам тестового формату державної системи освіти. В основі питань тестів покладено застосування аналітичних здібностей курсантів, що вимагає логічного та творчого підходу при розв'язку завдань. Дана система дозволила здійснити диференційований підхід до тих хто навчається та дала можливість значно покращити успішність підсумкової атестації у рамках окремого потоку командно-штабного факультету.

УДК 378.

Нефедов О. П., Сидоренко І. І.

БАЗОВІ КОМПЕТЕНТНОСТІ КУРСАНТА ТА ЇХ КОРЕЛЯЦІЯ З УСПІШНІСТЮ ПІДСУМКОВОЇ АТЕСТАЦІЇ

Педагогічна наука виокремлює два важливих фактори, що разом з іншими визначають позитивний ефект у засвоєнні навчального матеріалу у вищій школі. Перший фактор – це мотивація курсанта на засвоєння навчальної програми. При цьому сила мотивації може бути різної потужності та мати різні джерела – як внутрішні (особисті моти-

ви), так і зовнішні, що і є результатом організації навчального процесу у вищому навчальному закладі. Далі розглядається тільки перший варіант, оскільки за свідченням педагогічної та психологічної науки, він є найбільш ефективним, має довготривалий результат у навчанні та позитивну психологічну дію.

Другий фактор успішного засвоєння навчального матеріалу вищої школи є базисний або вхідний рівень знань першокурсника за окремою дисципліною та степінь сформованості його освітніх компетенцій. Цей фактор є основоположним у вивченні фундаментальних дисциплін, у першу чергу вищої математики.

Багаторічна статистика результатів підсумкових атестацій в Національній Академії Національної гвардії України свідчить про те, що навіть при наявності високої мотивації першого типу у того, хто навчається, але при низькому вхідному рівні знань потрібний ефект в успішності не досягається. За аналізом результатів вхідного контролю за останні 5 років, рівень базових знань абітурієнтів з шкільного курсу, необхідних для засвоєння вищої математики на оцінку E-D за системою ECTS, виявляється катастрофічно низьким. Згідно статистики за останні 5 років, проведеної у рамках навчальних груп першого курсу, 75-85% тих, хто навчається слабо знають арифметику, не володіють елементарними поняттями та означеннями алгебри, геометрії та початку аналізу. Такі важливі уміння, як дії з дробами, степенями, багаточленами, оперування поняттям функції однієї змінної, похідної функції, поняття вектору виявляються для цих курсантів необорною перешкодою у засвоєнні навчального матеріалу вищої школи навіть при наявності внутрішньої мотивації та позитивної мотивації ззовні.

Отже, дослідження показує, що виявлення кореляційної залежності між рівнем базовими компетенцій з математики у курсанта першого року навчання та результатами його підсумкових атестацій дозволяє скорегувати навчальний процес з метою підвищення успішності та якості знань як на організаційному рівні шляхом таргетованої виховної роботи з курсантами з низькою мотивацією, так і з методичної точки зору, наприклад, складанням портативних довідників з елементарної математики та проведенням факультативного курсу занять для окремих курсантів на централізованій основі за окремою програмою, яку доцільно складати кожного року з урахуванням актуальних результатів вхідного контролю. Дана низка заходів також дозволить здійснити диференціальний підхід у процесі вивчення дисципліни, що позитивно вплине на якість та успішність навчальної групи у цілому.

УДК 621.396. 6.019.3

Єльчанінов О. Д.

РОЗРАХУНОК ЧАСОВИХ ХАРАКТЕРИСТИК НАДІЙНОСТІ З ВИКОРИСТАННЯМ МАРКОВСЬКИХ ПРОЦЕСІВ

Визначення показників надійності дозволяє оцінити експлуатаційні властивості озброєння та військової техніки (ОВТ) на етапах проектування, виробництва або експлуатації і зробити висновок про їхню відповідність заданим вимогам і, таким чином, вжити заходів по забезпеченню необхідного рівня надійності.

Сучасне ОВТ є складними системами, для яких кількість розрізнених станів більше двох. Ознаки, за якими можуть розрізняти стани експлуатованої системи, можуть бути досить різноманітними: кількість елементів, що відмовили; режими роботи або заходи, які проводяться на системі (бойове застосування, технічне обслуговування, ремонт); типи або номери елементів системи, які у поточний момент часу використовуються за призначенням т.п.

Дуже потужним засобом, що дозволяює розв'язувати дуже широке коло експлуатаційних задач, включаючи розрахунок надійності складних систем, є марковські процеси.

Процес експлуатації складної системи можна подати у вигляді послідовності випадкових за тривалістю інтервалів, які у загальному випадку можуть бути випадковими або детермінованими, підпорядковуватися різноманітним законам розподілу зі сталими або змінними параметрами, бути залежними (корельованими) або ні й т.і.

Розрахунок середнього напрацювання на відмову системи, її середнього часу відновлення або простоювання (зберегання) та інших подібних часових характеристик у математичному сенсі є еквівалентним задачі знаходження середнього часу перебування системи в деякій підмножині станів системи.

Класичним підходом до розрахунку таких часових характеристик складних систем є використання теорії поглинаючих ланцюгів Маркова. Однак при цьому можуть виникати нездоланні обчислювальні проблеми, позв'язані, насамперед, з відшуканням коренів характеристичного рівняння.

Інший підхід полягає в припущенні існуванні стаціонарного режиму процесу експлуатації й розв'язанні відповідної йому системи лінійних рівнянь Ерланга. Він є набагато простішим й ґрунтується на розумінні періоду (циклу) регенерації марковського процесу.

У доповіді розлядається саме такий підхід до розрахунку часових характеристик надійності резервованих систем ОВТ.

УДК 623.618:519.686

Бекіров А. Е., Ковтуненко Н. М.

МЕТОД ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ МОВНИХ ПОВІДОМЛЕНЬ НА ОСНОВІ БАГАТОВИМІРНОГО ПСЕВДОВИПАДКОВОГО БІТОВОГО РОЗПОДІЛУ

На сьогоднішній день завдання забезпечення захищеності цифрового радіозв’язку вирішується на основі криптографічних алгоритмів. В той же час, для аналогових зразків обладнання радіозв’язку, які є на озброєнні Повітряних Сил Збройних Сил України, існує проблема забезпечення конфіденційності при обміні мовними повідомленнями. З одного боку, заміна існуючих аналогових бортових зразків апаратури на сучасні цифрові радіостанції вимагає значних матеріальних затрат та узгодження нормативних вимог та технічної документації. З іншого боку, існує критична необхідність захисту радіопереговорів, в тому числі під час виконання завдань в умовах Операції об’єднаних Сил. Існуючі методи захисту для аналогових радіостанції побудовані на принципі передачі мовного повідомлення у цифровому вигляді за допомогою частотної телеграфії. Обмеженнями при такому підході є значне зменшення якості мовних повідомлення та оперативності радіозв’язку. Актуальним напрямком досліджень є розробка методів захисту мовних повідомлень для передачі в аналоговому вигляді.

Серед найбільш розповсюджених методів є частотні та спектральні методи, недоліки яких обумовлені погіршенням якості зв’язку та необхідністю використання запам’ятовуючого пристрою. Використання спектральних методів вносить спотворення в результаті частотних перетворень навіть в умовах відсутності втрат та завад. Звідси пропонується обрати просторову область повідомлення для здійснення перетворень. Запропонований метод реалізується шляхом псевдовипадкового розподілу старших бітів вихідного повідомлення у цифровому вигляді. Використання старших бітів забезпечує стійкість повідомлення в умовах завад та збільшує ступінь відмінності вихідного та перетвореного повідомлення. Для внесення додаткових спотворень у трансформоване

повідомлення запропоновано представляти двійковий масив вихідного повідомлення у багатовимірному просторі. В цьому випадку псевдовипадковий розподіл бітів в елементі просторового представлення, елементів в субфрагменті та субфрагентів мовного повідомлення відбувається на основі визначеного закону. Ключову інформацію пропонується обирати окремо для кожної псевдовипадкової послідовності. Для забезпечення однозначного відтворення вихідного мовного повідомлення на приймальній стороні пропонується додавати нульові розряди на позиції старших біт елементів субфрагментів. В цьому випадку кількість біт на представлення кожного елементу є однаковою.

На приймальній стороні здійснюється побудова багатовимірного двійкового простору по заздалегідь відомому правилу. Характеристики побудови простору, а саме довжина фрагментів та субфрагментів, частота дискретизації та розрядність перетворення уявляє собою ключову інформацію. Другий етап зворотного перетворення передбачає побудову трьох вихідних псевдовипадкових послідовностей для побудови площини старших біт відтвореного вихідного мовного повідомлення.

Дорошенко Ю. А., Скворок І. М.

ІННОВАЦІЙНА ДІЯЛЬНІСТЬ ЯК ЗАСІБ ПІДВИЩЕННЯ ЯКОСТІ ПІДГОТОВКИ ОФІЦЕРІВ ЗАПАСУ

Сучасний стан розвитку національної системи освіти характеризується докорінними змінами, які відбуваються в усіх сферах життя нашого суспільства. Характерною ознакою цього періоду є творчий пошук інноваційних технологій у педагогічній та психологічній науці з метою вироблення політики стратегічного управління розвитком системи освіти України, підвищення якості підготовки фахівців, що є базовими для соціально-економічного, культурного становлення та розвитку суспільства. Невіддільною складовою цього процесу є система військової освіти.

Актуальність дослідження інноваційної діяльності в системі підготовки військових фахівців кадру та запасу усіх ступенів освіти та рівнів військового управління зумовлена подальшим реформуванням Збройних Сил України у відповідності з вимогами сучасних нормативно-правових документів з безпекової та оборонної політики держави, курсу на зближення з НАТО; інформатизацією освіти і науки, зниженням якості підготовки військових фахівців; формуванням нової ідеології стандартів вищої військової освіти на основі компетентнісного підходу; потребою зміни підходів щодо фінансування та матеріально-технічного забезпечення освіти [3; 4].

Поняття "інновація" походить від латинського – "оновлення, новизна, зміна". Новизна при цьому – це ідея, що є для конкретної особи новою, а також втіленою в практику. На думку С. М. Ніколаєнко, – "Інноваційна діяльність – вид діяльності, що виникає внаслідок пошуку новизни, оригінальних і ефективних рішень, яких раніше не існувало"[2, с. 416]. Л. І. Даниленко розглядає інновацію не лише як кінцевий результат упровадження нового, а й як новостворені або вдосконалені технології навчання, виховання, управління, які істотно змінюють структуру та якість освітнього процесу [1].

Рушійною силою, джерелом інноваційного розвитку військово-освітнього процесу, що реалізується в системі військової освіти, є об’єктивно притаманні йому суперечності. Вони виражають його специфіку, багатоманітність і спонукають до інноваційної діяльності. Виділимо деякі групи таких суперечностей, що мають місце в підготовці офіцерів запасу.

По-перше, це суперечності між вимогами до високої якості підготовки офіцерів запасу та її реальним станом; між досягненнями сучасної науки, озброєння та військової техніки та ступенем відображення їх в системі підготовкиі офіцерів запасу; між вдосконаленими способами бойових дій і методикою їх вивчення тощо. Головною умовою

розв'язання цих суперечностей є глибоке розуміння та оперативна реалізація через систему інновацій вимог держави до підготовки офіцерських кадрів запасу.

По-друге, це суперечності процесу формування особистості майбутніх офіцерів запасу в системі військової освіти: між цілісним характером формування особистості та мірою розвитку її окремих якостей; між прагненнями особистості та її реальними можливостями, між старими (тими, що склалися) і новими способами діяльності тощо. Головною умовою розв'язання суперечностей цієї групи є допомога майбутнім військовим фахівцям у їх усвідомленні та розв'язанні.

По-третє, суперечності, власне педагогічного характеру: між навчанням, розвитком, психологічною підготовкою офіцерів запасу та їх самовихованням, самоосвітою; між навчально-виховними впливами суб'єктів освітнього процесу та рівнем підготовленості, вихованості фахівців і військових колективів. Основними умовами їх розв'язання є піклування командування та науково-педагогічного складу щодо військово-професійної спрямованості освітнього процесу; наближення процесу навчання до умов бойової обстановки; постійне підвищення рівня педагогічної культури та методичної майстерності; цілеспрямоване керівництво самовихованням і самоосвітою.

По-четверте, це суперечності, що носять випадковий характер і були викликані суб'єктивними факторами – це різного роду відхилення від вимог військових статутів, інструкцій, відстала матеріально-технічна база, низька організація освітнього процесу, недостатня психолого-педагогічна підготовка науково-педагогічних працівників і т.ін.

Форми прояву та розв'язання суперечностей військово-освітнього процесу в системі підготовки офіцерів запасу багатоманітні. Але всі вони виступають для учасників інноваційних процесів у вигляді певних труднощів, подолання яких вимагає великої напруги, розумових і фізичних сил, творчого відношення до справи, спільних і зустрічних зусиль суб'єктів викладання та навчання .

Зупинимося тепер на конкретних методологічних підходах щодо здійснення інновацій в системі підготовки офіцерів запасу. Вони зводяться до наступного.

По-перше, слід впевнитися в недосконалості, неефективності, застарілості тієї військово-освітньої структури чи типу управлінської, педагогічної діяльності, яку планується реформувати. Об'єктивною основою в цьому випадку є аналіз і оцінка військово-освітньої системи за надійними критеріями, а саме: реальний розвиток професійної компетентності майбутніх офіцерів запасу, готовність їх до служби в Збройних Силах України, прагнення навчатися протягом подальшої служби тощо.

На другому етапі проведення інновацій слід шляхом широкого, ретельного аналізу провести пошук передових педагогічних технологій, зразків освітніх рішень, що носять випереджувальний характер і можуть бути використані для моделювання новацій, таких, що прийдуть на зміну застарілому та неефективному. При цьому слід відшукати передовий, прогресивний досвід як у вітчизняній, так і світовій практиці,

Наступним, *третім кроком* в ланці перетворень військово-освітньої системи є проектування її інноваційної моделі від ескізу до робочих проектів. Тобто створюється модель освітньої новації з конкретними, певним чином визначеними, властивостями, що відрізняють її від традиційного варіанту, на зміну якому вона пропонується.

Четвертим етапом методології перетворення освітньої структури є практичне здійснення новацій, побудова алгоритму втілення їх у практику.

Застосування методології інноваційних перетворень в системі підготовки офіцерів запасу має на меті надання реформаторському освітньому процесу наукового характеру, практичної спрямованості, запобігання втрат матеріальних та інтелектуальних ресурсів, сприяння підвищенню його ефективності.

Список використаних джерел

1. Даниленко Л. І., Паламарчук В. Ф. Наукові засади інноваційної освітньої діяльності в Україні // Постметодика. 2004. № 2-3. С. 16–20.

2. Ніколаєнко С. М. Теоретико-методологічні основи управління інноваційним розвитком системи освіти України: [монографія]. – К.: Київськ. НТЕУ, 2008. 419 с.

3. Указ Президента України від 24 вересня 2015 року 5287/2015 "Про Стратегію національної безпеки України". [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015.

4. Указ Президента України від 25 червня 2013 року №344/2013 “Про Національну стратегію розвитку освіти в Україні на період до 2021 року” [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/ru/documents/15828.html.

Мороз І. В., Чугуй Г. Є.

ІНФОРМАТИЗАЦІЯ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ ЯК ЗАСІБ ПІДВИЩЕННЯ ЇХ ГОТОВНОСТІ ДО ВЕДЕННЯ СУЧАСНИХ ВИДІВ ЗБРОЙНОЇ БОРОТЬБИ

Науково обґрунтовано, що інформатизація освіти є однією із найважливіших умов успішного, сталого розвитку суспільства, його конкурентоспроможності та обороноздатності. Однією з головних умов успішної реалізації основних засад розвитку інформаційного суспільства в Україні є забезпечення навчання, виховання, професійної підготовки людини для роботи в інформаційному суспільстві. Для цього необхідно: розвивати національний науково-освітній простір, розробити методологічне забезпечення використання комп'ютерних мультимедійних технологій, забезпечити пріоритетність підготовки фахівців з інформаційно-комутаційних технологій [1]. Стратегією національної безпеки України передбачено створення ефективного сектору безпеки і оборони…, запровадження інтегрованої системи освіти, бойової і спеціальної підготовки персоналу для органів сектору безпеки і оборони із залученням викладачів, інструкторів із держав-членів НАТО, ЄС, формування нової культури безпеки [2].

Інформатизація є важливою складовою системи підготовки військових фахівців. Про це свідчать досвід функціонування військових навчальних закладів провідних країн НАТО, світу, проведення Антитерористичної операції на сході України, операції Обєднаних сил, сучасні погляди на ведення збройної боротьби.

Метою інформатизаціїї військової освіти є створення всебічних умов для забезпечення всіх учасників освітнього процесу своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки. При цьому діяльність має спрямовуватись на такі дії: розроблення інструктивних, організаційних, змістових, науково-технічних, економічних, фінансових, методичних передумов процесу інформатизації підготовки військових фахівців; застосування та розвиток сучасних інформаційних технологій; створення бази інформаційних ресурсів; розвиток локальних та глобальних мереж інформаційного забезпечення освітнього процесу; підвищення якості підготовки військових фахівців на основі широкого використання інформаційно-комунікаційних технологій; продукування та запровадження інноваційно-інформаційних продуктів і послуг; інтеграція військової освіти в національний і зарубіжний інформаційний простір; формування системи моніторингу освітнього процесу.

Інформація в сучасних умовах стає науковою і філософською категорією поряд з такими категоріями, як час, енергія, матерія. Зростання потреби в інформації і збільшення її потоків в людській професійній діяльності зумовлюють появу нових інформаційних освітніх технологій, теоретичною основою розроблення яких є інформатика, кібернетика, теорія систем. Проникнення в освіту нових інформаційних технологій змушує розглядати дидактику підготовки військових фахівців як процес інформаційний, що зумовлюється такими чинниками: комп'ютеризацією та автоматизацією всіх складових воєн-

ної сфери; зміною поглядів на ведення сучасних бою та операції; модульною побудовою сучасного озброєння, військової техніки та особливостями їх функціонування, бойового застосування та експлуатації; необхідністю системного формування змісту освіти та компетенцій фахівців на основі стандартів НАТО; переходом від інформаційно-знаннєвої моделі підготовки фахівців до компетентнісної; можливостями динамічного програмування та моделювання будь-яких процесів, дій, ситуацій; зростанням достовірності прогностичних даних для прийняття різних рішень на основі здобуття потрібної для цього інформації сучасними засобами спостереження, зв'язку та розвідки.

Серед основних напрямів, що притаманні процесу інформатизації освіти, можна виділити такі: використання національних і світових інформаційних освітніх ресурсів; виникнення нових форм підготовки та перепідготовки фахівців; розширення сфери використання технологій навчання в підготовці фахівців; поява інноваційних засобів навчання; використання засобів нових інформаційних технологій в позааудиторній роботі, що наближає навчальну діяльність до дослідницької, конструкторської, творчої; формування основ інформаційної культури в процесі вивчення навчальних дисциплін; інформаційно-технологічне забезпечення основних видів освітньої діяльності.

В процесі інформатизаії підготовки військових фахівців мають здійснюватися такі управлінські функції: інформатизація всіх сфер діяльності з підготовки фахівців; захист авторських прав та баз даних і програм різного призначення; визначення норм і правил використання засобів і продуктів інформатизації; забезпечення доступу учасників освітнього процесу до джерел інформації; заохочення розроблення та запровадження інноваційних програмних і технічних засобів інформатизації; підтримка прикладних наукових досліджень щодо пошуку швидкісних математичних і технічних засобів обробки інформації; підготовка та підвищення кваліфікації спеціалістів з питань інформатизації та інформаційних технологій; організація сертифікації програмних і технічних засобів інформатизації; фінансове, матеріально-технічне та безпекове забезпечення системи інформатизації підготовки військових фахівців.

Основні шляхи інформатизації військової освіти:

- оснащення навчальних закладів сучасними засобами інформаційних і комунікаційних технологій (ІКТ), використання їх як нового педагогічного інструментарію, що дозволяє суттєво підвищити ефективність освітнього процесу;
- використання сучасних ІКТ, інформаційних телекомунікацій і баз даних для інформаційної підтримки освітнього процесу, забезпечення можливості віддаленого доступу викладачів, курсантів (слухачів) до наукової і навчально-методичної інформації як у своїй країні, так і в інших країнах світового співтовариства;
- розвиток і широке розповсюдження дистанційного навчання, що дозволяє суттєво розширити масштаби та глибину використання інформаційно-освітнього простору;
- перегляд і радикальна зміна змісту освіти на всіх рівнях, що зумовлюється стрімким розвитком процесу інформатизації військової сфери; ці зміни на теперішній час орієнтуються не тільки на загальноосвітню та професійну підготовку тих, хто навчається, але також і на створення якісно нової моделі підготовки фахівців до служби та діяльності в складних умовах планування та ведення бою, операції, протидії тероризму, на формування та розвиток у майбутніх офіцерів необхідних для цього якостей, знань, умінь і навичок.

Пріоритетні завдання інформатизації військової освіти: забезпечення розвитку особистості майбутнього військового фахівця, його компетентності, готовності до ведення сучасних видів збройної боротьби, творчого, лідерського потенціалу; формування інформаційної культури фахівця; удосконалення управління освітою; створення інформаційних мереж і баз даних; інтенсифікація науково-технічних, психолого-педагогічних і науково-методичних досліджень; запровадження нових форм і технологій навчання військових фахівців, підготовки, перепідготовки та підвищення кваліфікації наукових і науково-педагогічних працівників.

Список використаних джерел

1. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки (Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102).

2. Указ Президента України від 24 вересня 2015 року 5287/2015 "Про Стратегію національної безпеки України". [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015.

Приходько Ю. І.

ОСОБИСТІСНА ОРІЄНТАЦІЯ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ ТАКТИЧНОГО РІВНЯ

Актуальність дослідження проблем особистісно орієнтованої підготовки військових фахівців тактичного рівня зумовлена такими чинниками: необхідністю впровадження вимог сучасних нормативно-правових документів щодо стратегії національної безпеки України, партнерства з країнами НАТО на основі військових освітніх стандартів, розвитку сектору безпеки та оборони, ідей гуманістичної освітньої концепції; врахуванням в процесі навчання потреб та індивідуально-психологічних особливостей особистості; вимогами щодо підвищення якості підготовки фахівців, схильних до творчої діяльності, лідерства; швидкоплинністю оновлення знань і поглядів на ведення збройної боротьби, боротьби з міжнародним тероризмом; вичерпаністю можливостей багатьох традиційних форм і методів підготовки фахівців; необхідністю пошуку та застосування інноваційних педагогічних технологій, спрямованих на активізацію пізнавальної діяльності тих, хто навчається, на якісне засвоєння навчального матеріалу, формування та розвиток компетенцій, мотиваційної сфери.

Основою практичної реалізації викладених чинників стають, набуваючи все більшого значення, освітні технології особистісно орієнтованої спрямованості як у викладанні навчальних дисциплін, так і в організації навчально-пізнавальної діяльності майбутніх фахівців [1; 2; 4]. Організація навчання на таких засадах сприяє формуванню та розвиткові особистості фахівця, спроможного виявляти ініціативу, творчо виконувати поставлені завдання, приймати відповідальні рішення, самостійно, критично мислити, продукувати ідеї, захищати власну точку зору, переконання, систематично й неперервно поповнювати знання шляхом наполегливої самоосвіти протягом життя. Як слушно відзначає В. В. Серіков, – концепція особистісно орієнтованої освіти полягає “у розкритті природи та умов реалізації особистісно-розвивальних функцій освітнього процесу, що невіддільно від більш глибокого та цілісного розуміння їх сутності” [4, с. 27].

Розроблення та запровадження засад особистісно орієнтованої підготовки військових фахівців дозволить:

- визначитися з пріоритетами наскрізного цілеутворення на всіх етапах підготовки фахівців;
- забезпечити системний, комплексний підхід до планування, організації та здійснення процесу навчання та викладання;
- покращити управління навчальним процесом, аналіз, прогнозування, проектування та діагностику рівня знань, умінь, навичок;
- забезпечити єдність навчання, виховання, розвитку фахівців, їх психологічну підготовку до практичної діяльності;
- оволодіти фахівцями не тільки певною сумою знань, практичних навичок, а й навчитись самостійно їх здобувати та використовувати;
- широко застосовувати сучасні інноваційні технології;

- підсилити мотивацію навчання, відповідальність за результати навчальної праці, стимулювати розвиток творчого мислення;
- сформувати у майбутніх військових фахівців індивідуальний стиль мислення, спілкування, лідерства, активної діяльності;
- набути навичок прийняття оптимальних рішень в широкому спектрі ризиконебезпечних ситуацій, що виникають в ході практичної діяльності.

Зміст особистісно орієнтованої підготовки військових фахівців, форми, методи та навчально-матеріальне забезпечення мають проектуватися на засадах варіативності. При цьому модель їх розроблення характеризується блочно-модульною побудовою навчального матеріалу, високим ступенем самостійності та індивідуалізації навчання.

Організація та методика особистісно орієнтованої підготовки військових фахівців має базуватися на засадах всебічного вивчення їх індивідуально-психологічних особливостей, сприйняття їх як суб'єктів навчального процесу. При цьому вивчається: спрямованість особистості та її види; інтелектуальність (ступінь розвитку та структура інтелекту); емоційність (рівень реактивності, стійкості, неспокійності); вольові якості (уміння долати труднощі, наполегливість в досягненні мети); комунікативність, ступінь товариськості; самооцінка (низька, адекватна, завищена); працездатність, рівень самоконтролю; швидкість і точність виконання завдань, задач, дій; спроможність до групової взаємодії; уміння розв'язувати складні завдання, діяти в нестандартних умовах.

Вивчення та врахування переважної більшості зазначених індивідуально-психологічних особливостей тих, хто навчається, здійснюються викладачем в процесі викладання навчальної дисципліни, позааудиторного спілкування, індивідуальних бесід тощо і не потребує застосування спеціального інструментарію.

Методичну основу особистісно орієнтованого навчання на різних видах занять становить пошук та запровадження ефективних способів комунікативного впливу викладача та типів взаємодії з тими, зто навчається.

Важливою складовою особистісно орієнтованої підготовки військових фахівців є коригування педагогічної діяльності за результатами усіх форм контролю та самоконтролю. До основних елементів, які мають коригуватись, слід віднести такі: рівень цілепокладання; система потреб і мотивів діяльності суб'єктів навчального процесу; модель педагогічної та процесуальної діяльності (ефективність навчально-методичної роботи); уміння викладача конструювати навчальні завдання у відповідності з інтелектуальними та психофізіологічними можливостями тих, хто навчається; співвідношення реального характеру впливу викладача на майбутніх фахівців із загальногуманістичними та демократичними принципами взаємодії (суб'єкт-суб'єктні відносини); подолання стресових і конфліктних ситуацій (ступінь прив'язаності до реальних умов викладання навчальних дисциплін); подолання стереотипів і тенденцій до жорсткої алгоритмізації викладацької діяльності (індивідуальна система засобів педагогічної дії); система педагогічного контролю; комплексність засобів педагогічного впливу; ступінь і повнота матеріально-технічного та методичного забезпечення навчальних занять [3].

Висновки. Складовими організації і методики особистісно орієнтованої підготовки військових фахівців є такі: конструювання пакетів навчальних завдань на різні види занять з вивчення теоретичного та практичного матеріалу; вивчення індивідуально-психологічних особливостей тих, хто навчається і, в першу чергу, їх інтелектуальних здібностей та працездатності; організація та методика проведення різних видів навчальних занять з особистісно орієнтованим спрямуванням і використанням засобів спілкування та діалогізації; діагностика (контроль), моніторинг результатів навчально-пізнавальної діяльності суб'єктів навчання; коригування педагогічної діяльності.

Список використаних джерел

1. Богданова І. М. Технології в освіті: теоретико-методологічний аспект: монографія. Одеса: ТЕС, 1999. 146 с.

2. Пєхота О. М. Особистісно орієнтована освіта і технології / Неперервна професійна освіта: проблеми, пошуки, перспективи: монографія / За ред. І. А. Зязюна. Київ: Видавництво “Віпол”, 2000. 636 с.

3. Приходько Ю. І. Особистісно орієнтована самостійна робота як новий етап у еволюції поглядів на її природу // Зб. наук. праць “Вісник Національної академії оборони України. К.: МО України, НУОУ. 2010. № 5(18). С. 77–84.

3. Сериков В. В. Образование и личность. Теория и практика проектирования педагогических систем. М.: Логос, 1999. 272 с.

УДК 355/359. 159.9. 371.378

Шаповалов Б. Б.

ПОЛІЦЕЙСЬКИЙ ХОРТИНГ ЯК СИСТЕМА І СКЛАДОВА ДІЯЛЬНОСТІ СИЛОВИХ СТРУКТУР

Серед сучасних загроз національній безпеці України слід відзначити такі: корупція; діяльність кримінальних груп і незаконних збройних формувань; тероризм; котрабанда; зростання злочинності; рейдерство; порушення громадського порядку, прав громадян, екологічних норм; незаконне використання вогнепальної зброї тощо. Стратегією національної безпеки України [3] визначено шляхи досягнення цілей і реалізації пріоритетів державної політики у сферах національної безпеки, громадської безпеки та цивільного захисту України. Зокрема, Стратегією громадської безпеки та цивільного захисту передбачено: 1) готовність сил та засобів виконувати завдання за призначенням, інфраструктуру, напрями розвитку, інші показники, необхідні для планування діяльності Міністерства внутрішніх справ України, Національної гвардії України, Національної поліції України, Державної прикордонної служби України, Державної міграційної служби України, Державної служби України з надзвичайних ситуацій…; 2) державні програми, галузеві стратегії та програми, які мають бути спрямовані на реалізацію Стратегії громадської безпеки та цивільного захисту України, їхні цілі, відповідальних за розроблення документів, моніторинг їх виконання та оцінки.

Створення та функціонування поліцейського хортингу, на нашу думку, має сприяти успішному виконанню завдань, визначених Стратегією національної безпеки України, Законом України "Про національну безпеку України" [1; 3], підвищенню ефективності діяльності силових структур, покращенню професійної підготовки, перепідготовки, рівня кваліфікації працівників правоохоронних органів, військовослужбовців, працівників рятувальних служб, персоналу охорони тощо [2; 4].

Поліцейський хортинг заснований з урахуванням потреб правоохоронної діяльності, силових структур та є важливою складовою військово-патріотичного виховання молоді, засобом формування готовності людини до поведінки в екстремальних ситуаціях шляхом залучення військових, правоохоронців, рятівників та інших груп населення до тренувальної та змагальної діяльності. Завданнями поліцейського хортингу є: пропаганда здорового способу життя, розвиток фізичних, морально-вольових, інтелектуальних здібностей, технічна, тактична та психологічна підготовка працівників поліції, інших правоохоронних органів, силових структур. Універсальність поліцейського хортингу полягає у тому, що військові, працівники правоохоронних органів та рятувальники спільно реагують на загрози найвищим цінностям України. В умовах збройної агресії та миротворчих місій, як відомо, на військових покладаються обов’зки, характерні для поліцейської діяльності, зокрема, не-

сення служби на блокпостах, патрулювання районів зі складною оперативною обстановкою, супроводження конвоїв, проведення обшуків тощо [4; 5].

Поліцейський хортинг є: 1) національним філософським, духовним феноменом нашої держави; 2) професійно-прикладним спортом, в якому акумульовано бойові традиції українського народу та напрацювання в галузі національного бойового мистецтва «хортинг», імплементовано сучасні передові технології самозахисту; 3) системою окремих розділів спортивних єдиноборств, притаманних лише цьому виду спорту, що надає йому характеру яскравої індивідуальності та неповторності.

Поняття поліцейського хортингу є динамічним і змінюється відповідно до його розвитку, умов життя, тенденцій (негативних чи позитивних) криміногенної обстановки тощо. На теперішній час поліцейський хортинг визначається як система, як складова діяльності силових структур і містить такі компоненти:

- загальну та прикладну філософію, психолого-педагогічну теорію та практику;
- комплекс нормативних, науково-методичних, навчально-методичних матеріалів і документів;
- педагогічні технології: 1) професійної підготовки працівників правоохоронних органів, військовослужбовців, працівників рятувальних служб та персоналу охорони; 2) формування та розвитку готовності громадян до дій в екстремальних ситуаціях; 3) оздоровчі та реабілітаційні; 4) агітаційні;
- широкий комплекс дій і прийомів (бойове мистецтво, професійно-прикладний вид спорту, засіб формування та розвитку духовних цінностей, морально-психологічної стійкості);
- набір тренінгових, контрольних, моніторингових, коригувальних заходів і процедур;
- календар проведення міжнародних і національних змагань, агітаційних та показових заходів;
- узагальнений досвід діяльності фахівців силових структур України, провідних країн НАТО в міжнародних місіях з підтримання миру та безпеки, в екстремальних ситуаціях.

Кожний з компонентів психолого-педагогічної системи містить певні елементи, що пов’язані між собою дією та взаємодією. Навчальні заняття та тренінги суттєво підвищують військово-професійну, морально-психологічну підготовку; залучення працівників правоохоронних органів, військовослужбовців, працівників рятувальних служб та персоналу охорони до спортивних змагань підвищує ефективність їх професійної, фізичної підготовки; заняття поліцейським хортингом як видом спорту сприяє реабілітації осіб, що перебували в екстремальних ситуаціях, зокрема, учасників бойових дій у різних регіонах світу, Антитерористичної операції та операції Об’єднаних сил на сході України.

Подальшим розвитком Системи підготовки людини до дій в екстремальних ситуаціях стало створення Системи самозахисту та виживання і Поліцейської системи самозахисту та контролю, які є такими, що постійно оновлюються, зважаючи на теоретичні здобутки психолого-педагогічної науки, напрацювання з інноваційних форм, методів і засобів боротьби зі злочинністю, прийняття нових нормативно-правових документів тощо.

Список використаних джерел

1. Закон України "Про національну безпеку України" // (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241).

2. Єрьоменко Е. А. Філософсько-методологічні засади поліцейського хортингу як підготовча база працівників поліції в Україні [Електронний ресурс]. – Режим доступу: http://horting.org.ua/node/41568.

3. Указ Президента України від 24 вересня 2015 року 5287/2015 "Про Стратегію національної безпеки України". [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015.

4. Шаповалов Б. Б. Поліцейський хортинг як вид спорту та система формування готовності до дій в екстремальних ситуаціях // Теорія і методика хортингу. 2015. Вип. 3. С. 124–129.

5. Шаповалов Б. Б. Сучасні педагогічні технології формування готовності поліцейських до дій в екстремальних ситуаціях. // Сучасні проблеми правового, економічного та соціального розвитку держави: тези доп. V Міжнар. наук.-практ. конф., м. Харків, 18 листопада 2016 року. Харків: ХУВС. С. 389–391.

УДК 621.396.962

Herasimov S., Roshchupkin E.

STATISTICAL ANALYSIS OF HARMONIC SIGNALS FOR TESTING OF ELECTRONIC DEVICES

Nowadays, when electronics deeply penetrates in all spheres of human being via electronic devices from smart pocket devices to sophisticated computerized and robotized networks of systems with elements of artificial intellect, in many cases control of their proper functionality becomes of survival importance. Despite vast variety of such devices, which differ essentially by their functions, operation and design, commonly all of them are based on typical elementary electronic modules, such as power supplies, signal generators, amplifiers, filters, triggers, modulators, etc. The latter implies that their functional state can be monitored with universal controllers. Development of universal testing techniques capable for monitoring of electronic schemes and design of corresponding controllers are in great demand. Testing of electronic schemes with harmonic signals is one of the possibilities for universalization of testing protocols.

The principle of such an approach is as following. A harmonic signal from a generator is applied to the entrance of the inspected part of the electronic scheme of the device [1, 2]. The entrance testing signal is typically of the form $\cos^{k}\left(n\cdot\varphi+\delta\cdot\pi/2\right)$, where k and n are natural (positive integer) numbers, φ is the phase, measured in radians and δ takes the value 0 or 1 for the cosines or sinusoidal signals respectively. Depending on the type of the inspected module the output signal differs (usually by its phase and amplitude) from the input signal but is expected to be of a form standard for a given unit. In case of malfunction the output signal is affected additionally. Analysis of the deviation of the output signal from the expected standard form is used for conclusion on the technical state of the inspected unit. In this case, the parameter φ of the harmonic function can be considered as the initial phase of the signal, the statistical behavior of which was studied in details in [2].

However, in most practical cases, the parameter φ per se is of no importance, being usually known (for a standard signal). Instead, the value of its harmonic function is of interest. The latter is related to a specific functioning mode of many devices (such as selsyns, encoders, phase detectors, etc.), which deal with the harmonic function, rather than with φ. The same is for “indirect measurements”, at which the conclusion on the technical state of a device is also formulated via analysis of the measured valued of the harmonic function.

Truncation at the first term of the serial expansion of the output signal in assumption of high “signal-to-noise (s/n) ratio, often results in acceptable predicted s/n ratios of which was studied in details in [1]. However, consideration of next expansion terms is evidently needed for essentially non-linear signals [2]. Statistical analysis of testing harmonic signals in terms of varying parameters is thus in demand. To the best of our knowledge, handy expressions for statistical characteristics of the tested values of signals with harmonically varying parameters are not available in literature. Therefore, the aim of this paper is to derive statistical characteristics of harmonic functions of errors varying normally in accordance with Gaussian distribution.

Then, signals equal to $T\cdot\exp\left\{-\left(n\cdot\sigma_\varphi\right)^2\right\}$ and *T* from the output of the adders Σ_1 and Σ_2, respectively, are sent to the scheme of comparison and control, where *T* is the known accumulation time. From the output of the divider Σ_2/Σ_1, a signal equal to $\exp\left\{-\left(n\cdot\sigma_\varphi\right)^2\right\}$ arrives to the logarithmic amplifier $-\mathrm{Ln}(\Sigma_2/\Sigma_1)$, from the output of which the voltage $\left(n\cdot\sigma_\varphi\right)^2$ is obtained. The value of the voltage at the output of the adder Σ_1, different from *T*, indicates the non-quadrature character of the channels, i.e. the latter indicates the introduction of a $(\pi/2+\xi)$-phase shift by the phase-shift module, where ξ is the phase error. In such a case, the input of the controlled inverter receives a signal about the change in the sign of the entrance useful signal. The difference between the direct and inverted signals from the outputs of the adders Σ_1 and Σ_2 in the scheme of comparison and control will be of the form

$$\begin{aligned}\Sigma_1:\Delta^{\pm}_{\Sigma_1}&=\left(M^2\left[\cos(\varphi_n)\right]+M^2\left[\sin(\xi+\varphi_n)\right]\right)-\left(M^2\left[\cos(-\varphi_n)\right]+M^2\left[\sin(\xi-\varphi_n)\right]\right)=\\&=T\cdot\frac{4\cdot\cos(\varphi_{0n})\cdot\sin(\varphi_{0n})\cdot\cos(\xi)\cdot\sin(\xi)}{\exp\left\{\left(n\cdot\sigma_\varphi\right)^2\right\}}\end{aligned}\tag{1}$$

$$\begin{aligned}\Sigma_2:\Delta^{\pm}_{\Sigma_2}&=M\left[\left(\cos^2(\varphi_n)+\sin^2(\xi+\varphi_n)\right)\right]-M\left[\cos^2(-\varphi_n)+\left(\sin^2(\xi-\varphi_n)\right)\right]=\\&=T\cdot\frac{4\cdot\cos(\varphi_{0n})\cdot\sin(\varphi_{0n})\cdot\cos(\xi)\cdot\sin(\xi)}{\exp\left\{2\cdot\left(n\cdot\sigma_\varphi\right)^2\right\}}\end{aligned}\tag{2}$$

where the values of the functions $\cos(n\varphi_0)$ can be preliminarily estimated with the accuracy to a factor $\exp\left\{-\left(n\cdot\sigma_\varphi\right)^2/2\right\}$ by the values of the voltages, taken from the outputs of the integrators, respectively.

Thus, using the difference between the direct and inverted signals as a mismatch signal, the phase shift in the phase-shift module is eliminated, since $\Delta^{\pm}\to 0\big|_{\xi\to 0}$. The proposed scheme allows for control of the quadrature of the channels of the device, for measuring of the noise level as well as for the estimation of the dispersion of measurement errors, and can be used in existing and future control and monitoring systems.

We have derived expressions for mathematic expectation *M*, dispersion *D* and the error Δ*M* for four harmonic functions $F_i(\varphi_n)$ with the parameter φ_n varying normally in accordance with Gaussian distribution. On the basis of the obtained relationships, the scheme of the controller is proposed, which allows for testing of the channels quadrature, measuring the noise level and estimating the dispersion of the measurement errors. Obtained results can be used for testing of vast variety of existing and future systems of data processing, measuring systems and control systems.

References

1. Асавалюк А. В., Герасимов С. В., Рощупкін Є. С. Похибки визначення повного вектора швидкості в єдиній прямокутній системі координат системою оглядових станцій радіолокації з різною точністю // Системи озброєння і військова техніка. – Х.: ХНУПС. – 2017. – Вип. 2 (50). – С. 53-56.

2. Герасимов С. В., Рощупкін Є. С. Теоретические основы оценки ошибок значений сигналов с гармонически меняющимися параметрами // Озброєння та військова техніка. – 2018. – Вип. 2 (18). – С. 43-49.

УДК 621.396.962

Кудряшов В. Є., Литовченко Д. М.

ДВОБАЗОВА СИСТЕМА ПРИЙОМУ РАДІОМЕТРИЧНИХ СИГНАЛІВ

На основі підходу [1, 2] вважаємо, що об'єкт картографування випромінює коливання у вигляді випадкового стаціонарного процесу з нормальним законом розподілу та оброблювальні сигнали досить широкосмугові.

Правило виявлення в двобазовій радіометричній системі (РМС) визначається інтегралом:

$$Z_{12} = \int_0^{Ò_{itg}} \left[y_1(t) + y_2(t) \right]^2 dt = \int_0^{Ò_{itg}} y_1^2(t)\, dt + \int_0^{Ò_{itg}} y_2^2(t)\, dt + 2 \int_0^{Ò_{itg}} y_1(t) y_2(t)\, dt ,$$

де $ó_1(t)$, $ó_2(t)$ – вихідні сигнали першої та другої баз відповідно.

Для збереження енергії корисного сигналу необхідно прийняти коливання по першій та другій базі, звести їх до квадрату та провести інтегрування за часом $Ò_{itg}$. Третя складова виразу визначає напрямок РМ корисного сигналу, як взаємну кореляційну функцію (ВКФ) між коливаннями першої і другої баз багатоканального детектора. Одним з варіантів спрощеної структурної схеми для виявлення радіометричних (РМ) сигналів, при наявності частотних відмінностей (або просторових) між корисним сигналом і коливаннями завад, показана на рисунку 1. Вхідні коливання з пунктів прийому п1 (п3) проходять лінії затримки з кроком 0,5 ВКФ і надходять на кореляційні виявлювачі. Кількість відводів ліній затримки n визначаються дальністю дії системи і її смугою пропускання. На інший вхід виявлювача подаються коливання після поділу з пунктів п2 та п4. Вихід кожного кореляційного детектора другої бази ділиться на m. Результати розподілу подаються на перші входи міжбазових кореляторів.

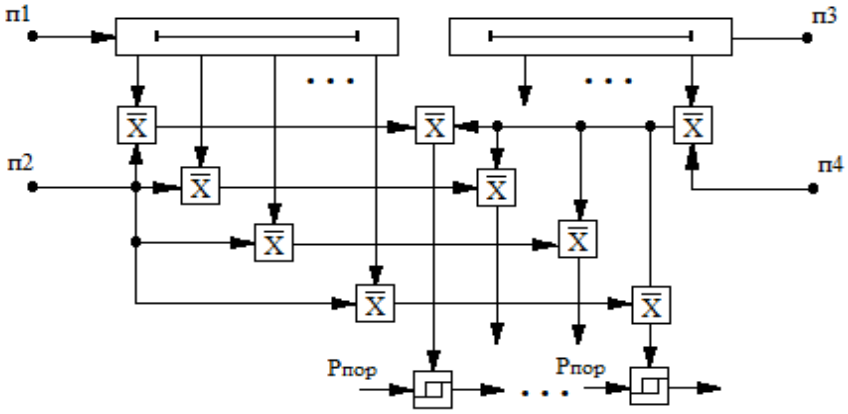


Рисунок 1 – Спрощена схема виявлення РМ сигналу при багатоканальному прийомі

Застосування схеми можливо не тільки в мм або (та) в інфрачервоному (ІЧ) діапазонах довжин хвиль. Використання ІЧ діапазону істотно збільшить роздільну здатність за різнецею ходу. Одночасне впровадження режиму синтезованої апертури антен в мм (ІЧ) діапазоні дозволить якісно проводити картографування не тільки поверхні Землі але й космічних об'єктів з навколоземної орбіти.

Однією з основних технічних характеристик РМС є дальність дії. Знижує дальність

дії системи температура атмосферного випромінювання $T_{atm}(\phi)$ при зенітному куті ϕ. Використуємо модель плоскої поверхні картографування при однорідному шарі атмосфери. Для ясної погоди враховуємо поглинання киснем та парами води (7,5 гр/м^3). Коефіцієнт поглинання РМ сигналів при наявності в атмосфері кисню, водяної пари та пилу визначаємо при дощі середньої інтенсивності в 4 мм / год для 3 мм діапазону і 5 мм / год для 1 мм діапазону довжин хвиль. Отримуємо на центальній довжині хвилі λ_1 3,37 мм, за ясної погоди та дистанції в 5,5 км $T_{atm}(15) \approx 193{,}8\,K$, а при дощі – $T_{atm}(15) \approx 239{,}6\,K$. Для центральної довжини хвилі λ_2 1,34 мм та за тих же умов, $T_{atm}(15) \approx 210{,}6\,K$ та дощу – $T_{atm}(15) \approx 256{,}7\,K$.

На рис. 2 представлені результати розрахунку дальності дії рознесеної РМС $R_i(S,T)$ в залежності від площі об'єкта *S* та його радіояскравісної температури *T*.

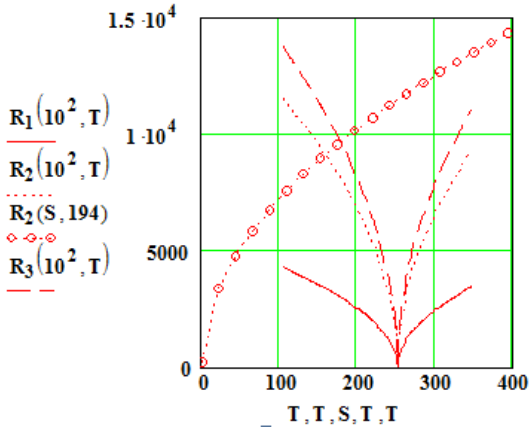


Рисунок 2 – Дальність дії рознесеної РМС

Перша крива $R_1(10^2,T)$ на рис. 2 (позначена безперервною лінією) показує значення дальності дії однобазової РМС при λ_1 та зміні *T* (105÷350 *K*) коли $S = 10^2\,\text{м}^2$. Отримали $R_1(10^2,194) \approx 2685$ м.

Друга крива $R_2(10^2,T)$ (крапки) розрахована при λ_2, причому $R_2(10^2,194) \approx 7240$ м. Така істотна зміна значень в 2,7 рази відносно $R_1(10^2,194)$ пояснюється збільшенням коефіцієнта стиснення та коефіцієнта підсилення антен системи. Дані результати розрахунків показують переваги роботи системи при переході з 3 мм діапазону до 1 мм діапазон довжин хвиль.

Список використаних джерел

1. Караваев В. В. Статистическая теория пассивных радиолокационных систем / В. В. Караваев, В. В. Сазонов. – Москва: Радио и связь, 1987. – 240с.

2. Кудряшов В. Є. Рознесена двохпозиційна радіометрична система картографування об’єктів / В. Є. Кудряшов, С. М. Тамаш, Д. С. Шмаков // Радіотехніка / Всеукраїнський міжвідомчій науково-технічний збірник. – Харків: ХНУРЕ, 2017. – Вип. 191. – С. 158-166.

УДК 358:007.35

Скопінцєв О. О.

ІНФОРМАЦІЙНА МОДЕЛЬ ОБ'ЄКТА УРАЖЕННЯ ПРИ ПЛАНУВАННІ УДАРІВ ПО ЗАХИЩЕНИМ ОБ'ЄКТАМ

Поява високоточної зброї дозволило говорити про виборчий спосіб ураження елементів об'єкта. Іншими словами – для досягнення мети операції цілком достатньо вражати не весь об'єкт як такий, а певні його елементи. Вводиться поняття «вражаємо комбінація», коли у складі групового об'єкта досить знищити одну або кілька елементарних цілей, втрата яких призводить до втрати боєздатності об'єкта у цілому.

На даний час основним засобом ураження неброньованих (слабо броньованих) цілей є касетні бойові частини (КБЧ), що оснащені некерованими осколково-фугасними бо-

йовими елементами (НОФБЕ) [1, 2].

При вибуху осколкового боєприпасу утворюється осколкове поле – потік осколків, що характеризуються напрямом і швидкістю руху, а також щільністю, тобто кількістю осколків на одиницю площі, яку вони перетинають [3].

Осколки в осколковому боєприпасі (НОФБЕ) можуть формуватися наступним чином: природним дробленням; заданим дробленням; готовими елементами ураження.

Таким чином, до початкових даних для НОФБЕ можливо віднести: загальну кількість вражаючих елементів, довжину НОФБЕ, висоту підривання, кут розльоту осколків та початкову швидкість метання.

Як початкові дані, можливо задати координати КБЧ розкриття, кількість НОФБЕ та кут їх розльоту. При цьому, конкретні значення координат розкриття КБЧ випадкові, розподілені за нормальним законом.

Попередньо розглянемо процес ураження одиночного малорозмірного захищеного об'єкта однієї фугасною бойовою частиною (ФБЧ).

З достатньою точністю для проведення оцінки застосування ФБЧ по малорозмірним об'єктам у цьому процесі будемо розглядати тільки сам об'єкт і ФБЧ, абстрагуючись від ряду факторів, наприклад, таких як погодні умови (стан атмосфери, швидкість вітру тощо).

Модель об'єкта ураження повинна відображати його міцність і геометричні розміри. Характеристики міцності об'єкта визначаються матеріалами його конструкції. Так при прямому влученні ФБЧ в об'єкт збиток оцінюється залежно від характеристик захисної споруди. Пропонується розглядати такі ступені руйнування:

1) сильне – настає при наскрізь пробитті захисної споруди;

2) середнє – настає при пробитті не менше 0,5 товщини захисної споруди;

3) слабке – настає при пробитті не більше 0,5 товщини захисної споруди.

Матеріал бокових стінок споруди опосередковано характеризується надлишковим тиском, що призводить до сильного, середнього та слабкого руйнування об'єкта. Крім того, утворюється надлишковий тиск при промаху ФБЧ по захисному спорудження.

При проведенні оцінки результатів застосування ФБЧ на перше місце виходить її бойова сила. Бойова сила насамперед залежить від ваги бойової частини і точності самого удару. Вага бойової частини виражається через вагу в тротиловому еквіваленті.

На точність удару впливають дві групи помилок: однакові для всіх пострілів (пусків) помилки цілевказівки і помилки індивідуального розсіювання.

Групові помилки підкоряються нормальному закону та характеризуються ймовірними відхиленнями (при нульових математичних очікуваннях).

Індивідуальні помилки також підкоряються нормальному закону та мають ймовірні відхилення від точки прицілювання.

Процес отримання об'єктом певної міри руйнування за своєю суттю є випадковим, так як в його основі лежить вибух ФБЧ, координати якого, виходячи зі сказаного вище, випадкові.

Таким чином, події отримання об'єктом сильної, середньої, слабкої ступеня руйнування випадкові та характеризуються відповідними можливостями їх настання. Дані ймовірності можуть служити оцінкою ефективності застосування ФБЧ при ураженні малорозмірних захищених об'єктів.

Отримання аналітичних залежностей ймовірностей отримання об'єктом відповідних ступенів руйнування при впливі ФБЧ важко через впливу багатьох важко прогнозованих факторів.

Імітаційний підхід дає можливість з достатньою достовірністю оцінити ці ймовірності. Для цього вводиться у розгляд три лічильника підрахунку отримання об'єктом ураження в кожній реалізації імітаційної моделі відповідного ступеня руйнування.

Таким чином, проведено аналіз зовнішніх чинників (засобів ураження, а також засобів розвідки), які впливають на процес ураження.

Запропонована імітаційна модель, що дає можливість отримати кількісну оцінку рішень, які спрямовані на підвищення живучості об’єкта ураження в умовах ведення бо-

йових дій (операцій) противника. В процесі роботи імітаційної моделі формується статистичний матеріал, який дозволяє вичислити оцінки ймовірності отримання кожного об'єкта ураження сильної, середньої та слабкої ступені ушкодження, знайти середнє число таких об'єктів ураження, що отримали вказані ступені ушкодження.

За умови зміни вказаних параметрів, з'являється можливість виробити найбільш раціональні рішення, що спрямовані на підвищення живучості об'єкта ураження в конкретних умовах ведення бойових дій (операцій) противника.

Напрямками подальших досліджень є: підготовка та формування імітаційної моделі оцінювання живучості об'єкта ураження для системи підтримки ухвалення рішень командиром різних (відповідних) рівнів.

Список використаних джерел

1. Забезпеченя оборони та безпеки України: проблеми і шляхи їх вивчення. Аналіз війн сучасної епохи [Електронний ресурс] / В. Горбулін. – Режим доступу: http://argumentua.com/stati/volodimir-gorbul-n-zabezpechenya-oboroni-ta-bezpeki-ukra-ni-problemi-shlyakhi-kh-vivchennya.

2. Світ після 2 серпня. Крах ракетної угоди: до чого варто готуватися Києву? [Електронний ресурс]. – Режим доступу: https://glavcom.ua/publications/svit-pislya-2-serpnya-krah-raketnoji-ugodi-do-chogo-varto-gotuvatisya-kijevu-615096.html.

3. Перепелиця Г. М. Конфлікти в посткомуністичній Європі : монографія / Г. М. Перепелиця ; Нац. ін-т стратег. дослідж. – К. : Фоліант, 2003. – 430 с.

УДК 519.873: 621.389(045)

Трофименко А. О.

ОБГРУНТУВАННЯ ПОКАЗНИКА ЕФЕКТИВНОСТІ СИНТЕЗУ ІНФОРМАЦІЙНО-ДІАГНОСТИЧНОЇ АПАРАТУРИ КОНТРОЛЮ ТЕХНІЧНИХ КОМПЛЕКСІВ

Ефективність використання за призначенням технічних комплексів залежить від їх поточного стану, для перевірки якого використовують різноманітні засоби контролю [1, 2]. На сьогодні найбільш перспективними засобами контролю поточного стану технічних комплексів є інформаційно-діагностична апаратура (ІДА) [2]. Складність ІДА обумовлює численність показників, що відображають різні їх властивості. Серед характеристик ІДА необхідно виділити наступні: ефективність, достовірність, точність, продуктивність контролю та діагностування, ресурс (загальний час роботи, наробіток на відмову тощо), вартість і обсяг можливих операцій з контролю та діагностування, кількість і характер тестових і вимірювальних сигналів, зміст і форма представлення результатів контролю та діагностування, режим роботи апаратури, можливість автоматичного регулювання параметрів контролю та діагностування, джерела живлення, маса та габарити, транспортабельність, кількість і кваліфікація обслуговуючого персоналу [3].

Серед зазначених характеристик до основних характеристик, які впливають на синтез структури ІДА, пропонується віднести: ефективність, достовірність, точність, продуктивність, ресурс, вартість та обсяг контролю та діагностування. До додаткових, але теж необхідних для врахування при синтезі структурної схеми ІДА, віднесемо кількість і кваліфікація обслуговуючого персоналу.

Ефективність контролю є мірою доцільності застосування контролю, тобто мірою цінності інформації, що добувається при контролі. Ефективність залежить від продуктивності, ресурсу ІДА, а також від вартості витрат на розробку та виготовлення ІДА і проведення контролю та діагностування поточного стану технічних комплексів.

Достовірність контролю є ступінь довіри до результатів контролю. Як показник достовірності контролю використовується ймовірність прийняття вірного рішення за результатами контролю. Будь-яка система контролю та діагностування працює з помилками, крім того, контролю та діагностуванню піддається тільки частина параметрів технічних комплексів [3]. Інформація, що отримана у результаті контролю параметрів, містить невизначеність. Достовірність контролю залежить від точності вимірювання та обсягу контролю параметрів технічних комплексів.

Точність контролю є характеристикою роботи вимірювальних трактів апаратури контролю. Зазвичай точність характеризується середньоквадратичною похибкою вимірювання.

Продуктивність контролю визначається часом, що витрачається на перевірку одного виробу. У цей час входить час підготовки апаратури контролю до роботи, час підготовки об'єкта контролю і, нарешті, час проведення контролю.

Вартість контролю містить дві складові: одна визначає вартість виробництва ІДА, а друга – вартість всіх витрат на проведення контролю та діагностування технічних комплексів протягом всього часу роботи ІДА.

Обсяг контролю є дуже важливою технічною характеристикою ІДА, що визначає основні параметри при контролі та діагностуванні. Обсяг контролю – це кількість і перелік параметрів, що підлягають контролю [3]. При визначенні обсягу слід виходити з умови отримання необхідної достовірності контролю та певної глибини діагностування технічного комплексу. Кількість і характер тестових і вимірювальних сигналів ІДА визначається обсягом параметрів контролю та діагностування та конструкцією технічного комплексу.

Результати контролю повинні містити рішення про придатність або непридатність технічного комплексу виконувати свої функції, числові значення показників якості та параметрів контролю та діагностування. Режим роботи ІДА може бути ручним, напівавтоматичним і автоматичним. У програмі контролю можуть бути передбачені повторне вимірювання ряду параметрів, самоконтроль і інші режими.

Основними технічними характеристиками ІДА, які суттєво впливають на синтез структури, є: кількість і вид контрольованих характеристик; точність; спосіб оцінки проміжних результатів контролю та діагностування, швидкодія.

Такі технічні характеристики ІДА, як маса, об'єм, габарити, ступінь автоматизації, простота відшукання та усунення несправностей, ступінь уніфікації, пристосованість до освоєння обслуговуючим персоналом, кількість, кваліфікація та умови роботи обслуговуючого персоналу, транспортабельність і маневреність, витрата ресурсу технічних комплексів, з точки зору контролю є додатковими.

Побудова ІДА може проводитися трьома методами: побудовою ІДА для існуючих технічних комплексів; побудовою ІДА для технічних комплексів на етапі структурної розробки; побудовою ІДА за заданими технічними характеристиками перспективних технічних комплексів.

При цьому пропонується використовувати к*омплексний показник ефективності синтезу ІДА для контролю технічних комплексів. Комплексність показника ефективності буде залежати від методу побудови ІДА.* Найвигіднішим буде компромісне рішення (комплексний показник ефективності), що дозволяє синтезувати потрібні тактико-технічні вимоги до ІДА забезпеченні заданого рівня достовірності контролю та діагностування технічних комплексів при низькій вартості та малому часу контролю та діагностування.

Список використаних джерел

1. Herasimov, S., Shapran, Yu. and Kirvas, V. (2017), Development and research of the method of calculating the reliability of the measurement control parameters of radio engineering systems of maritime transport, Systems of Arms and Military Equipment, № 4 (52), pp. 5-10.

2. Herasimov, S., Shapran, Yu. and Stakhova, M. (2018), Measures of efficiency of dimensional control under technical state designation of radio-technical facilities. Information processing systems, 2018, № 1 (152), pp. 148-154, doi: 10.30748/soi.2018.152.21.

3. Herasimov, S. and Gridina, V. Method justification nomenclature control parameters of radio systems and purpose of their permissible deviations. Information processing systems, 2018, № 2 (153), pp. 159-164, doi: 10.30748/soi.2018.153.20.

Protsiuk Yu., Chernych Yu., Maltseva I.

IDENTIFICATION OF POSSIBLE CHANNELS OF LEISURE OF INFORMATION AND ITS PROTECTION

The development of modern information technologies and data transmission systems requires constant monitoring of the security services market and timely application of up-to-date methods and means of identifying possible sources of information leakage. When building a reliable information security system, you need to apply a comprehensive approach, taking into account possible information leaks.

One of the threats of information leakage is the formation of probable leakage channels through the use of embedded devices.

In turn, the information intercepted by the mortgage devices can be recorded using portable means of audio and video, or transmitted via radio, optical channel, AC power lines, connecting lines of telecommunication systems, security and fire alarms, metal structures. buildings, pipes of heating and water supply systems, as well as specially laid cables (lines).

By the type of information intercepted it can be divided into: linguistic; species and information processed by technical means.

Among the most common methods of information leakage are acoustic control of the premises, listening to telephone lines, intercepting computer information, hidden photo and video shooting, receiving parasitic electromagnetic radiation, visual surveillance, bribery of employees, bribery of employees, etc. [1].

Acoustic control of the room is possible by: microphone, with cable output; voice recorder; stethoscope; radio microphone; telephone line; laser removal of information from window glass.

The telephone line is used not only for listening to telephone conversations, but also for listening to the office (the handset is not removed from the telephone). To do this, use the microphone effect, high frequency coil, TV monitor, telephone ear, and more. Some systems allow you to listen to any room through which a telephone cable runs, even from another country.

Removing information from your computer is possible by: "hacking" art; hidden camera; a special radio receiver that receives parasitic radiation from a computer (usually a monitor) with subsequent detection of useful information.

Any home appliance has side-by-side electromagnetic radiation that can be modulated by an acoustic signal (human voice).

The process of searching for mortgages involves a comprehensive special check for the availability of mortgages [2]:

1. Study of the operational situation near the object of inspection;
2. Analysis of the radio frequency situation outside the object of verification;
3. Analysis of the radio frequency situation at the object to be inspected;
4. Finding and detecting mortgages at the audited entity.

Protection of information from its leakage with the use of mortgage devices is ensured through technical and organizational measures. Technical measures are ensured by the installation of information security facilities (transformers, filters, external mechanical shutters, etc.) on the objects. Organizational measures are ensured by observing the requirements of the current legislation of Ukraine on technical protection of information. [3].

Thus, the protection of information from its leakage by the use of mortgaging devices should consist in the development of procedures for detecting leaks, detecting devices for silent removal of information and preventing unauthorized access to information.

УДК 004.056

Palamarchuk N., Palamarchuk S., Shemendiuk O., Ovsiannikov V.

DETERMINATION OF GENERAL ISSUES CONSTRUCTION OF SYSTEM CYBER SECURITY AND CYBER PROTECTION IN UKRAINE

The state of cyber defense of state bodies is possible due to the cumulative assessment of a number of factors and components, including: state of development of information infrastructure and protected electronic state services, security of special systems, implementation of complex systems of information protection, its cryptographic and technical protection, security of state information resources and information, requirement on the protection of which is established by law.

Formation and provision of cybersecurity and cybersecurity system for the Ukrainian information segment, passes the period of formation at the legislative, organizational and technical (technological) levels. At the legislative level:

1) adopted the Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine", which defines the legal and organizational bases for ensuring the protection of vital interests of the individual and the citizen, society and the state, national interests of Ukraine in cyberspace, the main goals, directions and principles of the state policy in the field of cybersecurity , the powers of public authorities, enterprises, institutions, organizations, individuals and citizens in this field, the basic principles of coordinating their activities for cybersecurity.

Coordination of cybersecurity activities as a component of Ukraine's national security is carried out by the President of Ukraine through the National Security and Defense Council headed by him. The National Cybersecurity Coordination Center, as a working body of the National Security and Defense Council of Ukraine, coordinates and controls the activities of the security and defense sector entities providing cybersecurity.

The State Service for Special Communications and Information Protection of Ukraine provides for the formation and implementation of the state cyberspace protection policy for state information resources and information, the requirement for protection of which is established by law, as well as the functioning of the State Cyber Security Center, the governmental computer emergency response team of Ukraine CERT-UA.

2) Decree No. 96/2016 of the President of Ukraine introduced the Decision of the National Security and Defense Council of Ukraine on January 27, 2016 "On the Cyber Security Strategy of Ukraine". The purpose of the Strategy is to create conditions for the safe functioning of cyberspace, its use for the benefit of the individual, society and the state. According to the Strategy, the establishment of a national cybersecurity system was initiated and the tasks of the entities forming it were identified (the main subjects are the State Special Communications and Information Protection Service of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces Forces of Ukraine, Intelligence Bodies, National Bank of Ukraine).

3) according to the Decree of the Cabinet of Ministers of Ukraine of August 23, 2016 No. 563 “On Approving the Procedure for Forming a List of Information and Telecommunication Systems of Critical Infrastructure Objects of the State” a mechanism for forming a list of critical infrastructure facilities of the state (information and telecommunication systems) has been defined are subject to protection.

4) according to the Resolution of the Cabinet of Ministers of Ukraine of June 19, 2019 No. 518 “On Approval of General Requirements for Cyber Security of Critical Infrastructure Objects” the organizational, methodological, technical and technological conditions of cyber

defense of critical infrastructure objects have been determined, which are mandatory for implementation by enterprises, institutions and organizations, which according to the legislation are assigned to the objects of critical infrastructure.

At the organizational level:

1) cyber security services and units are established at different levels of government (departments);

2) work is underway to establish a list of critical infrastructure facilities and to create (maintain) a state register of critical information infrastructure facilities of the state;

3) technological interaction of cybersecurity entities is organized and coordinated in order to determine the state-wide response to emergency response.

4) a scientific and educational institution shall be formed for the development, operation, improvement, and training of specialists in the field.

At the technical (technological) level:

1) a material and technical base (a set of technical, technological, information and psychological means) is formed to ensure the functioning of the cybersecurity system. The issue of securing the system is complicated by the use of a wide range of modern tools and technologies, on the basis of which information and telecommunications (telecommunication) systems are built, which are the basis of critical infrastructure.

Protection of information and telecommunication systems from the structure of critical infrastructure of the state against cyber attacks is provided by the owner (manager) of such systems in accordance with the legislation. Popular global solutions include the use of technologies such as Intrusion Detection System (IDS), Security Information Event Management (SIEM) systems and Data Leak Prevention (DLP).

Thus, at these levels the components of ensuring the cyber security system of Ukraine are identified. However, a wide range of components of network devices and applications for their analysis needs systematic and effective solutions for their use for the information and telecommunication systems (their components) of the Ukrainian information environment, with the obligatory harmonization of world standards and adaptation of related industries.

The importance of training cybersecurity professionals, including the practical component, should be mentioned. A good example would be large-scale NATO exercises.

References

1. The Law of Ukraine “On the Fundamental Principles of Cyber Security in Ukraine”

2. Decree of the President of Ukraine “On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016 №96 / 2016“ On the Cybersecurity Strategy of Ukraine”

3. Resolution of the Cabinet of Ministers of August 23, 2016 No. 563 “On Approving the Procedure for Forming a List of Information and Telecommunication Systems of Critical Infrastructure Objects of the State”.

4. Cybersecurity of Next Generation Networks: Educ. manual / O. O. Varaksin, E. V. Vasiliu, S. M. Gorokhov, V. Y. Kildishev, V. G. Kononovich; in a row. Corresponding Member MAZ V. G. Kononovich. – Odessa: ONAZ them. O. S. Popova, 2012. – 240 p.

5. Methods and tools used in SIEM systems for monitoring information security. Introduction. Part 1. [Electronic resource]. – Access mode: https://www.securitylab.ru/blog/company/gamma/344431.php.

6. Resolution of the Cabinet of Ministers No. 518 of June 19, 2019 “On Approving the Procedure for Forming a List of Information and Telecommunication Systems of Critical Infrastructure Objects of the State”.

Cherednychenko O., Martyniuk V., Karpenko A.

USE OF ARTIFICIAL NEURAL NETWORKS IN THE MILITARY SPHERE

To date, the existing automated troop management systems (ATMS) are using their marginal capabilities, which necessitates the search and use of unconventional approaches in the further development of ATMS. Given the thinking processes of the decision maker, the role of automation in decision-making will grow, necessitating the use of intelligent systems for planning and managing real-time, real-time combat and combat in a dynamic environment with the ability to transform unstructured data into knowledge, ready for immediate use.

A promising theoretical basis for the implementation of the ATMS system is artificial neural network (ANN), (Figure 1) technologies, which are convenient and productive when creating intelligent controllers for the control systems of complex technical devices, mobile robots, unmanned aerial vehicles.

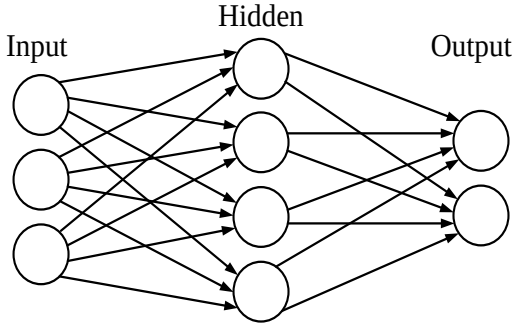


Figure 1 – Artificial neural network

Currently, a wide range of activities are being conducted in leading countries around the world to create intelligent systems of various types and purposes – to support decision – making, processing and recognition of ambiguous information, diagnosis and automatic control. The fundamental difference between such systems is the work with knowledge in a particular subject area.

The main architectural feature that distinguishes the intellectual system from the system built in the traditional scheme, is associated with the implementation of storage and processing of knowledge to realize the ability to perform its functions, in uncertain conditions and in the random nature of external influences. These may include unforeseen changes in purpose, performance of the system and control object, environmental parameters, etc. In addition, the composition of the system may, if necessary, be supplemented by self-study tools that provide a generalization of lessons learned and, on that basis, be supplemented by knowledge. Thus, the definition of the main directions of technology use with the use of ANN methods and technologies in the defense sphere is relevant.

The ANN will ensure in the near future an increase in the effectiveness of activities in such areas of military affairs as: modeling, combat operations and justification of the forces and means used; functioning of integrated intelligence and control systems, remote-controlled, reconnaissance and strike combat systems, robotic military systems, etc .; management of mobile distributed systems of military protection of the given borders and objects; the use of simulators, training systems.

It will be advisable to use ANN in new methods of improving the ATMS for both the medium and long term, since the automated system will constantly be self-learning and self-improvement, which will allow it to be used in the distant future.

Bondarenko O., Bondarenko T., Novak A., Poberezhets T.

PROTECTION METHODS OF SATELLITE COMMUNICATION SYSTEMS FROM THE INFLUENCE OF RADIOELECTRONIC INSULATION MEANS

An analysis of the military conflicts of recent years shows that successful military operations have been achieved, to a large extent, by a breach of the control of the enemy's troops by the electronic suppression of its communications systems. It is implemented, in particular, by the influ-

ence of deliberate interference on the reception devices of the satellite communication systems and / or the introduction of false information in them. Therefore, the task of protecting satellite communications systems (lines) from electronic jamming is important and relevant.

In peacetime, there may be limited use of electronic suppression devices for the short-term radio interference of a potential enemy satellite communication system, with a random character to these interferences. The purpose of this application is to evaluate early the level of noise immunity of the satellite communications systems, to identify the means of their protection and their algorithms, as well as the organizational measures for the protection of the satellite communications systems.

In this way, the enemy can detect all active satellites of the repeater in advance, even in peacetime, set the modes of their operation and frequency, analyze the signals used and determine the effective types and parameters of interference. That is why during wartime other (backup) frequencies and operating modes should be used in the system.

The most effective effect on satellites is the repeater, since it can damage all the satellite lines that operate through it. The impact of interference on territorially spaced earth stations is less effective, as they can be located in the folds of the terrain deep into their territory.

The protection of satellite lines from electronic suppression must be continuous and comprehensive. Continuity means the continuous prevention of satellite communications at the stages of development, upgrading, testing and their intended use. The comprehensive protection of satellite lines is achieved through a combination of technical and organizational measures to counteract intelligence and enhance the stability of satellite lines to the effects of electronic jamming. The effectiveness of the interference is determined by the ratio of the cost of the electronic suppression of the satellite lines to the cost of providing their interference.

Increasing the security of satellite lines is achieved by: operating transmitting devices with the minimum required radiation power; the use of narrow directional antennas; providing commercial satellite lines with military satellite systems; the use of redundant satellites repeaters involved in providing emergency information sharing (in the case of radio suppression of main relay satellites); using broadband (broadband) signals.

These methods make it difficult for the enemy to obtain intelligence. Increasing the stability of satellite communication lines when exposed to electronic suppression means (complexes) is achieved by: reducing the possibility of influence of electronic suppression means; improving the relationship between the temporal and energy characteristics of satellite lines and radio-electronic suppression complexes.

Reduction of the possibility of exposure to electronic suppression means achieved by: physical destruction of these means; the use of backup satellite lines; by simulating the operation of military satellite lines as lines of commercial systems.

Improving the correlation between the temporal characteristics of the satellite communication lines and the electronic suppression complexes is realized by increasing the response time of the electronic suppression complexes and reducing the response time of the satellite communication lines to the interference effects. These measures include: rapid transition to work through the unaffected relay satellite trunk and change in the polarization of radiation; use of complex signals, signal processing on satellites of repeaters, etc.

Improving the relationship between the energy performance of the satellite lines and the electronic suppression complexes, aimed at increasing the limited power plant interference required to suppress the satellite lines, is achieved by: enhancing the energy potential of the satellite lines; using broadband signals; the use of adaptive antenna systems and antennas with narrow beam patterns; using noise-coding; compensation and resection of interferences; using the protective (shielding) properties of the terrain and atmosphere.

To date, the most effective methods of protecting military satellite communications systems from electronic jamming are to broaden the signal spectrum, to use adaptive antenna systems and antennas with narrow beam patterns, and to use noise-immersive coding.

Let's take a look at the features of promising areas of satellite communications interference.

The system of spatial interference compensation, where the signal received by the compensation antenna of the system with the spatial compensation of the specified noise, is amplified and enters one of the inputs of the amplitude-phase controller, in which the amplitude and phase of the interference are altered in accordance with the process. The received “copy” of the interference through the amplitude-phase controller is fed to the compensation input of the common-mode power adder S. The other input S receives an additive mixture of useful signal and interference. From the output S, the signal through the power divider is transmitted to the protected station and through the adaptive processor to the second input of the amplitude-phase controller, where there is a further change in the amplitude and phase of the interference. As a result of iterative processes, an interference voltage S equal to the amplitude and phase opposite voltage to the main S input from the antenna of the protected station appears on the compensation input S. As a result, the output produces a useful signal and a minor signal of incompletely compensated interference. In this case, the effect of interference can be reduced by 20… 30 dB in the centimeter and decimeter wave bands, in the relative (up to 50%) frequency band.

The system of interference protection with the diversity of "receiving" and "transmitting" satellites-repeaters, contains earth stations ES1, ES2 ... ESn and two spatially spaced satellites-repeaters SS1 and SS2. The SS 1 satellite for receiving signals from all earth stations is receiving, and the SS2 is transmitting (it contains a simulator of noise interference efficiency). Signals received from all earth stations by the SS1 repeater satellite are transmitted to the SS2 by the Earth-to-Earth interconnect line. The SS2 satellite relays the received signal from the SS1 in the direction of the Earth already in the (lower) frequency band provided for the satellite communication systems. The security of such a satellite communication system is defined as follows. The interfering transmitter, receiving the emitted SS2 signals to the ES, emits interference in its direction of interference at the standard upward frequencies. The lack of a radio transceiver at these frequencies detracts from the interference of the interpreter. To disorient it on the SS2, a simulator of the impact of interference on satellite communication systems is installed.

Provided systematic materials on the subject, discussed some promising areas of satellite communications interference, namely:

- the use of spatial interference compensation, which reduces their effect by 20 to 30 dB in the centimeter and decimeter wavelengths, in the relative (up to 50%) frequency band;
- spacer satellite spacing, which allows you to hide the position of the receiving satellite of the repeater and to prevent it from intentional interference.

УДК 621.3

Ларін В. В., Лютий А. В., Ахмед Абдалла

ДОСЛІДЖЕННЯ МЕТОДІВ МАСКУВАННЯ ІНФОРМАЦІЙНОГО РЕСУРСУ В ЧАСТОТНІЙ ОБЛАСТІ

Найбільшого поширення серед всіх ортогональних перетворень в стеганографії отримали ДКП і вейвлет-перетворення, що пояснюється значним поширенням їх використання при компресії відеоінформаційного ресурсу. Крім того, для приховування даних доцільно застосовувати саме те перетворення зображення, якому останнє буде піддаватися згодом при можливій компресії. Наприклад, відомо, що комбінаторіка ДКП є базовим в стандарті JPEG, а вейвлет-перетворення – в стандарті JPEG 2000.

Ефективність застосування вейвлет-перетворення і ДКП для компресії відеозображень пов'язана з тим, що вони добре моделюють процес обробки елементів зображення, відокремлюючи істотні деталі від другорядних. Таким чином, дані перетворення більш доцільно використовувати в разі присутності реального порушника. Внесення змін до значущих коефіцієнтів може призвести до неприйнятного спотворення вихідного зображення.

Проведені результати експериментів, які дозволяють зробити рекомендації щодо вибору виду перетворення для стеганографії. Впорядкуємо ортогональні перетворення по досяжним виграшами від алгоритмів кодування.

Під виграшем від кодування мається на увазі ступінь перерозподілу дисперсій коефіцієнтів перетворення. Найбільший виграш дає перетворення Карунена-Лоєва, найменший – розбиття по основам одиничного імпульсу (тобто відсутність перетворення).

Перетворення, які характеризуються високими значеннями виграшу від кодування, такі як ДКП, вейвлет-перетворення, характеризуються різко нерівномірним розподілом дисперсій коефіцієнтів контурів відеозображень. Високочастотні контури не підходять для вбудовування через значний шум обробки, а низькочастотні – через високий шум зображення. Тому доводиться обмежуватися середньочастотними контурами, у яких шум зображення приблизно дорівнює шуму обробки.

УДК 656.7.08

Турінський О. В., Тимочко О. І., Осієвський С. В.

ОСНОВНІ ЕТАПИ ЖИТТЄВОГО ЦИКЛУ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ПІДРИМКИ ПРИЙНЯТТЯ РІШЕННЯ

Розробка інтелектуальних систем підтримки прийняття рішень (ІСППР) істотно відрізняється від розробки традиційного програмного забезпечення (ПЗ). Застосування методів, що є загальноприйнятими в класичному програмуванні занадто збільшує час розробки, або взагалі призводить до неможливості створення системи. Таким чином, неформалізованість завдань та необхідність участі людини-експерта на всіх етапах розробки призводять до необхідності зміни принципів і методів розробки інтелектуальних систем в процесі їх створення. Особливо гостро це питання постає в процесі нарощування знань розробників про предметні області.

Однак отримане в ході навчання представлення експертної інформації носить неявний характер, його інтерпретація і опис на природній мові нечіткі і представляють складність для подальшого аналізу. На сьогоднішній час прийнято “де факто” використовувати наступну послідовність етапів життєвого циклу нейромережевих ІСППР: ідентифікація – визначення вимог до системи, цілей і обмежень, що становлять специфікацію розробки нейромережі; формалізація – збір даних, які будуть використовуватися для навчання нейромережі, формування вихідного формату даних і складових документа з аналізу даних; навчання нейромережі як ітераційний процес, анотація навчання нейромережі; виконання, що передбачає розгортання і прийняття рішення нейромережею, розробка документів щодо інтеграції нейромережі; незалежне тестування і верифікація нейромережі, складання звіту по тестуванню.

Тобто, для експертних систем, що використовують для прийняття рішення механізм штучних нейронних мереж, невід'ємним етапом життєвого циклу є процес навчання, так як саме на цьому етапі відбувається вилучення неявних знань з навчальної множини. Очевидно, що в процесі навчання нейронних мереж неадекватність розв'язуваних завдань може призвести до появи на виході тільки шуму, а вагові коефіцієнти на даному етапі будуть проініціалізовані малими випадковими значеннями.

В наш час використовуються різні підходи до розуміння місця етапу навчання в життєвому циклі подібних систем. Пропонується виділяти етап навчання нейромережі в окремий етап життєвого циклу, проте логічніше вважати навчання нейромережевого механізму прийняття рішення частиною загального процесу відлагодження системи.

Для відлагодження системи пропонується використовувати дві основні групи методів: методи статичного аналізу, що здійснюють перевірку бази знань на рівні формаль-

ного контролю якості та не потребують запуску інтерпретатора системи; тестування, що полягає в прогоні ІСППР на заданій множині тестових даних і порівняння результатів виведення ІСППР з еталонними, що визначені експертами.

УДК 656.7.08

Захарченко І. В., Колесник А. В.

МОДЕЛЮВАННЯ ПОЗАШТАТНИХ ПОЛЬОТНИХ СИТУАЦІЙ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ ЙМОВІРНІСНОГО ПРОГРАМУВАННЯ

Одним із важливих елементів при дослідженні авіатранспортної системи є процеси моделювання розвитку можливих позаштатних польотних ситуацій. Для позаштатних польотних ситуацій, що потребують вимушеної посадки повітряного судна, актуальною є задача оцінки можливих варіантів завершення польоту. Це дозволяє авіаційному диспетчеру обрати одну з оптимальних стратегій з множини допустимих стратегій, які сформовані при виникненні певної позаштатної ситуації.

Слід зазначити, що задача вибору оптимального варіанту завершення польоту відноситься до класу задач, що характеризуються високим рівнем неповноти та невизначеності інформації. В області штучного інтелекту розроблено ряд методів, що дозволяють вирішувати проблему невизначеності знань при побудові експертних систем. Серед даних методів застосовуються: апарат нечіткої логіки, функції довіри, коефіцієнт впевненості, що відображає ступінь достовірності знань тощо. Останнім часом поширення набула теорія ймовірності, що має розвинутий та строго формалізований математичний апарат і яка надалі використовується в роботі.

Першим етапом в системі ймовірнісного міркування є створення моделі, що відображає всі наявні релевантні загальні знання щодо предметної області у вигляді ймовірностей. Створена модель застосовується для конкретної ситуації, для якої потрібно отримати заключення (відповідь). Для цього моделі необхідно надати конкретну інформацію про ситуацію, що склалася, тобто факти. Наступним етапом є запит, що представляється у такому вигляді, що допоможе в прийнятті різноманітних рішень. Процес, при якому отримується відповідь на запит з використанням створеної моделі та наявних фактів має назву ймовірнісний вивід.

Перевагою систем ймовірнісного виводу є можливість виконувати міркування трьох типів: передбачення майбутніх подій (найбільш ймовірний розвиток ситуації); вивід ймовірних причини подій, які вже мали місце; навчання на подіях, що вже відбулися (для покращення якості передбачення подій у майбутньому). Отримані від моделі заключення (відповідь на запит) мають вигляд ймовірностей і допомагають приймати рішення. Відносини між моделлю, фактами та відповіддю на запит математично строго визначаються законами теорії ймовірностей.

В роботі пропонується ймовірнісна модель прийняття рішення авіаційним диспетчером при виникненні особливого випадку в польоті – відмові двигуна повітряного судна в польоті, побудована на основі байєсівської мережі. Для представлення ймовірнісної моделі прийняття рішення пропонується застосування платформи FIGARO, що має розвинену структуру даних, легко інтегрується з іншими застосунками, застосовує універсальні алгоритми логічного виводу для міркувань щодо ймовірнісних моделей.

Дана платформа дозволить будувати множину можливих ймовірнісних моделей позаштатних польотних ситуацій; надає розвинуті засоби задання фактів; дозволяє застосовувати елементи, що відповідають змінним моделі, які можуть бути різних типів: булеві, цілі, масиви, дерева, графи тощо; надає можливість додавати до моделі очевидні рішення і підтримує вивід оптимальних рішень.

УДК 656.7.08

Гаєвський С. В.

АНАЛІЗ МЕТОДИЧНОГО АПАРАТУ З ПРОДОВЖЕННЯ РЕСУРСУ РАДІОЕЛЕКТРОННОЇ СИСТЕМИ ЛІТАКА

В доповіді проведено аналіз робіт з продовження ресурсів радіоелектронної системи літака як об'єкта довготривалої інтенсивної експлуатації. Даний аналіз показав відсутність їх досконалого науково-методичного забезпечення. В доповіді показано, що для ефективного в нових умовах вирішення завдань продовження ресурсів необхідна розробка методичного апарату:

- з розрахунку показників залишкового ресурсу на момент вироблення призначеного ресурсу;
- по розробці програм випробувань, обгрунтуванню планів випробувань та оцінки показників залишкового ресурсу радіоелектронної системи літака за результатами випробувань;
- по розробці заходів для підтримки працездатності і надійності літака на подовжений період експлуатації та по оцінці їх техніко-економічної ефективності.

Аналіз методик і методів розрахунку показників довговічності радіоелектронної системи літака вказує на наступні недоліки:

- розрахунок параметра потоку відмов РЕС літака передбачає необмежене число повних відновлень схемних позицій за призначений ресурс або термін служби, послідовну структурну схему надійності, спрощено враховує багаторівневу структуру радіоелектронної системи літака, режими функціонування його функціональних схем та функціональних вузлів при відновленні працездатності, тренуваннях та інших роботах;
- при розрахунках показників довговічності параметрична надійність радіоелектронної системи літака або не враховується, або її вплив враховується грубо, з великими похибками на рівні комплектуючих елементів;
- методики розрахунку показників довговічності не дозволяють коректно проводити розрахунки показників залишкового ресурсу радіоелектронної системи літака, що виробили призначений термін служби, з урахуванням їх фактичного стану і рівня надійності.

УДК 656.7.08

Головняк Д. В., Худов Г. В., Шило С. Г., Борозинець І. О., Ткачук С. С.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ УЗАГАЛЬНЕННЯ РАДІОЛОКАЦІЙНОЇ ІНФОРМАЦІЇ ВІД СУКУПНОСТІ РІЗНОТИПНИХ ДЖЕРЕЛ В КОМПЛЕКСАХ ЗАСОБІВ АВТОМАТИЗАЦІЇ КОМАНДНИХ ПУНКТІВ АВІАЦІЇ ТА ППО

Процес об'єднання інформації про повітряну обстановку від сукупності різнотипних джерел реалізується в комплексах засобів автоматизації командних пунктів (КЗА КП) авіації та ППО в складних умовах радіолокаційного спостереження. Це зумовлюється вогневим впливом авіаційної та наземної компонент супротивника, заходами щодо зменшення помітності, радіоелектронною протидією, маневруванням та постановкою активних та пасивних завад повітряними об'єктами (ПО). При цьому успіх операцій залежить від своєчасного виявлення ПО, встановлення їх державної належності, класифікації, розпізнавання їх ролі та цільового призначення. Сучасні умови ведення бойових дій характеризуються

суттєвою просторовою щільністю дії різнотипних ПО в обмеженій просторово-часовій площині. Процес радіолокаційного спостереження характеризується випадковим характером, епізодичністю та переривчастістю, крім того спостерігається вплив природного шумового фону та інших чинників, які впливають на якість отриманих оцінок для підготовки прийняття рішень по протидії повітряній агресії.

З логіко-математичної точки зору процес спостережності ПО різнотипними радіолокаційними джерелами (РРД) носить випадковий характер, координатні параметри та ознаки, які оцінені на джерелах та надходять на вхід обчислювальних комплексів КЗА КП авіації та ППО мають суттєві розбіжності щодо їх змісту.

Крім того, інформація надходить від джерел в різні моменти часу і розрахунки, що пов'язані з приведенням оцінок до єдиного моменту часу для ототожнення, призводять до зростання помилок, в основному, за рахунок похибок екстраполяції.

Існуючі методи об'єднання інформації про повітряну обстановку не враховують розбіжностей щодо складу інформації від джерел, що не дозволяє КЗА КП авіації та ППО у вказаних умовах забезпечити потрібні для споживачів значення показників якості інформації про повітряну обстановку.

Оскільки досягнення нормативних вимог щодо оперативності та якості РЛІ забезпечує отримання цілевказівок активними вогневими засобами без необхідності подальшого пошуку повітряних цілей, то відповідно і розробка методу об'єднання інформації про координатні параметри та різнорідні ознаки повітряних об'єктів, який би дозволив врахувати особливості функціонування різнотипних джерел, а також розбіжності в часі надходження даних від РРД, що в підсумку призводить до зменшення часу обробки РЛІ та до зменшення величини похибок оцінювання є нагальним науковим завданням, що потребує свого вирішення.

Наведена технологія сумісного об'єднання координатної та ознакової інформації в КЗА КП авіацією та ППО Повітряних Сил дозволяє о враховувати час надходження даних від джерел, та відрізняється від відомих вперше запропонованим способом приведення параметрів часткових траєкторій до моменту останньої за часом оцінки ЧТ та удосконаленими вирішальними правилами ототожнення вимірів різнотипних джерел.

УДК 656.7.08

Самокіш А. В., Литвинчук Д. В, Данилов Ю. О., Дроб Є. М.

АВТОМАТИЗАЦІЯ ПРОЦЕСУ ПРИЙНЯТТЯ РІШЕННЯ ПРИ УПРАВЛІННІ ДІЯМИ АВІАЦІЇ НА ОСНОВНІ НЕЧІТКОЇ НЕЙРОННОЇ МЕРЕЖІ

Досвід збройних конфліктів показує, що управління підрозділами армійської авіації при виконанні атак наземних цілей – це складна і досить відповідальна процедура. Вона вимагає ретельної підготовки та високого рівня професійних навичок особи, яка здійснює безпосереднє управління. Тому існує велика необхідність у підготовці висококваліфікованих фахівців, які будуть в змозі виконувати поставлені завдання. Тому для сучасних умов ведення бойових дій необхідно удосконалювати процес підготовки авіанавідника. На теперішній час це можна зробити шляхом автоматизації процесу підготовки авіанавідника. Наведення штурмової авіації на наземні цілі - це складний, динамічний і нелінійний процес. Елементи предметної області складаються з безлічі наборів даних різних типів і мають значну кількість причинно-наслідкових зв'язків. По-перше, описуючи процес наведення штурмової авіації на наземні цілі, ми отримуємо систему великих розмірів, в якій велика кількість входів і виходів. З великою кількістю входів і виходів експерту важко описати причинно-наслідкові зв'язки з нечіткими правилами. По-друге, у цих системах можна отримати надлишкові набори нечітких пра-

вил, які ускладнюють послідовність нечіткого виходу, що, у свою чергу, впливає на точність результату. Для вирішення цих проблем пропонується використовувати нечіткі нейронні мережі. Нечіткі нейронні мережі об'єднують в собі переваги нейронних мереж і систем з нечіткої логіки. Нечіткі нейронні мережі мають структуру ідентичну багатошарової нейронної мережі, але приховані шари в ній відповідають етапам функціонування нечіткої системи. Нечітка нейронна мережа являє собою багатошарову нейронну мережу спеціальної структури без зворотних зв'язків, в якій використовуються звичайні (НЕ нечіткі) сигнали, ваги і функції активації, а виконання операції $s = \sum_{i=1}^{n} w_i x_i + b_i$ підсумовування засноване на використанні фіксованої Т-норми, Т- конорми або деякої іншої безперервної операції. При цьому значення входів, виходів і ваг гібридної нейронної мережі є речові числа з відрізка [0,1]. Основна ідея, покладена в основу моделі гібридних мереж, полягає в тому, щоб використовувати існуючу вибірку даних для визначення параметрів функцій приналежності, які найкраще відповідають деякій системі нечіткого виведення. При цьому для знаходження параметрів функцій приналежності використовуються відомі процедури навчання нейронних мереж. Пропонується підхід до розробки автоматизованого методу наведення штурмової авіації на наземні цілі із використанням нейро-нечіткої мережі. Основна проблема для застосування подібного підходу є синтез структури мережі відповідно до вимог. В даній доповіді пропонується спосіб формування нейро-нечіткої мережі на основі асоціативних правил. Розглядаються методи виробки асоціативних правил на основі нечітких когнітивних карт побудованих на алгоритмі роботи авіанавідника.

Реалізація запропонованого підходу дозволяє отримати ряд переваг під час синтезу нечіткої-нейронної мережі для побудови системи підтримки прийняття рішення в перспективних автоматизованих системах управління.

УДК 656.7.08

Дубовик Г. В., Кривоножко А. М., Тимочко О. І., Захарченко І. В., Хмелевський С. І.

РОЗРОБКА МОДЕЛІ ДАНИХ ДЛЯ ВИРІШЕННЯ ЗАДАЧІ РОЗПІЗНАВАННЯ ПОВІТРЯНИХ ОБ'ЄКТІВ

Перспективним напрямком підвищення ефективності автоматизованих систем управління (АСУ) ППО є впровадження принципів інтеграції різноманітних джерел інформації у інформаційні підсистеми АСУ. Однією з основних задач аналізу та узагальнення інформації від різних джерел інформації є задача розпізнавання повітряних об’єктів (ПО) за їх ознаками.

На даний час основне навантаження по вирішенню задачі розпізнавання ПО покладається на особовий склад бойових розрахунків командних пунктів, в той час як за допомогою засобів автоматизації вирішується лише обмежене коло задач забезпечення. Це обумовлено тим, що даний клас задач важко формалізувати і труднощами при розробці ефективного алгоритму їх виконання. За своїм змістом задача розпізнавання ПО відноситься до класу інтелектуальних задач. Її ефективне вирішення можливе за рахунок використання знань та експертних систем, що в існуючих комплексах засобів автоматизації не реалізовано.

Проблеми побудови систем розпізнавання повітряних об’єктів розглядались в роботах. Недостатньо розглянутими є питання, присвячені врахуванню характеристик достовірності джерел інформації при формалізації структур даних про ознаки ПО та узагальнення результатів спостереження, а також формалізації знань, що використовуються при розпізнаванні ПО.

Основою розробленої методики розв'язання задачі розпізнавання ПО є методи формалізації процесу розпізнавання, оцінки ступеня істинності різнорідних ознак, об'єднання незалежних результатів розпізнавання, пошук рішень про класи розпізнаваних об'єктів з урахуванням неповноти і надмірності даних про ознаки.

Дана методика враховує характеристики точності і достовірності джерел інформації з нестохастичною невизначеністю і рекурентними правилами узагальнення оцінок значень ознак при багаторазовому спостереженні ВО. Це дозволяє врахувати вплив характеристик джерел інформації на результати розпізнавання і здійснювати розпізнавання не за окремими фрагментами прояви об'єктами ознак, а по їх узагальненій сукупності, що підвищує достовірність прийнятих рішень.

Особливістю розробленого методу формалізація процесу розпізнавання ВО на основі описів класів різнорідними ознаками, є використання ієрархічної функціональної мережі. Показано, що функціональна мережа процесу розпізнавання є однорідною в сенсі однорідності відносин між вершинами.

УДК 656.7.08

Павленко М. А., Павленко В. М., Берднік П. Г., Руденко В. М.

ВИРІШЕННЯ ЗАДАЧІ ВИЯВЛЕННЯ НАДМІРНОСТІ ОПИСУ КЛАСІВ АЛФАВІТУ ПРИ ВИРІШЕННІ ЗАДАЧІ РОЗПІЗНАВАННЯ

Надмірність класів алфавіту виникає внаслідок необхідності більш точного опису відмінностей в характері прояву окремих ознак об'єктами одного класу. Наприклад, для опису класу "Стратегічний розвідник" ознакою "швидкість", необхідно врахувати, що в цей клас входять швидкісні літаки типу SR-71A з максимальною швидкістю польоту, рівною 3300 км/год і нешвидкісні літальні апарати типу TR-1A з максимальною швидкістю, рівною 740 км/год. Для цього в опис класу вводяться кілька $\wedge$-наборів ознак з різними розподілами значень ознаки "швидкість". Природно, внаслідок помилок експерта неможливо повністю виключити випадки введення ідентичних розподілів значень однойменних ознак у різних $\wedge$-наборах опису класу. З синтаксичної точки зору подібний опис буде коректним. З точки зору семантичної коректності подібний випадок повинен бути віднесений до помилок.

Користуючись підходами, висновок про структурну надмірність опису аналізованого класу може бути отримано шляхом попарного аналізу середнього ризику при його розпізнаванні з використанням різних $\wedge$-наборів.

Як обмеження структурної коректності опису т-го класу ознаками приймемо істинність виразу:

$$\forall i \forall j (i \neq j) \wedge \left(\left[\sum_{\forall p \in P_{m_i m_j}} \overline{R}^{X_p}_{m_i m_j} \right] / P < 1 \right) \cdot$$

Рішення про необхідність усунення структурної надмірності опису класу має бути безумовно прийнято при наявності хоча б двох окремих $\wedge$-наборів. Зміна надлишкових знань повинно проводитися за участю експертів [1].

Сутність досліджуваного методу перевірки розрізнення описів класів алфавіту полягає в розрахунку значень середнього ризику при розпізнаванні кожної пари класів алфавіту і перевірки виконання введеного обмеження.

Метод відрізняється від відомих розробленими способами оцінки значення середнього ризику при розпізнаванні за кількісними, якісними ознаками і за сукупністю різнорідних ознак.

Використання методу дозволяє на етапі налагодження формалізованих знань виявляти некоректність, пов'язану з нерозрізненістю класів алфавіту і використовувати чисельне значення середнього ризику для виявлення інших видів семантичних некорректностей.

Рудковський О. М.

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ НАВЧАННЯ

Інформатизація є одним із пріоритетних напрямів реформування освіти в Україні. Це цілий комплекс соціально-педагогічних перетворень, пов’язаних з насиченням освітніх систем інформаційною продукцією, засобами й технологією, тобто впровадження в заклади системи освіти інформаційних засобів, що ґрунтуються на мікропроцесорній техніці, а також інформаційної продукції і педагогічних технологій, які базуються на цих засобах.

Однією із найістотніших складових інформатизації вищих навчальних закладів є інформатизація навчального процесу, а саме: створення, впровадження та розвиток комп’ютерне орієнтованого освітнього середовища на основі інформаційних систем, мереж, ресурсів і технологій. Головною її метою є підготовка фахівця до повноцінного життя і діяльності в умовах інформаційного суспільства, комплексна перебудова педагогічного процесу, підвищення його якості та ефективності.

Інформатизація вищого навчального закладу передбачає:

- оперативне оновлення навчальної інформації у зв’язку з розвитком науки, техніки, культури;
- отримання оперативної інформації про індивідуальні особливості тих, хто навчається, що забезпечить диференційований підхід до організації їх навчання і виховання;
- освоєння адекватних науковому змісту навчання й індивідуальних особливостей кожного курсанта, способів донесення потрібної навчальної інформації;
- отримання інформації про результативність педагогічного процесу, що дасть змогу оперативно вносити в нього необхідні корективи.

На сучасному етапі соціальних і технологічних перетворень однією з вимог до всіх учасників навчального процесу у вищих навчальних закладах є готовність майбутнього фахівця до практичного використання інформаційно-комунікаційних технологій, комп’ютеризованих систем загалом у навчанні та професійній діяльності.

Важливим елементом цієї готовності є не лише теоретична підготовка з певної галузі знань, а також і практичні уміння викладача організувати і провести навчальне заняття за допомогою комп’ютерних засобів і технологій; підготувати навчальне заняття за дистанційною формою навчання; застосувати фірмові розробки електронних навчальних посібників; створити власний електронний навчальний посібник з конкретної дисципліни; запровадити освітній Web-сайт з метою поглиблення власної наукової і викладацької компетентності.

Ефективність використання засобів інформаційних технологій у навчальному процесі залежить від успішності розв’язання завдань методичного характеру, пов’язаних з інформаційним змістом і способом використання автоматизованих систем навчання. Тому автоматизовані системи навчання доцільно розглядати як програмно-методичні комплекси (сукупність програмно-технічних засобів і реалізованих з їхнім використанням методів (методик) навчання, призначених для розв'язання конкретних завдань навчального процесу).

Навчання у вищому навчальному закладі за допомогою інформаційних технологій має низку суттєвих переваг, а саме:

- забезпечує оптимальну для кожного конкретного курсанта послідовність, швидкість сприйняття матеріалу, можливість самостійної організації чергування вивчення теорії, розбору прикладів, методів розв’язання типових задач тощо;

- формує навички аналітичної і дослідницької діяльності;
- забезпечує можливість самоконтролю якості здобутих знань і навичок;
- заощаджує час курсантів, необхідний для вивчення навчального матеріалу.

Крім того, за допомогою електронних видань, на основі спеціально розроблених комп'ютерних програм можуть бути реалізовані всі види контролю. Це знімає частину навантаження з викладача і підсилює ефективність і своєчасність контролю.

Використання інформаційних технологій у навчальному процесі впливає на характер навчально-пізнавальної діяльності тих, хто навчається, активізує самостійну роботу з різними електронними засобами навчального призначення. Найефективнішим є застосування інформаційних технологій для відпрацьовування навичок і умінь, необхідних для професійної підготовки. Воно також зумовлює скорочення обсягів і одночасне ускладнення діяльності викладача.

Так, наприклад, для засвоєння теоретичного лекційного матеріалу використовуються не тільки аудиторні заняття, а й створена система педагогічної підтримки (консультування, здійснення поточного контролю, проведення комп'ютерного тестування, робота з навчально-методичними матеріалами). Ускладнюється структура і такі форми навчальної діяльності, як контроль, консультації і самостійна робота курсантів.

Використання новітніх інформаційних технологій дає змогу значно підвищити ефективність інформації за рахунок її своєчасності, корисності, доцільного дозування, доступності та зрозумілості, мінімізації шуму, оперативного взаємозв'язку джерела навчальної інформації та курсанта, адаптації темпу подання навчальної інформації до швидкості її засвоєння, врахування індивідуальних особливостей тих, хто навчається, ефективного поєднання індивідуальної та колективної діяльності, методів і засобів навчання, організаційних форм навчального процесу.

Для ефективного використання в навчальному процесі сучасних інформаційно-комунікаційних технологій викладач повинен володіти певними специфічними вміннями:

- застосовувати сучасні інформаційно-комунікаційні технології в підготовці, аналізі, коригуванні навчального процесу, управлінні навчальним процесом і навчально-пізнавальною діяльністю курсантів;
- добирати найраціональніші методи і засоби навчання, враховувати індивідуальні особливості курсантів, їх нахили і здібності;
- ефективно поєднувати традиційні методичні системи навчання із новими інформаційно-комунікаційними технологіями.

Впровадження в навчальний процес у вищих навчальних закладах нових інформаційних технологій є об'єктивним процесом розвитку освіти. Але жодну з технологій не можна вважати універсальною: кожна з них в різних ситуаціях дає різні результати, і це необхідно враховувати при їх виборі.

Інтенсивне оновлення матеріально-технічної бази вищих навчальних закладів з урахуванням останніх досягнень науки і техніки дає змогу розвивати аудіовізуальну технологію навчання, яка передбачає використання різноманітних технічних засобів навчання, в тому числі комп'ютерних і електронних засобів. При цьому можливе використання різноманітних варіантів організації навчального процесу: від лінійного відео, за якого відбувається послідовний показ відео матеріалів із заданою швидкістю, до певною мірою діалогового, яке дає змогу здійснити зворотний зв'язок за правильними і неправильними відповідями, залежно від відповіді того, хто навчається.

Відкривається можливість широкого і різноманітного застосування в навчальній теле-, відеоапаратурі елементів автоматики, обчислювальної техніки, мікропроцесорних пристроїв, які приймають, записують і відтворюють навчальну аудіовізуальну інформацію, створення компакт-дискових систем, що значною мірою сприятиме досягненню вищого рівня освоєння навчального матеріалу тим, хто навчається.

Рудковський О. М.

РОЛЬ І МІСЦЕ КІБЕРБЕЗПЕКИ В ЄДИНІЙ СИСТЕМІ ЗАХИСТУ ДЕРЖАВИ

Епоха сьогодення – це епоха інформаційного суспільства, коли інформаційні технології та телекомунікації системи повністю охопили усі сфери життєдіяльності людини та у цілому держави.

Використання новітніх інформаційних технологій дає змогу значно підвищити ефективність інформації за рахунок її своєчасності, корисності, доцільного дозування, доступності та зрозумілості, мінімізації шуму, оперативного взаємозв'язку джерела навчальної інформації та людини, адаптації темпу подання навчальної інформації до швидкості її засвоєння.

Збройні сили та інші силові структури України не є у цьому винятком. На сьогодні сили охорони правопорядку повинні у будь-який момент, у будь-якому місці та у будь-якій обстановці швидко відреагувати на кризову ситуацію, бути готовими до рішучих дій з мінімальними втратами. Поряд з новими завданнями, що виникають внаслідок зміни форм і способів застосування сил охорони правопорядку, актуальним залишається питання управління силами та засобами для їх ефективного застосування.

Взявши на озброєння телекомунікації і глобальні комп'ютерні мережі задля підвищення мобільності і боєздатності, не слід забувати про можливі ризики, що створюють ці технології, особливо в умовах гібридної війни з боку РФ та потужних кібератак хакерів. Їх жертвами стають не тільки фізичні особи та окремі об'єкти інфраструктури, але й цілі галузі виробництва або держави.

За ефективністю та наслідками застосування кіберзброї, (такий термін все частіше використовують провідні вчені світу), її можна прирівняти до зброї масового ураження.

Тому кібербезпека стає основною проблемою сьогодення, яка викликає занепокоєння. Чим швидше йде розвиток інформаційних технологій, тим більшою є потреба в захисті інформаційно-телекомунікаційних систем. Оскільки критичні вразливості в програмному забезпеченні та автоматизованих системах викликають небезпідставні побоювання, уряди та суспільства в усьому світі шукають кращих, найбільш дієвих заходів і методів щодо захисту даних інтернет-ресурсів від кіберзагроз.

Під час проведення зустрічі на вищому рівні глав держав та голів урядів країн – членів Північноатлантичного альянсу було підписано договір між ЄС та НАТО про співпрацю у сфері безпеки, зокрема в питаннях гібридних війн та кібератак.

Кіберпростір, поряд із землею, повітрям, морем і космосом, було визнано новим оперативним простором, а кібероперації – невід'ємною частиною гібридної війни.

Найбільше уваги операціям у кіберпросторі приділяють провідні країни світу, а саме: США, Великобританія, Китай та ін. На розвиток кібернетичної складової вони закладають у бюджет не малі кошти, у життя втілюються програми щодо забезпечення національної безпеки та захисту об'єктів критичної інфраструктури від кібератак.

Ніхто не може з упевненістю стверджувати, що його мережі повністю захищені та можуть протистояти багатовекторним кібератакам. Кібернетична безпека стає пріоритетом розвитку сучасних армій та інших силових структур по всьому світу.

Основна з причин стрімкого розвитку підрозділів кібернетичної безпеки є гібридна війна, яку розв'язала і продовжує вести Росія проти України. Російська Федерація постійно збільшує кількість операцій по кібершпіонажу та намагається вплинути на громадську думку в багатьох країнах світу, не гребуючи використанням фейкових новин та відвертої пропаганди. Метою цих операцій є розхитування ситуацій всередині країни та створення хаосу та паніки, як підґрунтя для просування власних інтересів. Причому публічно країна-агресор залишається непричетною до такого конфлікту.

Рудковський О. М.

КІБЕРАТАКИ ЯК НЕВІД'ЄМНА ЧАСТИНА ГІБРИДНОЇ ВІЙНИ

Провідні експерти світу небезпідставно називають гібридну війну, яку розв'язала і продовжує вести проти України Російська Федерація, «війною нового покоління».

Гібридна війна являє собою як ведення бойових дій під прикриттям незаконних (неформальних) збройних формувань, так і одночасне використання широкого спектру політичних, економічних (енергетичних та торговельно-економічних), а також інформаційно-пропогандистських заходів, з яких як правило і починається ця гібридна війна та які її супроводжують упродовж усього періоду воєнних дій.

Російська стратегія перш за все спрямована проти слабких місць України. Постійно проводиться кібернетичні операції проти об'єктів критичної інфраструктури, приватного сектору, а також інформаційно-телекомунікаційних систем ЗС України.

Масштабні кібератаки організовані і проводяться не однією особою, а цілою групою хакерів за безпосередньою підтримкою впливових організацій, у тому числі силових структур.

З метою запобігання та вирішення цієї проблеми необхідно постійно проводити діагностування систем за допомогою певних тестів, з використанням спеціалізованого обладнання та із залученням кваліфікованих фахівців.

Вкрай важливим аспектом кібернетичної безпеки є проведення тренінгів з працівниками щодо запобігання та протидії кібератакам. Всі вони працюють у єдиному взаємопов'язаному мережевому просторі, тому зараження вірусом лише одного абонента може викликати ураження на всіх рівнях. При цьому слід враховувати те, що вірус може бути активований в будь-який час у будь-якій обстановці.

По наслідках проведення кібероперацій кібератаки поділяються на наступні:

- вандалізм – завдає репутаційних втрат державі як у світі, так і серед населення, викликає псування офіційних інтернет-сторінок або заміну змісту;
- пропаганда – розсилка спаму інформаційно-пропогандистського характеру, фейкові новини з метою дезорієнтації населення;
- збір інформації – злом серверів для збору цінної інформації або шпигунство, викрадення (заміна змісту) інформації;
- відмова сервісу – порушення функціонування сайтів або комп'ютерних систем, в наслідок атаки великої кількості комп'ютерів;
- втручання в роботу обладнання – відключення (виникнення помилок) системи з метою перешкоджання роботі комунікаційних цивільних або військових систем;
- атаки на об'єкти критичної інфраструктур – атаки на системи забезпечення життєдіяльності (водопостачання, електроенергетики, транспорту та ін.)

З метою мінімізації ризиків зусилля слід зосередити на наступних заходах щодо захисту інформації:

- *запобігання* – доступ до інформації та технології тільки для персоналу, який отримав допуск та має відповідні фахові навички;
- *виявлення* – забезпечення раннього виявлення злочинів та зловживань, навіть якщо механізми захисту були обійдені;
- *відновлення* – забезпечується ефективне відновлення інформації з наявності документованих і перевірених планів з відновлення.

На перший погляд може здатися, що кібератаки не можуть завдати великої шкоди та не забирають людських життів. Але це лише на перший погляд.

УДК 001:004:378

Метешкин К. А., Маслий Л. А.

МОДЕЛИРОВАНИЕ ЗНАНИЙ В КОНЦЕПЦИИ ЦИФРОВОГО ОБРАЗОВАНИЯ

В настоящее время еще не устоялось понятие «цифровое образование». Очевидно, данное понятие формируется в результате эволюционного развития, как средств цифровой электронной вычислительной техники, так и развития методологии образования и обучения от парадигмы традиционного образования к современной парадигме эдукологии. К сожалению, проект «Действие. Цифровое образование», который реализуется с 21 января 2020 года Кабинетом министров Украины сильно сужает рамки рассматриваемого понятия. Целью данного проекта является компьютерная грамотность 100% населения Украины, а целью образования, как это указано в Законе Украины об образовании, есть «всестороннее развитие человека как личности …» [1]. Учитывая эти противоречия воспользуемся определением, приведенным на сайте Белорусского государственного университета [2] – цифровое образование – это новая система образования, использующая средства ИКТ на основе совместного использования информации, открытых образовательных ресурсов, взаимодействия и сотрудничества для формирования и непрерывного развития компетенций и навыков обучаемого.

Опираясь на данное определение, можно утверждать, что реализовать в вузах цифровое образование можно на основе информатизации, интеллектуализации, а также систематизации основных видов обеспечения вузов используя при этом методы моделирования знаний.

В работах [3, 4] высказывается идея создания цифровых платформ моделей знаний, используемых при подготовке бакалавров по той, или иной специальности, а работа [5], в частности ее первый раздел, является описанием образовательной технологии «Систематизация».

Рисунок1 – Фрагмент цифровой платформы моделей профессиональных знаний

Фрагмент цифровой платформы моделей профессиональных знаний приведен на рисунке 1. Она имеет ряд особенностей. Во-первых, на ней размещаются модели учебных дис-

циплин одной конкретной специальности, и они имеют структуру, отражающую учебный план по блокам (гуманитарный, фундаментальный и профессиональный). Во-вторых, в ее основу положена модель, логически и семантически связанная со многими другими учебными моделями. В-третьих, данная модель представляет собой электронное интерактивное пособие, учебный материал которого сопровождается видео фильмами по тематике того или иного раздела пособия. В-четвертых, модели учебных дисциплин, разработанных преподавателями, предусматривают создание студентами собственных моделей учебных знаний. Моделирование собственных знаний студентов по той или иной дисциплине обеспечивает приобретение ими навыков обобщения учебной информации, а также абстрагирования от второстепенной информации.

Опыт создания моделей учебных дисциплин и использование их в учебном процессе, как одного из элементов цифровой платформы моделей знаний на кафедре показал, что организация учебного материала в виде моделей может быть альтернативой платформе обучения Moodle. Создание же студентами моделей своих знаний по конкретным дисциплинам, а затем объединение их в атлас профессиональных знаний уже показывает эффективность технологии «Систематизация», которая представлена в работе [5].

Список использованных источников

1. Закон України «Про освіту». [Електонний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/ laws/show/2145-19 (дата звернення 22.01.2020 р).

2. Институт бизнеса БГУ [Электронный ресурс] – Режим доступа : https://www.sbmt.bsu.by/confirmed/432 (дата обращения 17.01.2020 г).

3. Метешкин К. А. Моделирование как метод визуализации профессиональных знаний [Текст]: тезисы / К. А. Метешкин, Кухар М. А. / Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку / Збірник тез доповідей Міжнародної науково-практичної конференції, 14–15 березня 2019 р. // Національна академія Національної гвардії України, 2019. – С.3-5.

4. Метешкин К. А. Концепция создания и использования платформы цифровых знаний по специальности [Текст] / К. А. Метешкин, О. И. Морозова // Радиоэлектронные и компьютерные системы, 2019, №1(89). – С. 74-81.

5. Метешкин К. А. Параллели и меридианы геодезии и информатики или основы ноогеоматики [Текст] : учеб. пособие / К. А. Метешкин, А. Р. Левченко ; Харьков. нац. ун-т гор. хоз-ва им. А. Н. Бекетова. – Х. : ХНУГХ им. А. Н. Бекетова, 2019. – 203 с.

УДК 378.635.5

Романюк В. А., Стародубцев С. О.

УМОВИ ВДОСКОНАЛЕННЯ УПРАВЛІНСЬКИХ НАВИЧОК КУРСАНТІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Тенденції розвитку військово-професійної освіти визначають нові, досить високі орієнтири в підвищенні ефективності професійної діяльності випускників військових навчальних закладів. Потреба в здійсненні якісної підготовки у військовому навчальному закладі курсантів, що володіють знаннями, вміннями, необхідними особистісними якостями, визначають розробку системи формування управлінської компетенції курсантів, зумовлено соціальним замовленням, потребою військово-професійної освіти.

В сучасних умовах значно підвищується роль правильно і чітко організованого управління військами як основи підтримки їх постійної бойової готовності. Оскільки

відповідальність за ухвалення правильного і обґрунтованого рішення несе командир, безумовно, зростають вимоги до рівня його підготовки.

В той же час система військової освіти ще повільно адаптується до нинішніх вимог, програми підготовки у військових навчальних закладах не охоплюють усього комплексу питань, з якими доводиться стикатися командирові в повсякденній практиці. Не допустити зниження бойової готовності, допомогти керівникам з найбільшою ефективністю організувати свою роботу і роботу підпорядкованих підрозділів покликана добре відлагоджена система управління повсякденною діяльністю військ.

В умовах суттєвої модернізації озброєння і військової техніки, засобів збройної боротьби і специфіки бойового застосування частин і підрозділів, обумовлених темпами розвитку науково-технічного прогресу, процесами інформатизації суспільства, офіцер повинен мати високий рівень готовності до реалізації професійних функцій, вільно орієнтуючись у інформаційному просторі сучасного соціуму.

Тому особливості сучасних реалій в якості однієї з пріоритетних завдань, що стоять перед системою військової освіти визначають пошук шляхів і засобів вдосконалення професійної підготовки курсантів військових вузів НГУ в умовах масштабної інформатизації суспільства, НГУ, системи військової освіти.

Сьогодні вектор інформатизації військової освіти повинен бути спрямований на створення умов для підвищення якості освітнього процесу у військовому вузі за рахунок впровадження інноваційних методів і форм навчання, заснованих на сучасних інформаційних технологіях.

Успішність вирішення завдань, що стоять перед командирами частин і підрозділів, багато в чому залежить від кількісного обґрунтування різних варіантів рішень і вибору з них оптимального, в повній мірі відповідного реальній обстановці і яке враховує можливі наслідки.

Використання відповідних програмних засобів дозволяє в короткі терміни вирішувати завдання якісної тактичної підготовки і в цілому бойової підготовки, а також значно полегшити процес управління бойовою підготовкою частин і підрозділів.

Chernykh Yu., Chernykh O.

THE USE OF SIMULATION FOR TRAINING MILITARY SPECIALISTS

The use of analogy is a well-proven teaching method, through which an understanding of complicated situations can be achieved by relating them to simpler and more ordinary equipment arising from developments in computers technology. Within the armed forces, simulation had its early development in flying training but gradually spread to other areas, until now it has become a standard training technique in all forces where sophisticated and expensive weapons systems are being used.

The reasons explaining the increasing use of simulation techniques in training are numerous. First, the complexity of the weapons systems existing in the inventories of all armed forces requires more training than before to achieve and maintain a high level of combat readiness. It can be used to sustain skill levels when employment of the actual equipment is not practical for a host of reasons.

Also, from a learning standpoint, simulation allows realistic experimentation in a context sometimes difficult or impossible to replicate with the real equipment. A clear vision stands as an essential component of collective success. Leaders with an eye to the future must develop their vision with simulators based on a careful analysis of their experiences in sufficient detail to be of actual use in the future. The leader and his key colleagues must assemble a thorough set of milestones that assist the day - by - day work that actually creates the vision in the real world.

Finally, the leader has to commit time and energy to the hardest work of all - maintaining focus on achieving milestones and, eventually, the inspiring vision. Few items in your preparation for and execution of command will be as important or as rewarding.

Soldiers and their commanders with their staffs must be exposed to various battlefield conditions and environments in order to develop their skills and knowledge. Simulation will have a significant impact in the area of refresher training, skill maintenance, retaining combat proficiency, and the evaluation of units prior to live firing or operational deployment. Simulation includes the use of practice ammunition, sub-caliber devices, embedded training software in operational equipment, computer simulation of enemy activity, instrumented training ranges, etc.

The main objectives of war games are: to train military leaders to make decisions, to enable them to gain relevant experience, to provide them with the information required to perform their command activities under conditions that do not consume resources such as personnel and ammunition. In order to optimize the player's performance, it is usual to plan a game in such a way that the player fully attains some objectives, but only partially attains others. Games that predominantly give decision-making experiences are called instructional games and have as their main purpose the training of the players to make decisions based on the information provided in the course of the game. The impact of their decisions, together with details of the problems stemming from them in the course of the game is related to the players by the controller of the game or umpire. Frequently, only partial information is given so as to simulate for fog of war.

The other main type of war games are known as analytic games and are aimed at collecting information that may assist commanders in their decisions concerning the choice of plans, tactics, doctrines, etc. As an excellent and cheap instrument of analysis, simulation enable the effects of plans, tactics or doctrines to be tested in a variety of environments by repeating and replaying the scenario, thus, by different means, providing the opportunity to make objective choices based on the results obtained.

Черних Ю. О., Черних О. Б.

ОБҐРУНТУВАННЯ ВИБОРУ РАЦІОНАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ ДИСТАНЦІЙНИМ НАВЧАННЯМ ВІЙСЬКОВИХ ФАХІВЦІВ

Основними завданнями подальшого розвитку військової освіти є формування адекватної реформуванню Збройних Сил України системи підготовки офіцерських кадрів, виведення її на якісно новий рівень з урахуванням позитивних змін, що відбуваються у національній системі вищої освіти.

Однією із найістотніших складових системи забезпечення належної якості підготовки майбутніх офіцерів є інформатизація навчального процесу – створення, впровадження та розвиток комп'ютерно орієнтованого освітнього середовища на основі сучасних інформаційних систем, мереж, ресурсів і технологій. При цьому, головною метою системи забезпечення якості є підготовка військового фахівця до повноцінного життя і майбутньої службової діяльності в умовах інформаційного суспільства, комплексна перебудова педагогічного процесу, підвищення його ефективності.

На пошук оптимальних шляхів вирішення зазначених завдань була спрямована науково-дослідна робота «Теоретичні та технологічні засади дистанційного навчання у національній військовій освіті України» (шифр «Технологія-Д») [1], що виконана у Національному університеті оборони України імені Івана Черняховського (головний виконавець) та у низці вищих військових навчальних закладів (ВВНЗ), зокрема у Військовому інституті Київського національного університету імені Тараса Шевченка.

Актуальність дослідження проблеми розвитку дистанційної освіти в системі військової освіти зумовлена, на нашу думку, низкою суперечностей, які потребують свого

вирішення, а саме між швидким розвитком глобального інформаційного простору та нерозробленістю сучасних дистанційних технологій під час підготовки військових фахівців; необхідністю введення у навчально-виховний процес ВВНЗ новітніх інформаційних технологій та недостатністю науково-теоретичних та методичних розробок у цій галузі; потребами розвитку військової освіти в державі, у тому числі і шляхом запровадження дистанційних програм такого профілю, і недостатністю технологічного та організаційно-методичного забезпечення навчального процесу; потребою слухача (курсанта, студента) в отриманні комплексу освітніх послуг відповідно до індивідуальних потреб та низьким рівнем розвитку сегменту дистанційного навчання в системі військової освіти України.

Під час проведення наукових досліджень розроблено пропозиції щодо застосування технологій розробки та впровадження дистанційних навчальних курсів у навчальному процесі ВВНЗ. При цьому важливим кроком стало обґрунтування вибору раціональної системи управління дистанційним навчанням військових фахівців (платформи організації дистанційного навчання) – програмного забезпечення для його підтримки, метою якого є: створення та управління педагогічним змістом, організація індивідуалізованого навчання та телетьюторат. Воно включає засоби, необхідні для трьох основних користувачів: викладача, слухача (курсанта, студента) та адміністратора.

На сьогоднішній день у світі існує значне число e-learning платформ для організації електронного навчання, які поділяються на дві великі категорії: з закритим кодом (комерційні) та відкритим кодом (поширюються безкоштовно). Для дослідження були відібрані дев'ять найбільш популярних відкритих платформ і проведено зіставлення їх можливостей: Atutor, Dokeos, DotLRN, ILIAS, LON-CAPA, Moodle, OpenUSS, Sakai, Spaghetti Learning.

Зазначені платформи для організації електронного навчання порівнювалися за 34 параметрами, що були згруповані у 8 блоків: 1) інструменти управління навчальним курсом; 2) можливості адміністрування; 3) технічні аспекти; 4) можливості адаптації; 5) зручність використання платформи; 6) управління даними користувача; 7) об'єкти навчання; 8) кошти для спілкування. Слід зазначити, що останнім часом багато з перерахованих систем пройшли певні удосконалення. Тим не менш, з урахуванням безперервного вдосконалення система Moodle без сумнівів зберігає лідируюче положення.

Система Moodle є пакетом програмного забезпечення для створення курсів дистанційного навчання та веб-сайтів. До основних переваг системи відносяться [2]:

- спроектована з урахуванням досягнень сучасної педагогіки з акцентом на взаємодію між тими, хто навчається;
- може використовуватися як для дистанційного, так й для очного навчання;
- має простий та ефективний веб-інтерфейс;
- дизайн має модульну структуру і легко модифікується;
- підтримуються мовні пакети, що дозволяють добитися повної локалізації. На даний момент підтримуються 43 мови;
- користувачі можуть редагувати свої облікові записи, додавати фотографії і змінювати особисті дані та реквізити;
- кожен користувач може вказати свій локальний час, при цьому всі дати в системі будуть переведені для нього в місцевий час (час повідомлень у форумах, терміни виконання завдань тощо);
- підтримуються різні структури курсів: «календарний», «форум», «тематичний» тощо;
- кожен навчальний курс може бути додатково захищений за допомогою кодового слова;
- багатий набір модулів – складових для курсів – чат, опитування, форум, глосарій, робочий зошит, урок, тест, анкета, scorm , survey, wiki, семінар, ресурс (у вигляді текстової або веб-сторінки або у вигляді каталогу);
- зміни, що відбулися в курсі з часу останнього входу користувача в систему, можуть відображатися на першій сторінці курсу;

- майже всі тексти, що набираються (ресурси, повідомлення в форум, записи в зошиті тощо), можуть редагуватися вбудованим WYSIWYG RichText – редактором;
- всі оцінки (з форумів, робочих зошитів, тестів і завдань) можуть бути зібрані на одній сторінці (або у вигляді файлу);
- доступний повний звіт щодо входження користувача в систему і роботу, з графіками і деталями роботи над різними модулями (останній вхід, кількість прочитань, повідомлення, записи в зошитах);
- можливе налаштування E-mail – розсилка новин, форумів, оцінок і коментарів викладачів.

Список використаних джерел

1. Звіт про НДР «Теоретичні та технологічні засади дистанційного навчання у національній військовій освіті України» (шифр «Технологія-Д»), Київ, НУОУ, 2017, № держреєстрації 0117U002727, 267 с.
2. Платформа побудови сайтів дистанційного навчання Moodle - [Електронний ресурс]. – Режим доступу: http://moodle.org.

Соколіна О. В., Охрамович М. М.

ПЕРЕВАГИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ДИСТАНЦІЙНОГО НАВЧАННЯ В ОСВІТНЬОМУ ПРОЦЕСІ ВИЩИХ ВІЙСЬКОВИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

Завданням вищого військового навчального закладу сьогодні є підготовка висококваліфікованого, особистісно та професійно розвинутого військового фахівця здатного до саморозвитку та самовдосконалення. А це змушує шукати нові форми та технології навчання, що покликані на ефективну підготовку військових фахівців, а також їх адаптацію до міжнародних стандартів освіти. Технології дистанційного навчання забезпечують адаптацію процесу навчання до індивідуальних характеристик тих, хто навчається, звільняють викладачів від низки кропітких та часто повторюваних операцій за поданням навчальної інформації і контролю знань, сприяють розробці об'єктивних методів контролю знань і полегшують накопичення навчально-методичного досвіду.

Розрізняють кілька основних технологій дистанційного навчання:

Мережеві («хмарні») технології забезпечують збереження медіа-даних, перенесення ресурсів і даних на віддалені інтернет-сервери з можливістю отримання доступу до будь-якого пристрою у будь-якому місці. Перевагами «хмарних» технологій є наступні:

- безкоштовне використання;
- доступність з будь-якого місцезнаходження;
- відсутність необхідності придбання додаткового програмного та апаратного забезпечення;
- зрозумілий та доступний інтерфейс;
- економія дискового простору;
- можливість організації резервного збереження матеріалів;
- безпека та відкритість освітнього середовища для викладачів і курсантів (слухачів);
- безпосередня взаємодія: викладач → навчальна група, викладач → курсант, курсант → навчальна група, курсант → курсант;
- можливість застосування різноманітних видів навчальної роботи, on-line контролю й оцінювання рівня навчальних досягнень тощо.

Можна виокремити п’ять основних «хмарних» сервіси: iCloud, Google, Amazon CloudDrive, Windows Live, Dropbox.

Інтерактивні технології – це системний метод організації міжособистісної взаємодії всіх суб'єкті навчання, спрямований на відпрацювання вмінь комунікації, співпраці в групі (колективі), спільного вирішення проблем. Переваги інтерактивних технологій:

- розвиток критичного і креативного мислення курсантів;
- відпрацювання практичних умінь розв'язання різноманітних проблем;
- набуття досвіду міжособистісної взаємодії та комунікації;
- формування культури ділового спілкування.

Кейс-технології – це системний метод, що складається з різноманітних способів організації освітнього процесу (читання, аналіз, моделювання, ілюстрування тощо) і передбачає вивчення курсантами конкретних випадків (ситуацій, історій, тексти яких називаються «кейсами») з життя або професійної діяльності на основі спеціально оформленого пакету навчальних матеріалів – кейсу.Переваги кейс-технологій:

- розвиток умінь використовувати теоретичний матеріал для аналізу практичних проблем, оцінювати ситуації, знаходити й відбирати потрібну інформацію, формулювати питання, розробляти план дій та багатоваріантні підходи до його реалізації, самостійно ухвалювати рішення в умовах невизначеності;
- аналізувати ситуації, прогнозувати шляхи їх розвитку, набувати навичок конструктивної критики тощо;
- допускає варіативність навчання.

Використання технологій дистанційного навчання в освітньому процесі ВВНЗ вимагає змін у методиці викладання дисциплін. Викладач перестає бути для майбутніх військових фахівців єдиним джерелом отримання знань. Виникає необхідність зміни методики проведення аудиторних занять та удосконалення організації керованої самостійної роботи.

Застосування технологій дистанційного навчання в освітньому процесі вищих військових навчальних закладів дозволить курсантам стати активним суб'єктом освітнього процесу.

УДК 656.05.24

Подригало М. А., Тарасов Ю. В., Радченко І. О.

ПРОГНОЗУВАННЯ РІВНЯ ЕНЕРГО- І ТЕРМОНАВАНТАЖЕНІСТІ ГАЛЬМОВИХ МЕХАНІЗМІВ АВТОТРАНСПОРТНИХ ЗАСОБІВ

Збільшення максимальних конструктивних швидкостей руху автотранспортних засобів і вимог суспільства до ефективності їх гальмування тягне за собою підвищення енергонагруженності гальмівних механізмів. Останнє викликає підвищення робочих температур в контакті фрикційних поверхонь і може привести до порушення стійкості процесу гальмування. Цю обставину необхідно враховувати на етапі попереднього проектування автотранспортних засобів.

Максимальна кінетична енергія автомобіля, що розвивається при повної масі і максимальної конструктивної швидкості

$$E_{max} = \frac{m_П V_{a\,max}^2}{2} = \frac{N_{e\,max}}{Y_W}, \qquad (1)$$

де $N_{e\,max}$ – середнє значення питомої потужності автотранспортного засобу; $m_П$ – повна маса транспортного засобу; Y_W – рівень енергетичної навантаженості автотранспортного засобу.

При повній масі і реалізації максимальної конструктивної скорості, в разі подальшого гальмування автотранспортного засобу гальмівні механізми розсіюють найбільшу кількість енергії.

З огляду на величину Y_W, отримаємо

$$E_{max} = \frac{N_{e\,max}}{0{,}047(1 \pm 0{,}128)} = \frac{21{,}277}{(1 \pm 0{,}128)} N_{e\,max}\ , \text{Дж} \qquad (2)$$

Середня температура нагріву фрикційних поверхонь передніх і задніх гальм при циклічних гальмуваннях автотранспортних засобів можна визначити з виразу

$$t^0 = t_0^0 + \frac{21{,}277}{(1 \pm 0{,}128)} \frac{m_П N_{ПТ}}{z_T C_{уд} M_Р}. \qquad (3)$$

де t_0^0 – температура навколишнього середовища (початкова температура при гальмуванні; $N_{ПТ}$ – питома потужність автотранспортного засобу; $C_{ПТ}$ – питома теплоємність матеріалу ротора гальмівного механізму; M_P – маса ротора; z_T – число гальмівних механізмів автотранспортного засобу.

Якщо обмежувати температуру робочих поверхонь гальмівних механізмів максимально допустимою величиною $[t^0]$, то вимога до сумарною теплоємності гальм автотранспортних засобів визначається

$$C_Σ = C_{ПТ} M_Р z_Т. \qquad (4)$$

Можна виразити, перетворивши рівняння (4) до наступного вигляду:

$$[C_Σ] = \frac{13028 m_П}{[t^0] - t_0^0} \{1{,}043 - \exp[-0{,}382(1 \pm 0{,}366)(\lambda_0 + \Delta\lambda)]\}^2, \text{ Дж/град.} \qquad (5)$$

Рівняння (4) дозволяє прогнозувати мінімально допустиму величину сумарною теплоємності роторів гальмівних механізмів. Для побудови прогнозу необхідно знати максимальну допустиму температуру $[t^0]$ фрикційних поверхонь гальм.

Таким чином, отримані аналітичні залежності дозволяють прогнозувати збільшення енергонагруженість і теплонавантаженості тормозних механізмів з ростом максимальних потужностей двигунів і максимальних конструктивних швидкостей автотранспортних засобів.

УДК 614.2:004.087

Полоник И. С.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КИБЕРБЕЗОПАСНОСТЬ В ЗДРАВООХРАНЕНИИ В ЭПОХУ ЦИФРОВОЙ ГЛОБАЛИЗАЦИИ

Активное проникновение цифровых технологий во все сферы жизнедеятельности современного общества, преобразовывает многие виды его экономической и социальной деятельности и вносит не только ощутимые преимущества, но и новые риски, которые необходимо уметь прогнозировать и минимизировать. В охране здоровья населения стремительно набирают темпы развития, следующие приоритетные направления: создание новейших лекарственных препаратов, способных избавить человечество от ряда пока еще неизлечимых заболеваний и разработка вакцин против новых вирусов; повсеместное внедрение современных информационных технологий в медицину, таких как клиническая телемедицина, интеллектуальные системы, система распознавания патологии по изображениям, совершенствование лабораторных методов диагностики, создание «медицинского интернета вещей», включающего мобильные технологии экспресс-диагностики и мониторинга физиологических функций. Использование в здравоохранении последних разработок в сфере высоких технологий позволяет оперативно

решать такие задачи, как удаленный мониторинг, подключение к сетям общего пользования и международного информационного обмена, подключение к разнообразным специализированным облачным серверам [1].

В тоже время возрастает угроза в действиях деструктивного характера со стороны злоумышленников. По имеющихся в зарубежных источниках литературы наблюдениям и исследованиям, в последние годы происходит стремительный рост количества кибератак в сфере охраны здоровья [3,4,5,6,7]. По заявлению аналитического центра «Expirian» здравоохранение становится одной из востребованных целей киберпреступлений. Как отмечают многие авторы, интерес киберпреступников к медицинскому сектору вызван: оцифровкой медицинских документов, которые содержат личную информацию, конфиденциальные медицинские данные, номера кредитных карт, платёжную информацию, детали страхового обеспечения, номер социального страхования (М. Грег, М. Оркут); устаревшие или отсутствие системы кибербезопасности (Дж. Финкл, М. Оркут); взаимозависимость медицинского оборудования и растущая его интеграция в единую компьютеризированную сеть (М. Оркут, К. Грифантини, Д. Розиндейл); потребность пациента к широкому доступу своей электронной медицинской карты (М. Оркут); рентабельность продаж похищенных данных из информационных систем здравоохранения становится выше, чем из сектора розничной торговля, коммерческого и финансового (М. Оркут, Т. Саймонт). Кибератаки в здравоохранении способны наносить не только финансовый ущерб человеку, компаниям, медицинским учреждениям, но и потерей важной и конфиденциальной информации, а также являются угрозой для здоровья и жизни пациентов. Например, в случае удаленной атаки может происходить: блокировка функционирования медицинского оборудования, подключенного к общей сети и необходимого в неотложных ситуация; после нее изменения в отчетах данного оборудования о жизненно важных показателях здоровья.

В настоящее время в Республике Беларусь реализуются нормативно-правовые акты по развитию информатизации в стране. Динамично развивается база национального законодательства в области информационной безопасности, формируется новая комплексная отрасль – информационное право. Реализуется концепция развития электронного здравоохранения в Республики Беларусь до 2022 г., в которой одной из главной цели, является создание централизованной информационной системы здравоохранения, предполагающую интеграцию услуг электронного здравоохранения с общегосударственной автоматизированной информационной системой и Белорусской интегрированной сервисно-расчетной системой. Однако, имеется необходимость: включение в нормативную базу документов, определяющих обеспечение информационной безопасности при внедрении разработок высоких технологий в сферу здравоохранения; формирование мероприятий, рекомендаций по вопросам информационной безопасности, как для системы здравоохранения, так и всех заинтересованных лиц, на основе научно-методического изучения. Успешная реализация данных направлений возможно соединенными усилиями представителей практического здравоохранения, IT-индустрии, производителей медицинского оборудования, фарминдустрии, государственных органов управления и регуляторов, сообщества пациентов.

Список использованных источников

1. Концепция развития электронного здравоохранения Республики Беларусь на период до 2022 года Утверждена Приказом Министерства здравоохранения Республики Беларусь от 20.03.2018 г. № 244. / Министерство здравоохранения Республики Беларусь [Электронный ресурс]. – 2018. – Режим доступа: http://belcmt.by/ru/sanitation. – Дата доступа: 05.03.2019.

2. Правовая информатизация// Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: http://pravo.by/pravovaya-informatsiya/pravovaya-informatizatsiya-/ – 18.02.2020.

3. Finkle, J. Exclusive: FBI warns healthcare sector vulnerable to cyber attacks / J. Finkle // Reuters. Technology news [Digital]. – 2014. – 23 aprl. – Режим доступа:https://www.reuters.com/article/us-cybersecurity-healthcare-fbi exclusiv/exclusive-fbi-warns-healthcare-sector-vulnerable-to-cyber-attacks-idUSBREA3M1Q920140423 – 08.12.2019

4. Why Your Medical Records Are No Longer Safe / M. Gregg // Healthcare.Gov: Consequence of stolen identity hearing before the committee on science, space, and technology House of Representatives one hundred thirteenth congress second session. – Washington, 2014. – Serial No. 113-62. – P. 42-49.

5. Grifantini, K. "Plug and Play" Hospitals / K.Grifantini // MIT Technology Review [Digital]. – 2008. – 9 jun. – Режим доступа: https://www.technologyreview.com/s/410429/plug-and-play-hospitals/ – 10.12.2019.

6. Orcutt, M. Hollywood Hospital's Run-In with Ransom ware Is Part of an Alarming Trend in Cybercrime / M. Orcutt // MIT Technology Review [Digital]. – 2016. – 18 febr. – Режим доступа: https://www.technology review.com/s/600838/Hollywood-hospitals-run-in-with-ransom ware-is-part-of-an-alarming-trend-in-cybercrime/ – 02.03.2019.

7. Simonite, T. With Hospital Ransom ware Infections, the Patients Are at Risk / T.Simonite // MIT Technology Review [Digital]. - 2016. – 1 aprl. – Режим доступа: https://www.technology review.com/s/601143/with-hospital-ransom ware-infections-the-patients-are-at-risk/ – 19.02.2020.

УДК 621.391

Ємцев О. І., **Даневський М .Р.**

АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ЗНИЩЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

В зоні проведення операції об'єднаних сил (ООС) на Сході України продовжуються польоти безпілотних літальних апаратів (БпЛА) для ведення розвідки в інтересах артилерійських підрозділів як незаконних збройних формувань так і підрозділів російських збройних сил. Відомі факти, коли після обльоту БпЛА через нетривалий час були здійснені обстріли позицій підрозділів Збройних Сил України з артилерійського та танкового озброєння. Виходячи з цього боротьба з БпЛА являється одним із пріоритетних завдань. В зоні проведення ООС на Сході України продовжуються польоти безпілотних літальних апаратів (БпЛА) для ведення розвідки в інтересах артилерійських підрозділів як незаконних збройних формувань так і підрозділів російських збройних сил. Відомі факти, коли після обльоту БпЛА через нетривалий час були здійснені обстріли позицій підрозділів Збройних Сил України з артилерійського та танкового озброєння. Виходячи з цього боротьба з БпЛА являється одним із пріоритетних завдань.

Рекомендації щодо боротьби з БпЛА можна розділити на дві групи: організаційні та технічні заходи, а саме: розгортання в районі дії підрозділів спостерігачів, які б попереджали про появу БпЛА, здійснювали цілевказівки, маскування та дезорієнтації операторів БпЛА. Для вибору варіанту протидії БпЛА необхідно провести ідентифікацію літального апарату. В ряді випадків розпізнавання БпЛА проводиться за їх силуетами (розмірами), що зазвичай дозволяє визначити їх призначення – проведення розвідки, ударні задачі, забезпечення бойових дій. Низькі значення показників ефективності ураження малорозмірних БпЛА активними зенітними засобами обумовлюють необхідність розробки і проведення комплексу спеціальних заходів щодо організації їх ураження активними засобами, а також проведення ряду заходів з протидії системам розвідки і вогневого придушення, наявними на борту БпЛА.

Такий перелік заходів може включати:

- створення спеціальних груп із зенітних формувань, що включають різнотипні ЗРК, ЗАК, ЗПРК, ПЗРК, які мають порівняно високими розвідувальними і вогневими можливостями при виявленні та стрільби по малорозмірних цілям і призначені виключно для ураження БпЛА;
- вдосконалення (модернізація) існуючих зразків зенітного озброєння в інтересах підвищення ефективності боротьби з малорозмірними цілями;
- розробку перспективних зразків зенітного озброєння стосовно до вирішення специфічних завдань виявлення і ураження малорозмірних повітряних цілей, включаючи БпЛА;
- розробка спеціалізованих комплексів і засобів боротьби з малорозмірними цілями, заснованих на застосуванні нетрадиційних видів зброї;
- застосування комплексу «військових» заходів з протидії системам розвідки, управління і бойового застосування БпЛА.

УДК 621.391

Симоненко О. В., Маркуш В. О., Сироватко О. В.

УПРАВЛІННЯ МЕРЕЖЕВИМИ РЕСУРСАМИ З АДАПТИВНИМ ОБМЕЖЕННЯМ АБОНЕНТСЬКОГО ТРАФІКУ

Ефективність сучасних телекомунікаційних систем (ТКС), яка тісно пов'язана з наданням послуг гарантованої якості (Quality of Service, QoS), багато в чому визначається складом і результативністю рішень задач мережевого управління, що особливо проявляється в умовах перевантаження і обмеженості мережевих ресурсів. Особлива роль в рамках сучасних і перспективних ТКС відводиться засобам управління мережевими ресурсами (канальної ємністю, буферним простором і обчислювальною потужністю мережевих вузлів, параметрами трафіку і т.д.), заснованих на якісному і, що важливо, на узгодженому вирішенні задач управління чергами, пріоритетами, маршрутизацією, а при необхідності і самою структурою системи.

На практиці в сучасних ТКС, більшість з яких спроектовані на основі мережевих технологій IP (Internet Protocol), ATM (Asynchrony Transfer Mode) і MPLS (MultiProtocol La-bel Switching), завдання узгодженості рішень стоїть досить гостро. Координація роботи протоколів маршрутизації OSPF (Open Shortest Path First), IS-IS (Intermediate System - to - Intermediate System) і PNNI (Private Network - to - Network Interface), що використовуються в цих технологіях, з механізмами управління надходять в мережу трафіком GTS (Genetic Traffic Shaping) і DTS (Distributed Traffic Shaping) не провадиться. Алгоритми обслуговування черг WFQ (Weighted Fair Queuing), DFQ (Distributed WFQ) і WRR (Weighted Round Robin) і засоби обмеження транзитного (внутрішньомережевого) трафіку і трафіку, що надходить від абонентів (мереж доступу), – RED (Random Early Detection) і WRED (Weighted RED) здійснюють лише локальний контроль за перевантаженням кожного окремо маршрутизатора ТКС, що не може не позначитися на загальній продуктивності системи.

З метою з'ясування причин ситуації, що склалася, варто відзначити, що протоколи маршрутизації OSPF, IS-IS і PNNI засновані на комбінаторних методах пошуку найкоротшого шляху в мережі із заданою метрикою, а механізми GTS і DTS, в свою чергу, використовують евристичні схеми типу «кошика маркерів ». Різнотипність використовуваних моделей маршрутизації та доступу помітно ускладнює, а іноді і просто зводить до нуля можливість здійснення координації мережевих процесів і отримання узгоджених рішень задач мережевого рівня.

Таким чином, високий рівень узгодженості в рішенні задач маршрутизації та абонентського доступу може бути досягнуто лише при використанні єдиної математичної

моделі ТКС, яка забезпечує формалізацію процесів управління як мережевими ресурсами, так і доступом до мережі. У зв'язку з цим набуває особливої актуальності задача розробки моделі комплексного вирішення задач маршрутизації та обмеження абонентського навантаження в територіально-розподілених ТКС. При цьому за основу буде прийнята модель вирішення маршрутних завдань, тому що саме маршрутизація є основним засобом запобігання перевантаження мережі.

УДК 621.391

Захарченко В. В., Пархоменко Д. О.

ПІДХІД ДО АВТОМАТИЗАЦІЇ ПРОЦЕСУ ВИБОРУ МАРШРУТУ ПОЛЬОТУ ГРУПИ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПРИ ПРОВЕДЕННІ ПОВІТРЯНОЇ РОЗВІДКИ

Аналіз математичної моделі польоту групи безпілотних літальних апаратів (БПЛА) показав – знаходження оптимальної траєкторії навіть на короткій ділянці пов'язане з надмірною обчислювальною складністю, що призводить до необхідності пошуку більш простих моделей для визначення маршруту польоту групи БПЛА при проведенні повітряної розвідки. Тому запропонована методика базується на використанні дискретної моделі польоту групи БПЛА і розроблена з використанням теорії графів.

Для розробки дискретної моделі польоту групи БПЛА представимо політ БПЛА як послідовне відвідування певних областей простору. Розіб'ємо простір пошуку маршруту на елементи. При розбивці простору слід врахувати наступне:

- елемент повинен бути досяжний з одного або декількох попередніх елементів, щоб забезпечити безперервність маршруту польоту БПЛА;
- у процесі досягнення деяких наступних елементів БПЛА може змінити курс;
- можливість досягнення наступного елементу простору залежить від курсу БПЛА, з яким він увійшов у вихідний елемент, з врахуванням маневрених характеристик БПЛА;
- оскільки можливість досягнення наступного елементу простору залежить від поточного курсу БПЛА, необхідно одночасно з дискретизацією простору дискретизувати напрямок польоту. Кількість дискретних курсів польоту буде тісно пов'язана з розмірами елементу та маневреними характеристиками БПЛА;
- можливості досягнення наступних елементів повинні бути симетричні. Тому довжина елемента повинна бути дорівнює ширині;
- точність розв'язку буде зростати зі зменшенням елементу простору й збільшенням кількості дискретних курсів польоту.

Можливий підхід до розбиття простору, що враховує маневрені можливості БПЛА. Пропонується обрати вісім різних курсів польоту. З кожного елементу простору можливо буде досягнути три сусідніх фронтальних за курсом елементи з можливим поворотом на 45 градусів.

Формально простір пошуку маршруту опишемо за наступними допущеннями: вважаємо, що простір усередині елемента має однакові властивості; вважаємо, властивістю простору мультиплікативний штраф за прокладку маршруту БПЛА через елемент простору.

Опишемо політ БПЛА зваженим орієнтованим графом. Кожний елемент простору може бути відвіданий БПЛА з одним із дискретних курсів. Тому кожному елементу простору буде відповідати кількість вершин графу, що дорівнює кількості дискретних курсів польоту. Таким чином, кількість вершин графу дорівнює кількості елементів простору пошуку, помноженому на кількість дискретних курсів польоту. З кожної вершини виходять орієнтовані ребра, що з'єднують її із суміжними вершинами. Вони відповідають трьом наступним фронтальним за курсом елементам з можливим поворотом

на 45°. Вага ребра графу дорівнює кількості палива, необхідного для досягнення сусіднього елементу з обраним курсом, помноженому на штраф, відповідний елементу простору, у який ребро входить.

Таким чином завдання автоматизації процесу визначення маршруту БПЛА зводиться до завдання пошуку найкоротшого шляху між двома вершинами на графу.

УДК 629.7.067.8

Падалко І. О., Пархоменко Д. О.

ПЕРСПЕКТИВИ РОЗВИТКУ МЕТОДІВ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ СКЛАДНИХ СИСТЕМ БОРТОВОГО КОМПЛЕКСУ УСТАТКУВАННЯ

Головним завданням розвитку авіаційно-транспортної системи є пошук нових підходів у вирішенні проблеми підвищення безпеки польотів літальних апаратів. Очевидно, що традиційна ретроактивна ідеологія профілактики авіаційних подій, побудована на суворому дотриманні нормативних вимог і впровадженні профілактичних рекомендацій, розроблених за результатами розслідування подій, що відбулися, себе вичерпала [1]. Тому Міжнародна організація цивільної авіації – ІКАО розробила принципово нову ідеологію профілактики авіаційних подій та інцидентів, названу "управлінням безпекою польотів". Нова ідеологія запобігання авіаційних подій та інцидентів передбачає створення в авіакомпанії системи управління безпекою польотів [2], яка:

- виявляє фактичні та потенційні загрози безпеці польотів;
- гарантує прийняття коригувальних заходів, необхідних для зменшення факторів ризику / небезпеки;
- забезпечує безперервний моніторинг і регулярну оцінку досягнутого рівня безпеки польотів.

Система управління безпекою польотів акцентована не на очікуванні негативної події, а на виявленні небезпечних факторів в авіаційній системі, які ще не проявилися, але можуть стати причиною інцидентів, аварій і катастроф. Такий підхід у профілактиці авіаційних подій отримав найменування "проактивний". По суті, проактивне обслуговування передбачає той же реагуючий підхід, як і обслуговування за станом з контролем параметрів, але в якості діагностичних ознак вибираються такі параметри системи, спостереження яких дозволяє контролювати глибинні причини деградації факторів стабільності системи.

Накопичений досвід розслідування авіаційних подій показав [3], що кожне з них було обумовлено впливом кількох причин, які довгий час приховувались в вигляді недоліків (небезпечних факторів або факторів ризику) компонентів авіаційної системи. Заходи щодо забезпечення безпеки польотів повинні бути спрямовані на контроль за організаційними процесами, що містять приховані умови у вигляді недоліків в конструкції обладнання, упущення в підготовці персоналу і т.п., а також для поліпшення умов на робочому місці. При впровадженні управління безпекою польотів зміст профілактичної роботи визначається небезпечними чинниками компонентів авіаційної системи. Тому, відповідно до проактивного підходу, розробляються спеціальні методики, призначені для оцінки ступеня ризику прогнозованих подій.

Список використаних джерел

1. Doc. 9859 – AN/460. Керівництво з управління безпекою польотів. – Міжнародна організація цивільної авіації – ІКАО. 2006.

2. Doc. 9859 – AN/474. Керівництво з управління безпекою польотів. – Міжнародна організація цивільної авіації – ІКАО. 2009.

3. Коптев А. Н. Совершенствование технологических процессов технического обслуживания функциональных систем летательных аппаратов / А. Н. Коптев, Н. В. Чекрыжев // Известия Самарского научного центра Российской академии наук. – 2013. – Т.15. – №6(4). – С. 841-848.

УДК 621.396.6

Сакович Л. М., Мирошниченко Ю. В.

МЕТОД РОЗРОБКИ АЛГОРИТМІВ ДІАГНОСТУВАННЯ РАДІОЕЛЕКТРОННИХ КОМПЛЕКСІВ

Засоби зв'язку безперервно розвиваються в напрямку підвищення якості зв'язку, що викликає їх відповідне ускладнення. Крім того, засоби зв'язку об'єднуються в радіоелектронні комплекси (апаратні і комплексні апаратні зв'язку). При цьому кількість елементів також збільшується, що затрудняє пошук дефектів, а вимоги до середнього часу відновлення залишаються незмінними і постійними. Ця обставина вимагає розвитку технічної діагностики, пошуку нових методів локалізації дефектів у великих системах за обмежений час.

Розглядається можливість використання комплексного показника, що враховує надійність, часові та вартісні показники перевірки окремих підсистем об'єкту великої розмірності для побудови алгоритму його діагностування. Це дозволяє скоротити середній час відновлення комплексу за рахунок першочергової перевірки стану найменш надійних підсистем, які потребують мінімальних працевитрат і вартості на перевірку і відновлення. Наведений приклад використання методу та кількісна оцінка ефективності його застосування. Отримані результати в подальшому дозволяють скоротити час і працевитрати на відновлення при поточному ремонті перспективних зразків і комплексів зв'язку.

Технічна діагностика, як наука, досліджує практично реалізовані методи і методики скорочення часу і вартості локалізації дефектів, підвищення ймовірності знаходження їх місця в несправному об'єкті, але середній час діагностування при поточному ремонті радіоелектронних комплексів (РЕК) складає до 80% часу відновлення їх працездатності. Тому завдання підвищення ефективності технічного діагностування засобів зв'язку завжди є актуальним.

Відомі методи розробки алгоритмів технічного діагностування об'єктів відрізняються і залежать від інформації про його складові частини:

- при наявності тільки структурної схеми об'єкту, доцільно використовувати метод половинного ділення (діхотомію);
- якщо відомі інтенсивності відмов елементів і час виконання перевірок, то умовний алгоритм діагностування (УАД) виробу розробляють з використанням ймовірності переважного вибору перевірок, що значно скорочує середній час пошуку дефектів.

Але ці методи не враховують можливість відмови засобів вимірювань (ЗВ), тобто їх метрологічну надійність, а також вартість перевірок. Цю обставину враховує комплексний коефіцієнт, який використовують для визначення порядку перевірки РЕК при їх технічному обслуговуванні за станом.

Мета – отримання послідовності перевірки підсистем РЕК для мінімізації часу постановки діагнозу за рахунок першочергової перевірки стану найменш надійних підсистем, які потребують найменших працевитрат і вартості на перевірку та відновлення у вигляді УАД при обмеженнях, що відповідають ремонту РЕК в польових умовах (на склад ЗВ, кількість і кваліфікацію екіпажу).

Метод призначений для розробки УАД РЕК. Його сутність полягає в комплексному обліку показників надійності, вартості і часу перевірки стану елементів (підсистем)

об’єкту. Необхідні для реалізації вихідні дані отримують з технічної документації РЕК і результатів дослідної експлуатації:

- відомості про склад об’єкту;
- показники надійності окремих підсистем;
- відомості про ЗВ (вартість, метрологічні характеристики);
- дані про часові і вартісні показники перевірок підсистем РЕК.

Обмеження на використання методу:

- можливість поділу РЕК на окремі підсистеми;
- можливість автономної перевірки працездатності окремих підсистем РЕК;
- реалізація ремонту агрегатним методом;
- вибір ЗВ зі списку дозволених;
- відновлення працездатності фахівцями штатного екіпажу.

Припущення при використанні методу:

- врахування метрологічної надійності ЗВ;
- комплект ЗВ дозволяє перевірку усіх підсистем і залишається незмінним;
- кваліфікація фахівців відповідає посаді.

Перераховані обмеження і припущення відповідають умовам поточного ремонту РЕК у військових мобільних апаратних технічного забезпечення.

Метод дозволяє обгрунтувати послідовність виконання перевірок РЕК під час діагностування в процесі поточного ремонту штатними екіпажами або із залученням фахівців апаратних технічного забезпечення в польових умовах. Схема реалізації методу приведена на рис. 1.

Рисунок 1 – Схема реалізації методу розробки алгоритмів діагностування радіоелектронних комплексів

Запропоновано метод розробки умовних алгоритмів діагностування радіоелектронних комплексів на першому етапі поточного ремонту (визначення несправних підсистем або блоків) і порядок його реалізації, що дозволяє скоротити середній час відновлення за рахунок використання комплексного коефіцієнту при оцінці значення ймовірності переважного вибору елементів об’єкту. Це дозволяє при постійному значенні середньої кількості перевірок за рахунок їх упорядкування до десяти відсотків скоротити середній час відновлення в порівнянні з відомими методами. Отримані результати доцільно використовувати під час розробки діагностичного забезпечення перспективних зразків засобів і комплексів спеціального зв’язку для підвищення ефективності їх поточного ремонту.

Подальші дослідження слід направити на розгляд можливості удосконалення процесу пошуку кратних (множинних) дефектів при відновленні працездатності об’єктів зі

слабким ступенем аварійних або бойових пошкоджень в польових умовах фахівцями апаратних технічного забезпечення.

УДК 378.004

Радзіковський С. А.

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ЯКІСТЬ ПІДГОТОВКИ ВИПУСКНИКІВ ВІЙСЬКОВИХ ВИШІВ

Зростання кількості та об'єму інформаційних потоків призвело до зростання кількості інформації і, як наслідок, впровадження нових інформаційних технологій (ІТ) у повсякденну життєдіяльність. Ці зміни висунули нові вимоги до військових кадрів, їх підготовки та навчання, зумовили зміни нормативних вимог до посадовців, їх управлінської компетенції, здатності орієнтуватись у інформаційних потоках. Уміння офіцера використовувати надбання науково-технічного прогресу, вільно почувати себе в інформаційному просторі, у якому він виконує свої обов'язки, навички швидко та якісно працювати з інформацією, що постійно надходить, – ось головні пріоритети навчально-пізнавальної діяльності випускників Національної академії сухопутних військ імені гетьмана Петра Сагайдачного (НАСВ), де ІТ докорінно змінили підходи до процесу підготовки військових кадрів. Сьогодні використання новітніх ІТ передбачає у своєму складі сукупність інтелектуальних інформаційних систем, без яких організація управління освітнім закладом і процесом навчання стають неможливими.

В сучасному військовому виші всі інформаційні ресурси логічно пов'язані в єдиний процес, основним змістом реалізації відповідного підходу до формування якого є визначення стратегії навчального закладу та алгоритму її досягнення. Цей алгоритм містить опис взаємовідносин і взаємозв'язків між структурними підрозділами вишу, передбачає термін отримання результатів реалізації конкретних функцій. Локальна обчислювальна мережа є основною мережею в академії і забезпечує: використання навчальних класів для тестування, інтерактивного навчання тощо; роботу користувачів з внутрішньою web-сторінкою закладу, ftp-сервером, який містить необхідне програмне забезпечення, що не потребує ліцензування; вхід до внутрішнього чату за допомогою програмного забезпечення Jabber з питань повсякденної діяльності; доступ до електронного каталогу загальної бібліотеки на базі програмного забезпечення універсальний фондовий дім "Бібліотека". Доцільно виділити наступні функції бібліотеки: формування сучасних ресурсів, що складаються відповідно до специфіки підготовки військових фахівців; створення спільно з кафедрами електронних баз даних; налаштування пошукової системи електронного каталогу; застосування ефективних каналів передачі інформації і доступу до електронних ресурсів; переведення до електронного вигляду видань, яких недостатньо для забезпечення навчально-виховного процесу; використання локальної комп'ютерної мережі як ефективного засобу комунікацій внутрішніх і зовнішніх користувачів; використання інтернет-технології передачі інформації, отримання даних і відомостей у світовому інформаційному просторі тощо. Завдяки розумному поєднанню традиційних та електронних інформаційних ресурсів, індивідуальних і колективних методів роботи в академії тривалий час користується попитом дистанційна форма навчання, яка надає військовослужбовцям реальну академічну свободу, підвищує їхню відповідальність за якість навчання та успішність самоосвітньої підготовки.

Основою сучасної освітньої системи є високоякісні навчальні продукти, створені засобами ІТ. Серед них – електронні підручники, навчальні посібники, тестові комп'ютерні системи, електронні карти, електронні розрахункові завдання, що передбачають інтерактивні процеси навчання та забезпечують формування електронного на-

вчального середовища вишу. В НАСВ науково-педагогічними працівниками факультетів і кафедр запроваджені електронні навчальні ресурси за всіма напрямами підготовки військових фахівців, зокрема повнотекстові конспекти лекцій, доповнені ілюстративним матеріалом із використанням медіа-технологій.

Електронні навчальні посібники розміщуються на web-сторінках кафедр у локальній мережі академії, характеризуються доступністю та зручними умовами для використання, сприяють розвитку навичок самостійної роботи майбутніх офіцерів. Проте, розповсюдження електронних навчальних курсів і формування експертно-навчальних систем не вирішують наукову проблему щодо інформаційного забезпечення навчально-виховного процесу та передбачають запровадження новітніх педагогічних підходів в усіх сферах навчальної діяльності.

Поява таких технологій, як гіпертекст, використання в комп'ютерних програмах звуків і графіки, застосування графіки, відео в режимі реального часу, надання можливості здійснювати моделювання бою, використання електронних підручників забезпечило активне впровадження ІТ в освітній процес. Сьогодні мультимедійна техніка дозволяє інтегрувати різні засоби представлення інформації – текст, статичну та динамічну графіку, аудіо та відео в єдиний комплекс. Такий підхід суттєво впливає на процес інтенсифікації навчального процесу, слугує оптимальному поєднанню провідної ролі викладача та групових, індивідуальних способів підготовки випускників до майбутньої професійної діяльності.

Серед ІТ, які найбільш ефективно використовуються в навчальному процесі, слід відмітити наступні: мультимедійні системи (CD-sys), електронна пошта (e-mail), голосова електронна пошта (v-mail), електронний підручник, навчальний посібник (e-tbook), електронний бібліотечний каталог (e-libr), банк даних (db), локальні та розподільчі (глобальні) обчислювальні системи (LAN/WAN).

Безперервно триває процес впровадження інноваційних засобів навчання. Зокрема з 2017 року в академії ефективно функціонує Центр імітаційного моделювання бойових дій – це комплекс світового рівня, де готуються штаби батальйонів, бригад, проводяться командно-штабні комп'ютерні навчання рівня "рота – бригада". На базі Міжнародного центру миротворчості та безпеки (МЦМБ) запроваджено в підготовку програмне забезпечення з віртуального бойового середовища. Продовжується робота з використання в підготовці американської системи лазерної імітації ведення бойових дій MILES. Крім того, розроблено та пройшло випробування вітчизняне обладнання системи лазерної імітації бою LASERTAG.

Аналіз отриманих результатів дає підстави зробити висновок, що розглянута стратегія впровадження в освітній процес новітніх досягнень ІТ дозволяє формувати інформаційну інфраструктуру управління вишем, упорядкувати та систематизувати інформаційні потоки, автоматизувати процеси їхньої обробки та зберігання. Разом з тим, використання сучасних технологій сприяє забезпеченню якісної підготовки випускників на нових освітніх і професійних компетентностях, формуванню інформаційної культури всіх учасників освітнього процесу, дає можливість підвищення освітніх стандартів, що гарантує виведення системи підготовки військових кадрів і системи управління навчальним закладом на новий рівень розвитку.

В умовах збройного протистояння російській агресії інтеграційний курс України актуалізує проблему адаптації військової освіти до відповідних стандартів НАТО, за якими основоположною метою навчального закладу повинна стати якісна підготовка випускників до майбутньої професійної діяльності. Бойовий досвід українського війська, набутий в ході проведення операції Об'єднаних сил (Антитерористичної операції) на сході країни, переконливо свідчить, що вихованці НАСВ гідно виконують свої обов'язки на цій війні: за мужність і героїзм понад 300 із них відзначені державними нагородами, 9 – стали Героями України.

УДК 355.004.9

Радзіковський С. А., Середенко М. М.

ЩОДО ОСОБЛИВОСТЕЙ ЗАХОДІВ КІБЕРНЕТИЧНОГО ЗАХИСТУ ВІЙСЬКОВИХ ОБ'ЄКТІВ ЗА УМОВ ГЛОБАЛЬНОЇ ІНФОРМАТИЗАЦІЇ

Сьогодні інформаційна компонента в стратегії підтримання на відповідному рівні національної і воєнної безпеки держави вийшла на перший план, що обумовлено наступними чинниками: руйнування та дезорганізація інформаційної інфраструктури країни порівнюється з наслідками застосування зброї масового ураження; в умовах сучасної геополітики центр тяжіння протиборства розвинених держав переміщується від традиційної військової до інформаційної сфери; засоби, які використовуються для негативного впливу на інформаційний простір, є доступними терористичним угрупованням, внаслідок чого проблема забезпечення інформаційної безпеки (ІБ) стала міжнародною та порівняною з глобальною економічною та екологічною безпекою. В цьому контексті воєнна безпека держави залишається одним із пріоритетних напрямів забезпечення суверенітету України, її територіальної цілісності та недоторканості кордонів. Зміна характеру воєнних загроз на сучасному етапі розвитку військового мистецтва, а також форм і способів ведення збройної боротьби, гібридний характер дій противника висуває перед системою забезпечення воєнної безпеки держави нові вимоги щодо впровадження надійних захисних заходів. Водночас потребують подальшого вдосконалення методи та засоби кібернетичного захисту військових об'єктів за умов глобальної інформатизації.

Внаслідок бурхливого розвитку інноваційних технологій і глобальної інформатизації практично всі види озброєння та військової техніки (ОВТ) містять електронні та інформаційні компоненти, бойові дії плануються та здійснюються на єдиному інформаційному фоні за кібернетичними циклами та техніками. До найбільш важливих військових об'єктів, враховуючи ступінь ефективності управління військами та зброєю завдяки локальним і глобальним кібернетичним системам, слід віднести наступні: системи автоматизації, автоматизовані системи управління (АСУ), комплекси оперативного управління силами та засобами (пункти управління, вузли зв'язку, засоби спостереження та навігації тощо), системи управління зброєю. Крім того, інтенсивно розвиваються, впроваджуються та застосовуються технічні системи (засоби) розвідки, робототехнічні (безпілотні, безекіпажні) системи (комплекси) повітряного, наземного та морського (надводного, підводного) базування. Взагалі об'єктивною загальновизнаною реальністю став факт, який засвідчує збереження до певної міри стратегічного балансу, системи противаг і міжнародних угод у сфері звичайних озброєнь і зброї масового ураження, проте питання паритету в кібернетичному просторі залишається відкритим і проблемним. Наприклад, протягом 2016 року НАТО довелося реагувати в середньому на 500 спроб кібернападів на місяць, що становить збільшення їх кількості на 60 % порівняно із 2015 роком.

Для об'єктів, в тому числі військових, ІБ загрози можуть бути як зовнішні, так і внутрішні. Найбільшу зовнішню загрозу об'єктам ІБ завдає розвідувальна діяльність іноземних держав, кіберзагрози з метою проникнення в інформаційно-телекомунікаційні системи (ІТС) та комп'ютерні мережі. Внутрішніми загрозами є: аварії на підприємствах радіоелектронної промисловості, дестабілізація діяльності засобів масової інформації (ЗМІ), інформаційних і телекомунікаційних систем, які можуть привести до порушення громадської стабільності, викликати шкоду здоров'ю та загрозу для життя людей.

Процес забезпечення надійного кіберзахисту військових об'єктів передбачає, з одного боку, добування відомостей та інформації, що циркулює в інформаційних системах і комп'ютерних мережах, у тому числі з використанням несанкціонованого доступу, та їх обробка за допомогою апаратно-програмних засобів, а з другого боку, виявлення, ви-

вчення та систематизація даних щодо потенційних джерел кіберзагроз, що припускає використання абсолютно нових технологій і технічних прийомів.

Зрозуміло, що показниками ІБ військового об'єкту від кіберзагроз є конфіденційність, доступність і цілісність інформації або комплекс заходів, спрямованих на забезпечення захисту інформації від несанкціонованого доступу. Вплив на будь-який з цих компонентів можна розглядати, як кібернетичну атаку. Об'єктом атаки може бути персональна електронно-обчислювальна машина (ПЕОМ), мережевий пристрій, інформаційна мережа або система в цілому. Головною метою кіберзахисту є прогнозування кіберзагроз і відбиття кібератак на військовий об'єкт. Для вирішення цієї мети необхідно знати основні методи добування даних, несанкціонованого доступу (впливу), які використовує противник. Додатково може використовуватися інформація від whois-серверів, перегляд інформації DNS-серверів мережі для виявлення записів, що визначають маршрути електронної пошти. Використання методів несанкціонованого доступу неможливо здійснити без попереднього дослідження мережі, в якій знаходяться різні програмно-апаратні засоби зв'язку, а також інформаційні ресурси досліджуваного об'єкта. Наявність у противника засобів радіоелектронного придушення значно збільшують їх уразливість, тому існує гостра потреба розробки комплексного захисту та забезпечення стійкості цих об'єктів від насамперед кіберзагроз. Перед керівництвом військового відомства постає питання щодо зосередження зусиль на мінімізацію наслідків дії потенційних і реальних загроз. Разом з тим, актуальність питання обумовлена недосконалістю науково-методологічного апарату щодо забезпечення захисту об'єктів ІБ у військовій сфері.

Аналізуючи особливості першочергових заходів кібернетичного захисту військових об'єктів, слід зазначити найбільш суттєві серед них: створення системи раннього виявлення інформаційних небезпек (викликів, загроз, впливів); налагодження ефективної системи кіберзахисту військових об'єктів з урахуванням їх категорій за ступенем уразливості; підвищення ефективності інформаційно-аналітичної роботи суб'єктів інформаційної безпеки; створення та постійне оновлення бази даних порушників і порушень, у тому числі кіберзлочинців. Крім того, необхідно забезпечити умови для дотримання режиму експертного контролю та нерозповсюдження несертифікованих програмно-апаратних засобів і систем, комп'ютерної техніки, оперативного реагування на інциденти, які пов'язані з виведенням із ладу військових ІТС, а також налагодження каналів формального та неформального обміну інформацією стосовно загроз комп'ютерної злочинності та кібертероризму.

Основними напрямами підвищення рівня захищеності військових об'єктів мають бути: забезпечення комплексного підходу до вирішення завдань ІБ з урахуванням необхідності диференціювання її рівнів; розробка паспортів інформаційних небезпек – викликів, загроз, впливів; оцінка уразливості цих об'єктів; розвиток і вдосконалення захищених засобів обробки інформації; забезпечення ефективного моніторингу стану ІБ тощо.

Таким чином, практичне вирішення проблем щодо кібернетичного захисту військових об'єктів, особливо інформаційно-телекомунікаційних систем воєнного призначення, доцільно здійснити шляхом створення підрозділів швидкого реагування на злочини проти зазначених об'єктів, здатних на співробітництво з міжнародними організаціями тощо.

УДК 656.7.08

Павленко М. А., Хмелевський С. І., Хмелевська О. О., Петров О. В.

ЗАПРОПОНОВАНІ ВИМОГИ ДО МОВНИХ ЗАСОБІВ ПРЕДСТАВЛЕННЯ ЗНАНЬ

Серед вимог до мовних засобів нової інформаційної технології, можна виділити дві групи. Вимоги першої групи, складаються в забезпеченні математичної строгості мови, яка

може бути досягнута, якщо при його розробці встановити взаємно-однозначну відповідність між елементами мови і засобами математичної формалізації експертних знань. Невиконання вимог строгості не дозволяє реалізувати процедури пошуку логічного виведення при пошуку вирішення задач розпізнавання систем і не гарантує формальної коректності описів експертних знань. Тому ці вимоги повинні дотримуватися неухильно.

Вимоги другої групи, складаються з скорочення всіх видів витрат на розробку програмних засобів, призначених для вирішення завдань розпізнавання систем. Поставлена мета може бути досягнута, якщо забезпечити достатню простоту освоєння і зручність користування мовними засобами. Очевидно, що ступінь дотримання цих досить розпливчастих вимог до мови, важко піддається вимірюванню і вони можуть бути задоволені різними шляхами. Тому вимоги, віднесені до другої групи, які не є жорсткими. Щоб зменшити невизначеність цих вимог, спробуємо їх конкретизувати, спираючись на накопичений до теперішнього часу досвід розробки мовних засобів програмної інженерії. З урахуванням специфіки експертних знань сформульовані більш детальні вимоги до мови.

Концептуальна єдність мовних засобів, що застосовуються на різних стадіях розробки експертних систем. Сутність вимоги полягає в тому, щоб мовні засоби, що застосовуються на ранніх стадіях і етапах створення представляли собою підмножину мови, якою розробники користуються на наступних стадіях. Недотримання цієї вимоги ставав перешкодою на шляху скорочення витрат на розробку за рахунок наскрізної автоматизації процесів проектування і реалізації таких систем. Можливість чіткої структуризації описів експертних знань. Мова про слідування при розробці мовних засобів принципам структуризації знань, націлених на скорочення трудовитрат на їх формалізацію.

Можливість візуалізації формалізованих описів експертних знань у вигляді наочних графічних образів. Необхідно, щоб мовні засоби включали графічні символи, які дозволяють наочно представляти структуру різних аспектів формалізованого опису експертних знань з необхідним ступенем деталізації за вибором користувача, як на моніторі, так і у вигляді твердої копії, придатною до використання в складі технічної документації.

УДК 355.004:001;007

Алєксєєв В. М., Матала І. В., Безсонов В. І.

НОВІТНІ ТЕХНОЛОГІЇ ТА ЗАСОБИ ЗВ'ЯЗКУ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ: ШЛЯХ ТРАНСФОРМАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Рівень готовності Збройних Сил України до виконання завдань за призначенням безпосередньо залежить від наявності у їх складі новітнього озброєння та військової техніки, але жодне озброєння і техніка не зможуть забезпечити ефективного виконання бойових завдань без своєчасного, достовірного та безперервного управління військами і озброєнням. Тому сучасні системи управління повинні мати високі бойову готовність, пропускну здатність, стійкість, мобільність, доступність, розвідувальну захищеність, керованість, а також забезпечувати виконання вимог щодо своєчасності, достовірності та безпеки інформаційного обміну. Отже, аналіз можливостей цифрових засобів зв'язку, сучасних інформаційних технологій, які використовуються збройними силами провідних країн світу, розгляд етапів застосування цих засобів, технологій та тенденцій їх впровадження в ЗС України, дозволить виокремити основні, найбільш доцільні напрями їх подальшого впровадження під час побудови сучасної системи управління військами ЗС України.

На відміну від західних країн структура управління Збройних Сил України має характер жорсткої ієрархії, однак, «гібридна війна» на Сході України відчутно змінила ставлення до управління військовими частинами і підрозділами та використання сучасних

засобів управління і зв'язку. Сьогодні система зв'язку і автоматизації управління Збройних Сил України має стійку тенденцію до всебічного розвитку та модернізації, переоснащення військ зв'язку новітніми високотехнологічними засобами зв'язку та переходу на сучасні цифрові технології із забезпеченням необхідної якості обслуговування. Сучасні телекомунікаційні та інформаційні технології дозволяють створювати складні інформаційно-телекомунікаційні системи, складовими частинами яких є сучасні комплекси засобів зв'язку та автоматизації.

Основою польової складової системи зв'язку ЗС України сьогодні залишається супутниковий зв'язок. З причини відсутності в Україні власних супутників зв'язку, цю послугу орендують в оператора зв'язку ПрАТ «Датагрупп», з використанням їх терміналів супутникового зв'язку компанії Tooway (станцій супутникового зв'язку – ССЗ). Застосування системи Tooway дозволяє забезпечити ефективні, захищені, інтерактивні лінії зв'язку високої якості за технологією Ethernet із сотнями і, навіть, із десятками тисяч віддалених пунктів. Віддалені термінали Tooway можуть забезпечувати двосторонній супутниковий зв'язок через мережу Інтернет.

Водночас у Збройних Силах України ефективно використовуються комплекси ультракороткохвильового транкінгового зв'язку компанії «Motorola», які характеризуються високою якістю і функціональними можливостями. Ефективність застосування цих засобів пов'язана, насамперед, з невеликими габаритами і стійкістю до перешкод, можливістю технічного маскування під час ведення радіообміну.

Також, під час створення та переоснащення системи зв'язку ЗС України, велику увагу слід приділити засобам зв'язку, які вже використовують провідні країни світу – радіостанціям з параметрами, що програмуються (SDR – Software-Defined Radio). Принцип SDR технологій полягає у поєднанні функціональних можливостей комп'ютера і радіостанції. Зокрема, пристрій з SDR використовуючи декілька рівнів програмного забезпечення для виконання різних задач, так як і комп'ютер, може, наприклад, виконувати обробку тексту, забезпечувати перегляд Інтернет-ресурсів, а також управляти базами даних залежно від вимог користувача.

Протягом 2017–2019 років у ЗС України вжито ряд заходів щодо переоснащення польової (мобільної) компоненти автоматизованої системи управління, зв'язку, розвідки та спостереження, що відповідає стандартам НАТО.

Сьогодні в Сухопутних військах Збройних Сил України майже не залишилось пунктів управління підрозділів і військових частин, вузли зв'язку, в яких використовують застарілі технології та аналогові засоби зв'язку. Як первинну (транспортну) мережу передавання даних сьогодні використовують цифрові канали передавання даних, утворені за допомогою технології Ethernet з використанням проводових, волоконно-оптичних, супутникових ліній зв'язку. Провайдерами надання телекомунікаційних послуг є ПрАТ «Укртелеком» (виділення ресурсу телекомунікаційної мережі загального призначення, послуга MPLS), ПрАТ «Датагрупп» (послуга MPLS, надання супутникових каналів) тощо.

За останні роки на озброєння ЗС України надійшла система інтерком Harris RF-7800I – сучасна, гнучка, має модульну структуру, багатофункціональна цифрова система внутрішнього зв'язку для бронетехніки та інших транспортних засобів, в яку інтегруються автомобільні радіостанції Harris та засоби зв'язку інших виробників. Інтерком дозволяє значно покращити координацію екіпажів бойових машин та підвищити їх бойові можливості.

Таким чином, актуальним питанням залишається розвиток системи зв'язку та автоматизованого управління військами в напрямі створення єдиного інформаційного простору, що дозволить збільшити бойовий потенціал за рахунок автоматизації управління військами та зброєю, а також запровадити єдину автоматизовану систему управління – програмну платформу, сумісну зі стандартами НАТО.

Отриманий досвід управління підрозділами під час операції Об'єднаних сил свідчить, що системи управління та зв'язку ЗС України, як і провідних країн світу, розвиватимуться шляхом створення єдиного інформаційно-телекомунікаційного середовища, із

впровадженням сучасних інформаційно-телекомунікаційних технологій, комплексів і систем зв'язку спеціального призначення, що забезпечить обмін інформацією між органами та пунктами управління всіх ланок.

Сьогодні у Збройних Силах України відбувається цілеспрямоване переоснащення підрозділів на цифрові засоби зв'язку та автоматизації, що дозволяє надавати в інтересах пунктів управління різнорідні якісні інформаційно-телекомунікаційні сервіси.

Це дозволило особовому складу опанувати сучасні цифрові технології та об'єднати у стислі терміни достатньо велику кількість вузлів різного рангу в єдину мережу. Сьогодні активно застосовуються сучасні методи та технології. Але, знову ж виходячи з такого досвіду, досі триває пошук різних варіантів побудови системи зв'язку, в цілому, поряд з цим існує нестача військових висококваліфікованих фахівців в галузі зв'язку та телекомунікацій.

Таким чином, новітні технології та засоби зв'язку, їх трансформація та подальший розвиток у недалекій перспективі дозволять забезпечити ефективне управління підрозділами Збройних Сил України. А це в подальшому дасть можливість впровадити в Збройних силах концепцію ведення бойових дій в єдиному інформаційному просторі.

Вільгуш Д. В., Середенко М. М., Пастухов В. В.

ЗАПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАННЯ В СИСТЕМУ НАВЧАННЯ ВВНЗ ЗС УКРАЇНИ

Процес та результати реформування вітчизняної системи вищої військової освіти базуються на співробітництві з іноземними військовими навчальними закладами, вивченні їхнього досвіду, впровадженні кращих методик у процес підготовки військових фахівців для Збройних Сил України з урахуванням національних здобутків.

Скоординовані шляхи створення навчальної матеріально-технічної бази (далі – НМТБ) Збройних Сил України, визначений порядок та пріоритетність, часові рамки виконання робіт з розвитку НМТБ на період до 2020 року та подальшу перспективу, дають можливість підвищити рівень підготовки військовослужбовців ЗС України до виконання поставлених завдань.

У Національній академії сухопутних військ імені гетьмана Петра Сагайдачного існує актуальна необхідність встановлення програмного забезпечення VBS-3 («Virtual Battlespace 3»). Система віртуального моделювання воєнних конфліктів та бойових дій військ на тактичному рівні VBS-3 є професійним програмним забезпеченням і була створена приватною американською компанією, розробником військових симуляторів Bohemia Interactive Simulations (м. Орландо, Флорида, США) на замовлення уряду США у березні 2014 року, та є ведучою системою у питаннях здійснення підготовки особового складу у тривимірному просторі.

VBS-3 призначена для підготовки підрозділів рівня відділення-рота. Вона симулює основні аспекти сучасного загальновійськового бою, включаючи особовий склад, озброєння та бойову техніку та має змогу симулювати будь-яке середовище для здійснення підготовки одиночного солдата, командирів відділень використовуючи місцевість, на якій проводиться навчання (рис.1).

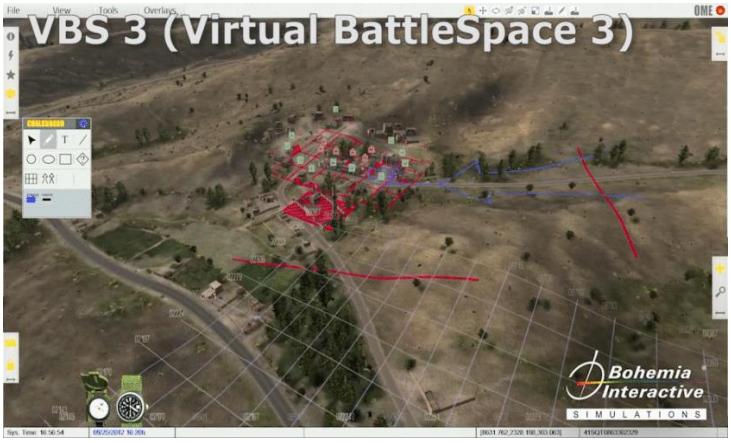


Рисунок 1 – Програмне забезпечення VBS-3

Програмне забезпечення VBS-3 використовується в збройних силах 19 країн-членів НАТО та 9 країнах-партнерах, серед них:

- ЗС США (Корпус Морської Піхоти (USMC), Сухопутні війська (US ARMY));
- ЗС Великобританії, Німеччини, Франції, Бельгії, Польщі, Австралії, Нової Зеландії, Бразилії та ін.;
- Об'єднаний багатонаціональний Центр імітаційного моделювання (JSMC);
- Національна лабораторія Лоуренса Лівенмора (LLNL);
- Південно-Європейська тактична група (SETAF).

Програмне забезпечення VBS-3 дозволяє в широкому діапазоні можливих сценаріїв імітувати:

- тактичні дії як окремого солдата, так і підрозділу (до роти включно);
- процес бойового застосування будь-якого озброєння та військової техніки;
- будь-яке середовище, кліматичні та погодні умови, в яких можуть вестись бойові дії.

Можливості VBS-3:

- розробка та моделювання будь-якого сценарію ведення бойових дій;
- тактична підготовка (до рівня роти);
- загальновійськова або міжвидова підготовка;
- аналіз операцій (сприяння ефективному прийняттю рішень);
- додаткове віртуальне середовище для реального та конструктивного імітаційного моделювання чи тренажеру для відпрацювання навичок екіпажу ОВТ;
- орієнтування на полі бою;
- реакція на саморобні вибухові засоби, масові виступи місцевого населення, гуманітарна допомога, захист мирного населення та інше;
- можливість моделювання різноманітних ввідних за будь-якими умовами обстановки.

Отже, використання програмного забезпечення VBS-3 дозволяє створити реальну обстановку, відтворювати реальне виконання бойових завдань в віртуальному середовищі, здійснювати управління підрозділом в реальній обстановці, значно підвищує практичні навички курсантів в організації бойових дій, а також дозволяє економити ресурс бойової техніки та паливно-мастильних матеріалів;

Тренування особового складу доцільно проводити протягом всього періоду навчання курсантів на I-IV курсах, особливо доцільно проводити тренування в поєднанні з вивченням дисципліни «Управління діями механізованих підрозділів» («Управління діями танкових підрозділів») при вивченні дій відділення, взводу, роти; водночас доцільно проводити тренування перед проведенням практичних занять в полі.

Зважаючи на обмежену кількість робочих місць та технічні можливості ЦІМ МЦПП МЦМБ, оптимальна кількість курсантів, з якими можливо одночасно якісно проводити подібне тренування – 3-4 навчальні групи.

В основу подальшого реформування системи військової освіти покладені завдання підвищення якості та приведення змісту й технологій навчання військових фахівців у відповідність до сучасних завдань Збройних Сил України та вимог щодо їх підготовки з максимальним використанням досвіду операцій об`єднаних сил та передових методик підготовки армій країн-членів НАТО, впровадження технологій дистанційного навчання.

УДК 355.623.62

Пастухов В. В., Пашковський В. В.

КІБЕРБЕЗПЕКА ЯК ВАЖЛИВА СКЛАДОВА СИСТЕМИ ЗАХИСТУ ДЕРЖАВИ

Ми живемо в епоху інформаційного суспільства, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини в державі.

Сьогодні ми все більше використовуємо їх у своїй діяльності, не є винятком і Збройні Сили України. Але взявши на службу телекомунікації і глобальні комп'ютерні мережі, слід знати та розуміти, які можливості для зловживання створюють сучасні технології. Сьогодні жертвами хакерів можуть стати не лише люди, але і держави.

За ефективністю та наслідками застосування кіберзброї, а саме такий термін все частіше використовують вчені, можна прирівняти до засобів масового ураження. Тому кібербезпека – одна з основних проблем, що викликає занепокоєння. І чим швидше людство розвиває інформаційні технології, тим більшою є потреба в захисті інформаційно-телекомунікаційних систем кібератак. Оскільки критична вразливість в програмному забезпеченні та автоматизованих системах викликають небезпідставні побоювання про глобальність порушень і негативних наслідків втручання, то не дивно, що уряди та суспільство в усьому світі шукають кращих заходів і методів для захисту особистих даних Інтернет-ресурсів від кіберзагроз. На підтвердження цього, під час проведення зустрічі на вищому рівні глав держав та голів урядів країн-учасниць Північноатлантичного альянсу, яка проходила у 2016 році у Варшаві, була підписана перша в історії угода між ЄС та НАТО «Про співпрацю у сфері безпеки», зокрема в питаннях гібридних війн та кібератак. Кіберпростір, поряд із землею, повітрям, морем і космосом, визнано новим оперативним простором, а кібероперації – невід'ємною частиною кібервійни.

Кібервійна – це можлива війна найближчого майбутнього, безкровна, проте – смертельна. Це в своєму роді – переворот в мистецтві ведення війн. Людство дійшло до такого ступеню розвитку, що і звичайний ноутбук стає в руках професіоналів справжньою зброєю. В сучасному світі від комп'ютерів залежить багато: тиск в нафтопроводах, функціонування енергосистем, рух повітряних суден, робота лікарень и екстрених служб. Дані системи функціонують з використанням програмного забезпечення та зусиль фахівців і, відповідно, вразливі для вірусних програм, дія яких може призвести до феноменальних наслідків з нанесенням економічного і фізичного збитку, якій наближується, а іноді перевищує, дію звичайної зброї.

Найбільше уваги операціям у кіберпросторі приділяють такі провідні країни світу як Сполучені Штати Америки, Великобританія, Китай та ін. У них бюджетом закладені величезні кошти на розвиток кібернетичної складової збройних сил, а також постійно втілюються в життя програми для забезпечення національної безпеки та захисту об'єктів критичної інфраструктури від кібератак. Оскільки ніхто не може з упевненістю стверджувати, що його мережі повністю захищені та можуть протистояти багатовекторним кібератакам кібернетична безпека стала пріоритетом розвитку сучасної армії. Однією з причин такого стрімкого розвитку підрозділів кібернетичної безпеки стала «гібридна війна», яку розв'язала та продовжує вести Росія проти України. Агресор активно використовує кіберпростір у війні не тільки проти України, а й проти інших держав. Наприклад масштабна кібератака на корпоративні та державні мережі за допомогою вірусу «NotPetya», яка відбулася 27 червня 2017 року – яскравий урок важливості кібернетичної безпеки для функціонування держави.

Подібні кібератаки спрямовані на дестабілізацію суспільства – «обмежити, знищити, дестабілізувати» – ось їхня мета. Хоча, на перший погляд може здатися, що кібератаки не можуть завдати значної шкоди оскільки не забирають людських життів, проте наслідки можуть бути незворотними і небезпечними тому, що під час кібератак застосовують: вандалізм – атака, яка, не вбиває людей, але завдає удару авторитету держави; пропаганда – розсилка спаму, що містить інформацію пропагандистського характеру та дезорієнтує населення; збір інформації – злом приватних сторінок або серверів баз даних для збору цінної інформації та її заміни на інформацію, корисну іншій стороні; відмова сервісу – атаки з великої кількості комп'ютерів, основна мета яких — порушення функціонування сайтів або комп'ютерних систем; втручання в роботу обладнання – атаки на комп'ютери або сервери, які, наприклад, забезпечують роботу комунікаційних цивільних або військових систем; атаки на об'єкти критичної інфраструктури – атаки

на комп'ютери та системи, що забезпечують життєдіяльність міст, а саме: системи водопостачання, електроенергії, транспорту тощо.

До того ж, масові відключення електроенергії, телефонного зв'язку та Інтернету, шахрайство при обслуговуванні клієнтів і проведенні банківських операцій, реальні фінансові збитки – це те, що використовує ворог вже сьогодні.

Для мінімізації ризиків в Україні набрав чинності закон «Про захист даних». Ним передбачається різке підвищення штрафів за розголошення чи втрату персональних даних, що змушує компанії й організації переглянути свої підходи і стандарти щодо забезпечення інформаційної та кібернетичної безпеки і випадків витоку інформації, в тому числі, введення окремих посад відповідальних за захист інформації та кібернетичну безпеку. Також, на сьогоднішній день забезпечення економічної безпеки України будується на основі офіційно прийнятого в країні нормативного акту: Закон України «Про національну безпеку України» прийнятий у 2018 р. Цей Закон визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.

Оскільки розвиток інформаційних технологій обумовлює появу нових видів кібератак, відповідно, однією з основних складових національної безпеки держави стає забезпечення інформаційної безпеки. Важливим фактором посилення заходів кібернетичної безпеки є збереження балансу між комфортом, свободою доступу до інформації та забезпеченням надійного захисту інформації – від яких багато в чому залежить благополуччя громадян і мир в Україні. Однак завдання кібербезпеки непрості і їх доведеться вирішувати ще протягом тривалого часу. В Україні почалася активна робота в цьому напрямі і для реалізації завдань інформаційної безпеки необхідно застосовувати не лише інфраструтуру, стійку до кібератак (наприклад квантові комп'ютери можуть стати одним із компонентів вирішення цього завдання), а й забезпечувати цифровий суверенітет – розвивати українське програмне та апаратне забезпечення.

Дані процеси неможливі без значних інвестицій. Крім того, для створення надійності функціонування і кіберзахищеності інформаційно-комунікаційної системи потрібно здійснювати регулярний моніторинг загроз, проводити оцінку ризиків, аналізувати кіберінциденти і вчитися мислити по-новому та створювати й удосконалювати процес підготовки кадрів – інтелектуальний потенціал – професійно підготовлених спеціалістів, здатних ефективно працювати в галузі безпеки держави для подальшого розвитку боєздатності ЗС.

Отже, кібербезпека сьогодні набуває значення нової галузі в українському соціумі і призначена забезпечити національну безпеку держави, тому своєчасне планування й реалізація заходів забезпечення кібербезпеки на глобальному і регіональному рівнях стає одним із пріоритетних завдань України.

УДК 355:623.61

Вільгуш Д. В., Кізло Л. М., Бабій Я. В.

КІБЕРБЕЗПЕКА В НАУКОВИХ УСТАНОВАХ ЗБРОЙНИХ СИЛ УКРАЇНИ: ОСОБЛИВОСТІ, ТЕНДЕНЦІЇ РОЗВИТКУ

Однією із важливих складових сучасної практики забезпечення безпеки в державних та приватних структурах є кібербезпека, що включає заходи: захисту інформації з обмеженим доступом від несанкціонованого доступу; захисту інформації з обмеженим доступом та відкритої інформації від загроз її несанкціонованої модифікації, блокування та знищення; протидії розповсюдженню неповної, невчасної та неправдивої інформації у кіберпросторі.

Здебільшого сучасні заходи із забезпечення кібербезпеки обумовлюються технологічними особливостями та можливостями сучасного кіберпростору, охоплюють технічні питання захисту інформаційних ресурсів (продуктів / активів) та захисту іміджевих позицій, як організації, так і її співробітників (професійності, гідності, ділової репутації та майнових прав фізичних і юридичних осіб).

Найбільш вразливим об'єктом у системі забезпечення безпеки вважається людина, а ступінь її вразливості залежить від багатьох факторів: рівня усвідомлення (сприйняття) можливих загроз та їх наслідків; обізнаності і досвіду щодо застосування методів захисту; індивідуальних психологічних особливостей, світоглядних позицій та морально-етичних цінностей; психологічного клімату колективу; сімейних обставин та інших складових.

Не другорядним компонентом забезпечення кібербезпеки є також рівень «інформаційної культури», яка безпосередньо пов'язана з поняттям «культура кібербезпеки». Поняття культура кібербезпеки (стосовно захисту інформації) почало поширюватися у світі після прийняття у 2003 році Резолюції Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки». У звіті Європейське агентство з питань мережевої та інформаційної безпеки (ENISA) 2017 року «Культура кібербезпеки організації» запропоновано таке визначення культури кібербезпеки: знання, переконання, уявлення, норми і цінності особистості стосовно до кібербезпеки та використанню колективних інформаційних технологій. Отже, культура кібербезпеки наукових установ – це компетентність та корпоративні цінності наукового співтовариства, пов'язані із забезпеченням особистої безпеки у кіберпросторі у відповідності із визначеною політикою кібербезпеки наукової установи.

Формування культури кібербезпеки організації (установи) направлене на зміну мислення співробітників, сприйняття ризику та спільної відповідальності за забезпечення кібербезпеки організації, сприймання заходів із забезпечення особистої кібербезпеки як звички.

Політика кібербезпеки наукової установи повинна бути орієнтована, перш за все, на попередження загроз витоку електронної інформації щодо результатів наукових досліджень, до їх офіційного опублікування та оформлення авторських прав, попередження випадків неправомірного звинувачення у порушенні авторських і суміжних прав та негативного впливу на іміджеві позиції наукового співтовариства.

Реалізація політики кібербезпеки наукової установи повинна передбачати заходи: захисту особистої кібернетичної інфраструктури співробітників установи від загроз несанкціонованого доступу до електронної інформації, її модифікації та знищення; передбачати можливість доведення авторства, цілісності та дати виготовлення електронної інформації; урегулювання питань щодо безпечного використання технологій мережі Інтернет. Політика кібербезпеки наукової установи також повинна передбачати заходи взаємодії та реагування на інциденти порушення безпеки користування інформацією у рамках діяльності наукової установи.

Відповідно, у якості основних складових формування культури кібербезпеки можна виділити навчання та мотивування співробітників наукової установи, а також етичний контроль. Але попри все, основними принципами формування культури кібербезпеки наукової установи можна вважати своєчасність, зрілість та доступність заходів із формування у співробітників корпоративних етичних норм безпекової поведінки в кіберпросторі.

Для цього в Національній академії сухопутних військ імені гетьмана Петра Сагайдачного регулярно проводяться навчання з основ формування особистої та корпоративної культури кібербезпеки. В програмі занять заплановані і проводяться заходи (лекції, тренажі, інструктажі) для опанування технологіями кіберзахисту та здійснюється контроль (здаються іспити за тестовою методикою) з визначенням рівня засвоєння знань і професійної компетентності. Проте, доцільно пам'ятати що всі заходи потрібно організовувати з врахуванням розвитку особистості кожного співробітника, пропонувати індивідуальні мотиватори для підвищення усвідомлення про важливість і відповідаль-

ність за рівень особистої культури кібербезпеки для за забезпечення спільної кібербезпеки організації.

Підсумовуючи, зазначимо, що формування культури кібербезпеки суб'єктів наукової та науково-технічної діяльності відноситься до завдань системи управління персоналом, яка повинна спрямовуватися на посилення заходів забезпечення корпоративної безпеки в питаннях захисту інформації з обмеженим доступом, авторських і спільних прав, негативного впливу на іміджеві позиції наукового співтовариства. З позиції соціального партнерства доцільно звернути увагу на заходи інформування навчання та мотивації співробітників до виконання норм корпоративної культури кібербезпеки. З технічної – це забезпечення співробітників засобами технічного і криптографічного захисту інформації, надання необхідних послуг (у тому числі, з моніторингу контенту кіберпростору) та створення умов для широкого використання електронного цифрового підпису. З правової – створення умов для надання своєчасної правової допомоги співробітникам у питаннях захисту авторських і суміжних прав, захисту честі, гідності, ділової репутації кожного.

Отже, враховуючи сучасні проблеми, з якими зустрілись ЗСУ за останні роки, а саме військова агресія, напруження в сфері міжнародних відносин, однією з найширших за своїм масштабом сфер напруження стали інформаційне і кіберсередовища. В зв'язку з чим, питання забезпечення стійкої і надійної системи кіберзахисту в ЗС України є актуальним і важливим завданням на сьогодні і – в майбутньому. Для цього буде доцільним дотримуватися елементарних правил: використовувати засоби захисту особистої інформації, пам'ятаючи, що здоровий глузд – це ваш найкращий захист; захищати ваші локальні мережі підрозділу (відділу) використовуючи паролі; при спільному використанні комп'ютера переконайтеся, що у всіх є окремі облікові записи і немає привілейованого доступу; використовуйте багатофакторну аутентифікацію – це додає захищеності завдяки персоналізованому способу для входу в систему, наприклад, отримання повідомлення або дзвінка на мобільний телефон. Проте, цей перелік не є достатнім для повного захисту, створення надійної і кіберзахищеної інформаційно-комунікаційної системи треба здійснювати постійно і регулярно за наступним алгоритмом: моніторинг загроз, оцінка ризиків, планування захисту, аналіз кіберінцидентів та виправлення помилок.

УДК 355.623:002.

Кізло Л. М., Жук О. В.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ВІЙСЬКОВИХ ФАХІВЦІВ

Становлення та розвиток інформаційного суспільства є характерною рисою XXI століття. Саме в інформаційному суспільстві набувають активного розвитку інформаційно-комунікаційні технології, створюються умови для ефективного використання знань у вирішенні різноманітних завдань, які постають перед суспільством. В Україні, в умовах сьогодення, під час проведення операції Об'єднаних сил на Сході нашої держави, запровадження системних політичних, економічних, соціальних реформ, а також трансформації системі цивільної та військової освіти, що відбуваються в країні, значно підвищився інтерес до проблеми формування професійної спрямованості та фахової підготовки військових кадрів.

Сучасний етап розвитку вищої військової освіти України характеризується повномасштабною інтеграцією в європейський освітній простір. Основою цього процесу є наближення стандартів підготовки майбутніх фахівців до загальноєвропейських. З огляду

на те, що в динамічній трансформації вищої військової школи сьогодні домінують інформаційні процеси індивідуальної траєкторії надання знань, розвиток творчих можливостей курсантів, викладачів, і всіх тих, хто забезпечує навчальний процес (парадигма особистісно-орієнтованого навчання) основою сучасної освітньої системи стають високоякісні новітні навчальні продукти, які здатні наблизити освітню систему в Україні до світових параметрів інформатизації суспільства.

Мета інформатизації суспільства – створення гібридного інтегрального інтелекту всієї цивілізації, здатного передбачити і управляти розвитком людства. Освітня система у військовій сфері в такому суспільстві має бути системою випереджувальною. Перехід від консервативної освітньої системи до випереджувальної повинен спрямовуватися на створення і розвиток інформаційного простору для широкого використання інформаційних технологій в процесі навчання. Побудова ефективних систем інформатизації освіти з урахуванням світового досвіду, особливостей і реального стану вітчизняної освіти – це одна із актуальних і важливих наукових і практичних проблем. Думка стосовно потреби сучасної освіти в інформатизації у науковців однозначна і сумнівів не викликає – і проголошується вона стосовно як середньої, так і вищої освіти, як технічної, гуманітарної так і галузевої, в тому числі і військової, як на рівні міністерського управління галуззю, так і на рівні окремих навчальних закладів.

Особливе місце у Збройних Силах (ЗС) та інших військових формуваннях України займає офіцерський склад, тому питання ефективної підготовки офіцерських кадрів є пріоритетним у концептуальному баченні забезпечення обороноздатності держави. Світовий досвід і практика доводять про доцільність впровадження у підготовку офіцерських кадрів сучасних інформаційних технологій, заснованих на досягненнях науки і техніки проте, успішність цього процесу істотно залежить від готовності системи освіти в цілому і військової освіти зокрема, в найкоротші терміни здійснювати реформи, необхідні для забезпечення належного рівня інформаційної компетентності кожного учасника світового інформаційного простору.

З погляду інформаційної природи соціуму проблема інформаційної компетентності набуває нового змісту. Її суть у тому, що в умовах сьогодення індивід (група) опиняється віч-на-віч із величезним обсягом інформації, що характеризується високою мірою невпорядкованості, часто виявляє непередбачені смислові зв’язки і прагматичні підтексти. Отже проблема формування інформаційної компетентності не в тому, що молодь не володіє навичками та засобами застосування комп’ютерних технологій і програмного забезпечення, а в тому, що уявлення про реальність разюче відрізняються від самої реальності, що, іноді, призводить до психологічного перенапруження та нестабільності й невизначеності суспільних зв’язків. У суспільних відносинах все менше йдеться про загальну користь, і все більше – про пріоритети і домінування тому сучасні інформаційні технології мають бути засобами підтримки навчально-виховного процесу, в ході якого формуються навички ефективно мислити і діяти в навчальному середовищі, основні ознаки якого відповідають сучасному технологічному середовищу. Використання засобів інформаційних технологій повинне забезпечувати системність і спрямованість підготовки майбутніх військових фахівців на вирішення професійних завдань в умовах інформатизації військово-професійної діяльності.

Необхідно враховувати, що засоби інформаційних технологій, які використовуються в навчально-пізнавальній діяльності, повинні бути професійно-значущими засобами, а їхнє використання повинне забезпечувати здатність особистості: орієнтуватися в інформаційному просторі; уміння працювати з різними видами інформації; знаходити й відбирати необхідний матеріал, класифікувати його, узагальнювати, критично і відповідально до нього ставитися; на основі здобутих знань вирішувати будь-яку інформаційну проблему, пов’язану із професійною діяльністю. Отже, інформаційна компетентність є основним компонентом інформаційної культури, яка є частиною загальної культури людини; це інтегральна характеристика особистості, здатність засвоювати знання і виконувати завдання за

призначенням з допомогою інформаційно-комунікаційних технологій. Зміст військової освіти також має враховувати такі чинники та складові: національні інтереси, національну безпеку держави, соціокультурний характер, психологічні уявлення щодо характеру та структури військово-професійної діяльності, а військово-педагогічний процес базуватися на парадигмі особистісно-орієнтовного навчання та передбачати цілеспрямовану і змістовну взаємодію того, хто вчить і того, хто навчається.

Для реформування процесу навчання і переходу до нової системи військової освіти в Національній академії сухопутних військ імені гетьмана Петра Сагайдачного (НАСВ) зроблені рішучі кроки. Попри все шлях удосконалення освітнього процесу задля досягнення сумісності із стандартами НАТО обрано пріоритетним. Запроваджено вивчення курсантами процедур ухвалення рішень за натовськими стандартами у навчальній дисципліні «Основи військового управління, штабні процедури НАТО» і переведено навчання на систему використання тактичних знаків Альянсу за стандартом APP-6 та системою координат MGRS. У курсантів НАСВ є унікальна можливість практикуватися, як на етапі підготовки до міжнародних тренувальних місій, так і у процесі міжнародних навчань – таких, як Rapid Trident, де викладачі та курсанти діють у складі штабу бригади, штабах батальйонів і багатонаціональних підрозділів. Якісний і достатньо високий рівень підготовки наших учасників неодноразово відзначало керівництво і представники країн-членів НАТО. Досягненню операційної сумісності сприяє і залучення викладачів та курсантів НАСВ до навчання у військових вишах США, Канади й Великої Британії.

І на завершення: століття, в якому ми сьогодні живемо – це середовище домінування інформації і наукових знань. На сьогоднішній день Україна робить рішучі кроки до влиття в світовий інформаційний простір, вбачаючи одним з головних пріоритетів – інформатизацію освіти, як запоруку підготовки інтелектуального потенціалу нації – кадрів нового покоління з високим рівнем професійної компетентності, важливого стратегічного ресурсу для зміцнення обороноздатності держави, підвищення її авторитету та конкурентоспроможності на міжнародній арені та збереження національних інтересів.

УДК 004:001; 007

Кізло Л. М., Юрченко Р. В.

СУЧАСНІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ ГРОМАДСЬКОЇ БЕЗПЕКИ

Тенденцією останнього десятиліття є розвиток і поширене впровадження сучасних інформаційно-комунікаційних технології (ІТ) у систему функціонування інфраструктур великих місць. Це зумовлено, як загальносвітовими процесами урбанізації із зростанням кількості населення міст, так і наслідками перетворення міст на осередок сучасних інновацій із запровадженням ІТ в усі сфери міського життя, тобто створення “розумних міст”. В теперішніх умовах перенаселеності міст, коли під загрозою опиняється благо громадян, коли вони залежать від погіршення криміногенної ситуації, тотального екологічного забруднення, постійно існуючих заторів на дорогах чи відсутності місць для паркування автотранспорту, що призводить іноді до трагічних інцидентів, саме створення “розумних міст” виглядає найперспективнішим напрямом розвитку суспільства і забезпечення громадської безпеки їх мешканців.

Система “розумне місто” – це середовище, жити в якому цікаво, комфортно і безпечно. Для бізнесу – це територія з перспективами зростання і розвитку; для міської влади – простір, у межах якого будь-які рішення приймаються на основі даних про стан міських комунікацій та інфраструктури, отриманих від різноманітних електронних

пристроїв, всіляких датчиків, вимірювачів, камер спостереження – інтелектуальних інформаційних систем, які збирають, накопичують і передають інформацію.

Проте, надважливим завданням "розумного міста" є забезпечення громадської безпеки. Застосування камер відеоспостереження і фотофіксації, засобів відеоаналізу, засобів зв'язку та комп'ютерних інформаційних технологій надає можливість забезпечувати безпеку міському середовищу, комфортну для проживання. "Розумне місто" здатне самостійно простежити за належним рухом транспорту і пішоходів, за ситуацією в громадських місцях, за лікарнями і школами. Утім, з точки зору безпеки, "розумне місто" повинно навчиться самостійно стежити не тільки за цим, але й за електромережами, газо- і водопостачанням, безпекою у транспорті, станом тепломереж і водостоків та інше. Наразі міста стають "розумними" не тільки за рахунок того, що вони можуть автоматизувати рутинні функції для обслуговування конкретних людей, будівель та систем руху, а й тому, що вони здатні контролювати, розуміти, аналізувати та планувати дії для підвищення ефективності та якості життя для своїх громадян у режимі реального часу.

Натомість опоненти "розумного міста" висловлюють побоювання щодо можливості недотримання належного збереження і розповсюдження конфіденційних персональних даних, забезпечення процесу невтручання в особисте інформаційне поле. Вони стверджують, що іноді наявність датчиків і камер може сприйматися людиною, як вторгнення в її приватність, перетворення спостереження на державний нагляд і примусовий контроль.

Але "плюси" системи "розумне місто" очевидні: безпечне і комфортне життя для жителів міст – безвідмовно працює міська інфраструктура, максимально оперативний ремонт міських комунікацій у разі надзвичайних чи аварійних ситуацій; налагоджене житлово-комунальне господарство – автоматична передача показань лічильників і нарахування оплати за комунальні послуги; контроль ефективності роботи міських транспортних артерій – в мобільних додатках пасажири легко отримують інформацію про графік руху трамваїв, автобусів і тролейбусів. "Розумна" транспортна інфраструктура також може включати детектори контролю транспортного потоку, засоби автоматичної фіксації порушень ПДР, роботи адаптивних світлофорів, інформаційних табло систем автоматизованого управління освітленням, пристроїв, що допомагають уникати заторів на дорогах. Отже, переваги є і це зрозуміли і успішно використовують в мегаполісах Сінгапура, Амстердама, Чикаго та багатьох інших.

Оцінюючи успішність реалізації проектів «розумних міст» у світі, слід відзначити, що сьогодні Україна значно відстає, як за темпами впровадження інновацій, так і за їх якістю та комплексністю їх застосування. Фактично, в Україні ще жодне місто повністю не адаптовано до життя в режимі Smart. Окремі елементи "розумного міста" впроваджують у Києві. Львів має стати першим в Україні містом, де буде запроваджено «розумний» мікрорайон із застосуванням сучасних ІТ інновацій. Також зроблені перші кроки "цифровізації" всієї країни а саме: у кінці вересня 2019 року Міністерство цифрової трансформації України презентувала бренд "Держава в смартфоні". Продукт був створений за гроші зарубіжних донорів – швейцарсько-української програми EGAP, проекту USAID, проекту EGOV4UKRAINE, що фінансується ЄС та його країнами-членами: Данією, Естонією, Німеччиною, Польщею і Швецією.

Реалізовувати проект почали наприкінці 2018 року – створили електронний кабінет для малої забудови та розробили транспортний портал, який об'єднав електронні сервіси у всіх сферах транспортної галузі в одну "розумну" систему. З 2019 року, в тестовому режимі, запустили єМалятко у Харкові, Кривому Розі, Вінниці та Луцьку. Цей проект об'єднав 10 базових послуг, пов'язаних із народженням дитини, в одну систему. Поступово впроваджується цифрова трансформація на всіх рівнях влади: від міністерства до районної адміністрації. Доступність он-лайн послуг – це також і вміння ними скористатися, тому, на державному рівні, було запроваджено національну програму цифрової грамотності, яка за 3 роки має охопити 6 мільйонів українців. В межах цього проекту розроблено також додаток і сайт "ДіЯ", який запрацював в країні з 6 лютого

2020 року. “ДіЯ” – перша національна он-лайн-платформа, що допоможе українцям будь-якого віку освоїти базові цифрові навички, батькам – дізнатися про те, як захистити своїх дітей від небезпеки Інтернету, а вчителям – навчитися застосовувати он-лайн-інструменти, щоб зробити свої уроки більш ефективними та захопливими.

Чому “цифровізація” важлива для України? Це не тільки громадська безпека а, насамперед, ліквідація корупції та бюрократії, зручність державних сервісів для громадян, економія часу і коштів бюджету. Мета уряду – впровадити 100% державних послуг он-лайн до 2024 року і 50 основних послуг – вже у 2020 році. Завдяки “цифровізації” до 2024 року можна буде отримати будь-яку держпослугу, не виходячи з дому «... в тому числі – голосувати на президентських, парламентських чи місцевих виборах. Це наша мрія, і ми це зробимо. Це виклик амбітний, але досяжний!», – заявив В. Зеленський під час презентації проекту “ДіЯ”. Також президент з гордістю заявив, що Україна стала третьою країною в Європі, яка має подібний сервіс. Наступним напрямом – має стати покращення доступу громадян до екстрених служб реагування, це є пріоритетним завданням Кабінету Міністрів України. Саме система екстреної допомоги населенню за єдиним телефонним номером 112 згідно Концепції має стати основою для покращення доступу до екстрених служб і відповідного реагування як єдиний номер та сервіс оперативної допомоги. Швидкість реагування на надзвичайні ситуації повинна відповідати світовим стандартам щодо швидкості та комплексності надання таких послуг.

Отже, перехід з “аналогової” на “цифрову” державу надає Україні низку істотних переваг – країна стає більш конкурентоспроможною на світовій арені, у десятки разів збільшується як швидкість обміну даними між державними структурами, так і швидкість надання державних послуг населенню та бізнесу. Але попри все – “цифровізація” для України це шлях не лише до європейської інтеграції, але і до економічного добробуту, процвітанню, стабільності та безпеки в державі.

УДК 355.338:004

Троценко О. Я.

ВПРОВАДЖЕННЯ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМИ В РОБОТУ КАДРОВИХ ОРГАНІВ ЗБРОЙНИХ СИЛ УКРАЇНИ

Концепцією військової кадрової політики у ЗС України на період до 2020 року (Затверджена наказом Міністерства оборони України № 342 від 26.06.2017 р.) одним з основних завдань розвитку військової кадрової політики визначено – впровадження єдиної автоматизованої інформаційно-аналітичної системи обліку та управління персоналом до окремої військової частини та застосовування її у повсякденній діяльності служб персоналу.

На сьогоднішній день в ЗС України існує розгалужена система кадрового менеджменту ієрархічного рівня, що дає можливість здійснювати кадровий супровід всіх категорій особового складу відповідної номенклатури призначення.

Для оптимізації процесу виконання зазначених функцій у кадрових органах ЗС України використовуються наступні автоматизовані системи (далі – АС):

- інформаційно-аналітична система обліку особового складу ЗС України “Персонал” (ІАС “Персонал”);
- програмний комплекс “Автоматизація роботи районного (міського) комісаріату при проведенні призову громадян” “Призов” (ПК “Призов”);
- інформаційно-аналітична система планування мобілізаційного розгортання ЗС України “Ствол-М/1” (ІАС “Ствол-М/1”);
- АС “Оберіг” (Єдиний державний реєстр військовозобов’язаних).

Проте, жодна з існуючих у ЗС України АС нездатна повною мірою забезпечити виконання завдань, які покладені на кадрові органи.

Можливість використання наявних АС на різних рівнях органів управління ЗС України наведено у таблиці 1.

Таблиця 1

Використання АС на різних рівнях органів управління ЗС України

№ з/п	Назва АС	Рівні органів управління		
		верхній	середній	нижній
1	ІАС “Персонал”	+	+	+
2	ПК “Призов”			+
3	ІАС “Ствол-М/1”	+	+	
4	АС “Оберіг”	+	+	+

У кадрових органах ЗС України верхнього рівня, які здійснюють функції управління персоналом, а саме: Департаменті кадрової політки МО України, Головному управлінні персоналом ГШ ЗС України, Кадровому центрі ГШ ЗС України, та середнього рівня, а саме: управління персоналу та Кадрові центри видів ЗС України, впроваджується АС “Оберіг”, яка буде об’єднувати дані від систем, які вже працюють у ЗС або будуть створюватись. Зазначений програмний продукт має потужний механізм для аналітичного опрацювання всієї інформації, яка вноситься до загальних баз даних, та можливість відображати данні у зручній наочній формі. Крім того, АС “Оберіг” має низку переваг, а саме:

- є можливість створювати аналітичні звіти;
- до підсистеми закладено потужний пошуковий механізм за всіма типами даних, що внесені до баз даних;
- забезпечено цілісність та повноту накопиченої інформації;
- унеможливлено багаторазове введення даних та наявність розбіжностей в них;
- розширені можливості для створення і здійснення не тільки звітності, але й смарт-форм (бланків, що автоматично заповнюються на основі запитів);
- ведення документообігу.

У кадрових органах середнього рівня, які, у загальному вигляді, здійснюють функції обліку, а саме: управління персоналу та Кадрові центри видів ЗС; управління оперативних командувань, повітряного командування; та нижнього рівня, а саме: відділення персоналу бригад, окремих військових частин та підрозділів, відділення персоналу військових комісаріатів, впроваджена інформаційно-аналітична система (далі – ІАС) “Персонал”, яка була розроблена на замовлення МО України і є його власністю.

Для отримання початкової інформації ІАС “Персонал” у своїй роботі має взаємодіяти з ІАС “Ствол-М/1” та ПК “Призов”. Для підтримки цієї взаємодії у складі ІАС “Персонал” передбачено програмний комплекс ведення інформаційного обміну та окремі компоненти інформаційного обміну інших програмних комплексів, що забезпечують використання єдиного механізму обміну даними.

Інформацію стосовно призовників, допризовників та військовослужбовців військової служби за контрактом має надавати ПК “Призов”.

ІАС “Ствол-М/1” є джерелом інформації щодо організаційно-штатної структури військових підрозділів, мобілізаційних та призовних ресурсів. Крім того, від зазначеної ІАС до ІАС “Персонал” мають надходити класифікатори і словники. Також після звільнення військовослужбовця з військової служби у запас його послужна карта в електронному вигляді має передаватися до ІАС “Ствол- М/1”.

Але необхідно зосередити увагу на декількох проблемних аспектах.

Платформа SAP – це система звязку, яка працює в реальному часі, і для того, щоб її використовувати, канали зв’язку повинні забезпечувати передачу інформації в “on-line” режимі за вищим ступенем секретності. Нездатність телекомунікаційної системи ЗС

України забезпечити “закриті” канали зв’язку стало причиною того, що зазначена платформа не була впроваджена у діяльність ЗС України до цього часу. Проте, слід зауважити, що ця проблема стосується всіх АС, які працюють в “on-line” режимі.

Окремого розгляду потребує питання використання програмного забезпечення зі світового ринку програмного забезпечення.

Під час пошуку відповіді на це питання необхідно враховувати наступні аспекти:

- можливість попадання у залежність від закордонного постачальника на всіх етапах співробітництва, починаючи із закупівлі ліцензій і закінчуючи налагодженням постійного обслуговування;
- наявність таких програмних продуктів, які ми не в змозі розробити самі, або розроблення яких потребуватиме не підйомних витрат коштів;
- необхідність для України інтегруватись до європейської та євроатлантичної систем колективної безпеки та відповідно потреба у приведенні змісту оборонного планування до загальноприйнятих стандартів держав-членів НАТО.

Як показує проведений аналіз функціонування АС, що застосовуються у кадрових органах ЗС України, найбільш доцільною системою для інтеграції АС кадрових органів є підсистема “Особовий склад”. Вона найбільш повно забезпечує виконання функції кадрових органів і є складовою ЄАСУ АГП ЗС України.

Отже завершення створення єдиної автоматизованої інформаційно-аналітичної системи обліку та управління персоналом і запровадження сучасних АС в роботу кадрових органів дасть змогу, перш за все, вирішити завдання щодо укомплектування військових частин та підрозділів ЗС України професійно підготовленим особовим складом та оптимізувати процес збереження і зміцнення кадрового потенціалу.

УДК 355.371.64/.69

Троценко О. Я., Середенко М. М.

ЗАСТОСУВАННЯ НОВІТНІХ ЗАСОБІВ НАВЧАННЯ В ПРОЦЕСІ ВОГНЕВОЇ ПІДГОТОВКИ ВІЙСЬКОВОСЛУЖБОВЦІВ

Світовий досвід показує, що широке впровадження в практику підготовки військ сучасних засобів і технологій навчання значно підвищує професійний рівень військовослужбовців, покращує вишкіл, бойову готовність і боєздатність військових частин і підрозділів. Найбільш ефективним способом навчанням вважається комплексне впровадження технічних засобів навчання в поєднанні з іншими ефективними заходами (організаційними, методичними, науковими) шляхом їх концентрації у вищих військових навчальних закладах (далі – ВВНЗ), військових навчальних підрозділах закладів вищої освіти (далі – ВНП ЗВО), навчальних центрах (далі – НЦ).

Однією з основних складових індивідуальної підготовки військовослужбовців є вогнева підготовка. Події, які відбуваються на Сході України, різка зміна умов і обставин, в яких військовослужбовцям Збройних Сил (далі – ЗС) України доводиться застосовувати зброю, обумовлюють зміни і вимоги до змісту, форм і методів процесу їх навчання стрілецький справі (володінню стрілецькою зброєю, озброєнням бойових машин і застосування її в бойових умовах)

Діюча програма навчання курсантів з дисципліни «Вогнева підготовка» перестала відповідати специфічним вимогам, які висуваються до курсантів на сучасному етапі, традиційні засоби вогневої підготовки не можуть повною мірою вирішити завдання з оволодіння тими знаннями, вміннями і навичками, які можуть знадобитися військовослужбовцям в сучасних умовах ведення бою.

Сформовані стереотипи викладання вогневої підготовки долаються з труднощами. Нові інформаційні технології, комп'ютерна техніка, електронні тренажери в навчальний процес впроваджуються повільно. Внаслідок цього, процес вдосконалення вогневої підготовки для ВВНЗ (ВНП ЗВО), НЦ, які займаються підготовкою фахівців родів військ і служб, як ніколи, набуває актуального значення.

Досвіду провідних країн світу з цього питання свідчить, наприклад, вогнева підготовка в збройних силах США носить професійний і науково обґрунтований характер. Відповідні програма і методика проведення занять розробляються в НЦ навчання влучної стрільби сухопутних військ США USAMU (United States Army Marksmanship Unit). В процесі початкового навчання та навчання влучній стрільбі передбачається обов'язкове використання електронних та лазерних тренажерів. Такий тренажер, як EST 2000 (Engagement Skills Trainer) і лазерна система LMTS – призначені для тренувань зі стрільби і допомагають набувати і удосконалювати влучність стрільбі в різних умовах – сутінках, темряві, в закритих приміщеннях та проводити групову тактичну підготовку. В тренажерах EST 2000, для максимально реального відтворення віртуального виду бою, використовується цифрова система передачі відеоінформації, екран з високою роздільною здатністю, комп'ютерна графіка на ігровій основі та високоточне моделювання з застосуванням основ балістики.

Такого роду обладнання, яке достатньо поширене в зарубіжній практиці, поступово впроваджується до процесу навчання наших ВВНЗ (ВНП ЗВО), НЦ, але застосування новітніх технічних засобів вимагає і відповідного методологічного забезпечення для удосконалення процесу вогневої підготовки майбутніх офіцерів із застосуванням такої техніки.

Розроблені за останні кілька років технічні засоби навчання швидко впроваджуються у навчальний процес багатьох навчальних закладів, але разом з тим, вони вимагають відповідної навчально-методичної, інформаційної та практичної підготовленості викладачів. Тільки правильно застосована методика вогневої підготовки, яка підкріплена необхідними тренажерними засобами з високими технічними можливостями дозволить підготувати особовий склад ВВНЗ (ВНП ЗВО), НЦ до практичного застосування стрілецької зброї і озброєння бойових машин в різних умовах обстановки.

Сучасний тренажер, це складний багатофункціональний електронний пристрій, який використовується спільно з комп'ютером та дозволяє з достатньою точністю імітувати весь процес стрільби з озброєння бойових машин. Основним завданням тренажерів з використанням засобів імітаційного моделювання є досягнення якомога вищого рівня наближення умов тренування до реальних умов застосування озброєння бойової машини. Засоби імітаційного моделювання дозволяють створити на заняттях і навчаннях обстановку напруженості, раптовості, небезпеки і ризику, проте це не є самоціллю. Завдяки створенню віртуального простору, у який заглиблюється людина, набуваючи уявлення про картину сучасного бою, підвищуючи гостроту реакції, вона привчається активно діяти в умовах значних психічних навантажень і, тим самим, здобуває необхідний досвід долати труднощі та забезпечити себе від впливу негативних факторів, які супроводжують реальну бойову діяльність.

Але існуючі тренажери, поряд з багатьма перевагами, мають деякі недоліки, що властиві всім лазерним засобам та пристроями – не враховують вплив зовнішніх умов, таких як температура повітря, швидкість вітру, рух цілі на «політ кулі», а найголовніше – вони не враховують траєкторію польоту кулі в просторі.

Як показує досвід, всі початкові та підготовчі вправи під час проведення занять з вогневої підготовки необхідно виконувати спочатку на тренажерах (це скорочує час на проведення занять, заощаджує ресурси і виключає серйозні наслідки чи травмування, до яких може призвести порушення вимог заходів безпеки). Після виконання вправ на тренажерах доцільно проводити зайняття та тренування на бойовій техніці, виконуючи навчальні та контрольні стрільби. Таким чином, курсант, перш ніж виконати стрільбу з озброєння бойової машини, зобов'язаний відпрацювати свої дії на тренажері, набуваю-

чи вміння (повне засвоєння дій) і навички (виконання дії з високим рівнем майстерності, доведеним до автоматизму) в безпечних аудиторних умовах.

Використання сучасних навчальних технічних засобів та технологій в процесі бойової підготовки дозволяють отримати наступні результати: збільшення кількості навчених військовослужбовців; скорочення термінів навчання і підвищення якості підготовки військовослужбовців; досягнення високого рівня готовності військовослужбовців до виконання навчальних і бойових завдань.

При цьому забезпечується: максимальна об’єктивність контролю рівня підготовки військовослужбовців; комплексна підготовка військовослужбовців, екіпажів (розрахунків) з використанням сучасних комп'ютерних технологій в комплексі з застосуванням традиційних форм і методів навчання; ефективна підготовка військовослужбовців, підрозділів до бойових дій в складних умовах місцевості, в містах і населених пунктах; підвищення морально-психологічної стійкості особового складу в умовах обстановки, близької до реальної.

Таким чином, за рахунок гнучкого застосування оновлених форм і методів навчання з використанням сучасних інформаційних технологій в систему вогневої підготовки військовослужбовців можливо значно покращити ефективність ведення вогню зі стрілецької зброї та озброєння бойових машин.

УДК 355.37:004.85

Троценко О. Я., Кізло Л. М.

ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ МЕТОДІВ НАВЧАННЯ У ПІДГОТОВКУ ОФІЦЕРСЬКИХ КАДРІВ

На сьогоднішній день Україна робить рішучі кроки до входження в Світовий інформаційний простір, вбачаючи одним з головних пріоритетів – інформатизацію освіти, як запоруку майбутнього інтелектуального потенціалу нації.

Інформатизація освіти – це не тільки комп’ютеризація, це процес, який має свої закономірності, свої стадії розвитку, це зміна мислення, способів діяльності, засобів управління, використання можливостей телекомунікацій для міжособистісної та колективної взаємодії, компетентність і вільна орієнтація у сфері інформаційних технологій, гнучкість і адаптивність мислення, обізнаність і виконання основних правових норм регулювання інформаційних відносин та інформаційної культури.

Побудова ефективних систем інформатизації освіти з урахуванням світового досвіду, особливостей і реального стану вітчизняної освіти – це одна із актуальних і важливих наукових і практичних проблем. Думка відносно потреби сучасної освіти в інформатизації у науковців однозначна і сумнівів не викликає – і стосується вона як середньої, так і вищої освіти, як технічної, гуманітарної так і галузевої, в тому числі і військової, як на рівні міністерського управління галуззю, так і на рівні окремих навчальних закладів.

У час теперішніх військових перетворень, на тлі воєнного конфлікту, який все ще триває на Сході України, коли відбувається реформування Збройних Сил (далі – ЗС) України та у зв’язку з переходом на стандарти, які прийняті в збройних силах країн-членів НАТО система підготовки військовослужбовців (курсантів), в свою чергу, потребує прогресивних змін. Отже, з метою якісної підготовки майбутніх офіцерів в Національній академії сухопутних військ імені гетьмана Петра Сагайдачного (далі – НАСВ) проводиться робота щодо синхронізації системи підготовки в академії за стандартами НАТО, послідовне впровадження у процес навчання курсантів і слухачів Національної академії прогресивних інноваційних методів навчання.

Для підвищення якості підготовки офіцера військового управління тактичного рівня керівництвом, науковим, науково-викладацьким складом НАСВ, протягом 2019 навча-

льного року, активно здійснювалося впровадження у навчальний процес оновлених методів навчання з використанням проблемного, репродуктивного, евристичного, дослідницького методів, а також – із застосуванням елементів імітаційного моделювання та інтерактивного дистанційного навчання (35 викладачів НАСВ підвищили кваліфікацію за допомогою дистанційного навчання на базі Moodle).

Також проводяться заходи для посилення практичної компоненти процесу професійної підготовки курсантів, для чого заняття з курсантами-випускниками проводяться виключно інтенсивним, практичним методом. Крім того удосконалюється програма індивідуальної підготовки офіцерів, посилюються заходи для покращення професійної майстерності науково-педагогічних працівників, організовані курси мовної підготовки усіх категорій особового складу Національної академії.

До того ж, для оптимізації процесу навчання в НАСВ розроблена і затверджена «Концепція інформатизації академії». В її основу закладені вимоги для створення «єдиного інформаційного простору академії», складовою частиною якого можна вважати інформаційно-освітнє середовище – системно організовану сукупність компонентів інформаційного, технічного і навчально-методичного забезпечення, нерозривно пов'язаного з підготовкою майбутнього офіцера, як суб'єкта освітнього простору, компонентами якого є:

- інформаційно-організаційний (державний професійний стандарт, навчальні програми, навчальні плани, графіки навчального процесу);
- програмно-апаратний (сукупність засобів автоматизації навчального процесу (ПК, проектори і тому подібне).

Разом з тим, поряд з позитивними результатами впровадження інноваційних засобів навчання у навчальний процес курсантів НАСВ, існують і недоліки:

- обмеженість доступу курсантів до локальної мережі;
- недостатній рівень «інформатизації» викладачів, їх спроможність розробляти і застосовувати сучасні інформаційні технології в навчанні;
- слабкі навички викладачів у роботі з інформаційно-комунікаційними системами;
- складності розробки програм дистанційних курсів;
- відсутність можливостей контролювати рівень засвоєння знань курсантів в результаті самостійного вивчення навчального матеріалу.

Проте, галузь військової освіти в цілому і окремі освітні процеси сьогодні гостро потребують інформатизації, тому що:

- насичення інформаційними технологіями навчально-виховного процесу підвищує його ефективність і привабливість для тих, хто навчається, це ж саме стосується і застосування інформаційних технологій в управлінні навчальним закладом;
- курсанти, які поповнять майбутнє покоління захисників нашої нації, мають крокувати в ногу з часом і вміти використовувати інформаційні технології на своєму робочому місці;
- наша система військової освіти має випускати кваліфікованих обізнаних в сучасних питаннях інформатизації фахівців, які будуть конкурентноздатними на європейському і міжнародному ринках праці, що підвищуватиме престиж України у світі;
- інформатизація освітньої галузі гармонізує її з іншими сферами суспільної життєдіяльності, які раніше розпочали активну комп'ютеризацію і використання програмного забезпечення для підготовки кадрів, здатних успішно виконувати свої функції за призначенням.

Згідно Концепції Національної програми інформатизації інновації в освіти спрямовуються на формування та розвиток інтелектуального потенціалу нації, удосконалення форм і змісту навчального процесу, впровадження комп'ютерних методів навчання та тестування, що поширює можливості для вирішення проблем освіти на вищому рівні, з урахуванням світових вимог.

Запорукою підвищення якості освіти та забезпечення конкурентоспроможності випускників вищих навчальних закладів на ринку праці є безперервне оновлення змісту освіти на основі новітніх досягнень культури, науки, техніки, зокрема застосування інноваційних методів при використанні інформаційних технологій у навчальному проце-

сі. Аналіз розвитку передових у економічному відношенні країн показує, що однією з основних умов, яка визначає прогресивний розвиток економіки, науки і культури в державі є інформатизація системи вищої освіти. Знання і навички, якими сьогодні оволодівають майбутні фахівці, у подальшому визначатимуть шляхи розвитку суспільства. Саме у вищих навчальних закладах зосереджена найбільша кількість прогресивних та відкритих до науково-технічних інновацій людей, що суттєво полегшує впровадження інформаційних технологій у навчальний процес.

Отже, новітні технології навчання, які впроваджені у навчальний процес НАСВ, дають можливість підвищити ефективність навчання та забезпечити підготовку курсантів за стандартами ЗС країн-членів НАТО.

Черноног О. О., Івко С. О., Москаленко А. О.

АНАЛІЗ ПІДХОДІВ ДО СУЧАСНОЇ МОДЕЛІ КІБЕРОБОРОНИ

Глобальний розвиток інфокомунікаційних технологій та засобів масової комунікації дав початок появі нових технологій впливу на вирішення міждержавних конфліктів. Розвиток інформаційного суспільства дозволяє використовувати для вирішення політичних, економічних, соціокультурних завдань можливості прихованого впливу на підсвідомість людей та масштабного маніпулювання суспільною думкою населення інших країн. Це, у свою чергу, призвело до появи нових форм і методів досягнення зовнішньополітичних цілей без застосування воєнної сили.

Розгляд питання інфокомунікаційних технологій впливу на людську діяльність потребує проведення аналізу основних складових таких як інформаційна війна та кібервійна. Це в свою чергу надає можливість розкрити методи, які використовує держава-агресор, виявити недоліки сучасної інформаційної політики України та запропонувати підходи до обґрунтування не розкритих в діючій нормативно-правовій базі засад державної політики по забезпеченню інформаційної безпеки та кібербезпеки у воєнній сфері.

Метою роботи є обґрунтування шляхів удосконалення кібербезпеки у воєнній сфері в умовах інфокомунікаційного впливу. Удосконалення державної політики кібербезпеки у воєнній сфері пропонується здійснити шляхом поступового розгляду факторів, які безпосередньо впливають на стан кібербезпеки в умовах інфокомунікаційного впливу:

- поширення практики проведення воєнних і спеціальних кібернетичних операцій та дій провокаційного характеру для створення конфліктних ситуацій у кіберпросторі;
- інтенсивна модернізація збройних сил сусідніх держав, активізація розробок кіберозброєння та військових засобів програмно-математичного впливу з принципово новими можливостями як фізичного ураження так і дистанційного управління;
- активне нав’язування в інформаційному просторі необхідної суспільної думки, що до зовнішньої політики Російської Федерації, направленої на дестабілізацію внутрішньополітичної ситуації щодо сусідніх держав, а також міжнародних організацій, включаючи ООН, ЄС та НАТО;
- модернізація та вдосконалення спеціальними службами іноземних держав систем і комплексів кібернетичної розвідки, нарощування їх можливостей, спроби несанкціонованого кібернетичного доступу до об’єктів критичної інфраструктури України, реалізація кібератак, впровадження програмних закладних пристроїв та розповсюдження спеціально створеного шкідливого програмного забезпечення;
- кібервійна Російської Федерації проти України.

Враховуючи зазначені фактори, що можуть призвести до виникнення надзвичайних ситуацій та катастроф, а також певну ймовірність застосування з боку більш розвиненого противника кібернетичної зброї, силам безпеки і оборони необхідно готуватись до дій в умовах масованого впливу кібернетичних атак та ударів на об’єкти як цивільної

так і військової інфокомунікаційної інфраструктури. Потенційним воєнним противником в кіберпросторі Україна визнаватиме державу (коаліцію держав), дії або наміри якої (яких) матимуть ознаки загрози застосування в кіберпросторі воєнної сили проти України. Основним завданням кібероборони є підтримка виконання військовими формуваннями поставлених завдань. Основою сил кібероборони є підрозділи Збройних Сил України, інших утворених відповідно до законів України військових формувань, а також правоохоронних органів спеціального призначення.

Рижов Є. В., Сакович Л. М., Пащетник О. Д.

ФОРМУВАННЯ ВИМОГ ДО ЗАСОБІВ ВИМІРЮВАНЬ ДІАГНОСТИЧНИХ ПАРАМЕТРІВ АПАРАТНОЇ ЗВ'ЯЗКУ ПІД ЧАС ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ТА ПОТОЧНОГО РЕМОНТУ

Апаратні польових вузлів зв'язку складаються з тисяч елементів і відносяться до об'єктів великої розмірності, технічне обслуговування і поточний ремонт яких виконується екіпажами із залученням фахівців ремонтних органів з апаратних технічного забезпечення. У цих випадках визначення технічного стану об'єктів здійснюється групою фахівців за умовними алгоритмами. При технічному обслуговуванні за станом, що пропонується керівними документами [1], в заданій послідовності перевіряється значення діагностичних параметрів і при їх відхиленні від норми виконується пошук дефектів з подальшим усуненням несправності. При цьому реалізуються різні види групового пошуку дефектів (ГПД) за умовними алгоритмами [2-6].

У відомих роботах вирішуються завдання підвищення ефективності діяльності екіпажів в процесі встановлення реального технічного стану апаратних зв'язку.

Метою цієї доповіді є формування вимог до засобів вимірювань зі складу апаратних зв'язку та апаратних технічного забезпечення за критерієм мінімуму їх вартості при обмеженнях на час визначення технічного стану.

Відомо, що вартість засобів вимірювань визначається класом точності аналогових або числом розрядів цифрових приладів, які в свою чергу, залежать від мінімального значення ймовірності правильної оцінки результату виконання перевірки [7, 8].

У практиці технічного обслуговування і поточного ремонту апаратних зв'язку знаходять застосування всі види ГПД [2-6]:

- незалежний ГПД – при технічному обслуговуванні апаратних зв'язку та поточному ремонті різних типів технічних об'єктів в універсальних апаратних технічного забезпечення;
- спільний (ГПД) – при поточному ремонті об'єктів великої розмірності з просторово рознесеними елементами;
- зонний (ГПД) – при ремонті однотипних об'єктів модульної конструкції в спеціалізованих апаратних технічного забезпечення.

Припущення при вирішенні завдань відповідають умовам функціонування військових ремонтних органів:

- розглядається найгірший варіант з точки зору діагностики, випадок рівномірного розподілу дефектів в об'єкті;
- при діагностуванні нових дефектів в об'єкті не виникає;
- організаційні витрати часу не враховуються;
- кваліфікація фахівців відповідає посаді;
- при оцінці стану об'єкта допускається можливість не більше однієї помилки в оцінці результату виконання перевірки.

Принципова відмінність зонного ГПД і спільного ГПД полягає в тому, що в першому випадку помилка шукача збільшує трудовитрати тільки для нього і не впливає на якість роботи інших, а в другому випадку помилка одного впливає на результат роботи

всіх і збільшує загальні трудовитрати. Крім того, спільний ГПД не залежить від розподілу засобів спеціального зв'язку на конструктивні одиниці.

Незалежні ГПД використовують, наприклад, при технічному обслуговуванні радіостанцій середньої потужності (Р-140, Р-161 та інших), коли фахівці незалежно один від одного перевіряють параметри радіоприймача, збудника, електроживлення та інших підсистем апаратної зв'язку. У цих випадках кожен фахівець працює на певній ділянці зі своїми засобами вимірювання, перевіряючи параметри за бінарним або однорідним умовним алгоритмом.

Таким чином, у доповіді розглянуто можливі види взаємодії групи фахівців при технічному обслуговуванні і поточному ремонті апаратних зв'язку. Отримані результати доцільно використовувати при обґрунтуванні метрологічних характеристик засобів вимірювальної техніки для комплектування апаратних зв'язку та технічного забезпечення.

Список використаних джерел

1. Керівництво з технічного забезпечення зв’язку та автоматизації управління військами Збройних Сил України / В. М. Дзюба, Є. Д. Ковальчук, В. А. Рижаков, Л. М. Сакович і інші. – К.: Воєнне видавництво, 2003. – 259 с.

2. Ксёнз С. П. Диагностика и ремонтопригодность радиоэлектронных средств. – М.: Радио и связь, 1989. – 248 с.

3. Рыжаков В. А. Групповой зонный поиск кратных дефектов при ремонте техники связи / В. А. Рыжаков, Л. Н. Сакович // Зв'язок. – 2005. – №1. – С.57-60.

4. Сакович Л. Н. Совместный групповой поиск кратных дефектов при ремонте техники связи / Л. Н. Сакович, В. А. Рыжаков // Зв'язок. – 2005. – №2. – С.59-62.

5. Рижов Є. В. Дослідження показників якості групового пошуку дефектів під час поточного ремонту військової техніки зв'язку / Є. В. Рижов, Л. М. Сакович // Збірник наукових праць Військової академії (м. Одеса). – 2017. – № 2(8). – С. 82-88.

6. Сакович Л. Н. Определение численности специалистов при восстановлении работоспособности техники связи с аварийными повреждениями / Л. Н. Сакович, Р. А. Бобро // Зв'язок. – 2006. – №1. – С.41-44.

7. Яковлев М. Ю. Комплексна методика проведення метрологічної експертизи військової техніки зв’язку / М. Ю. Яковлев, П. Л. Аркушенко, Є. В. Рижов // Вимірювальна техніка та метрологія. – 2018. – Вип. 79 (3). – С. 55-63. doi: https://doi.org/10.23939/istcmtm2018.03.055.

8. Яковлев М. Ю. Підхід до вибору засобів вимірювальної техніки військового призначення для метрологічного обслуговування військової техніки зв’язку / М. Ю. Яковлев, Є. В. Рижов // Військово-технічних збірник Академії СВ. – 2014. – № 1 (10). – С. 115-121. doi: https://doi.org/10.33577/2312-4458.10.2014.115-121.

Пащетник О. Д., Живчук В. Л.

РЕЗУЛЬТАТИ РОЗРОБОК ЩОДО ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ЧАСТИНАХ (ПІДРОЗДІЛАХ) СУХОПУТНИХ ВІЙСЬК ЗА СТАНДАРТАМИ НАТО

Досвід ведення бойових дій на сході України показує нагальну потребу в автоматизації процесів управління в діяльності командирів всіх ланок Збройних Сил. У зв'язку із вимогами Державної програми розвитку Збройних Сил України на період до 2020 року (стратегічна ціль №1 – розвиток системи управління Збройних Сил України на основі прийнятих у державах-членах НАТО принципів і стандартів), а також Стратегічного оборонного бюлетеня України, схваленого Указом Президента України від 6 червня 2016 року № 240/2016 (додаток 1 бюлетеня), щодо переходу системи управління

Збройних Сил на стандарти НАТО, стає актуальним питання розробки програмно-математичного та інформаційного забезпечення документообігу автоматизованих систем управління тактичної ланки Сухопутних військ. Для формування вимог до такого програмно-математичного забезпечення проведено аналіз керівних документів (стандартів) країн-членів НАТО, які визначають обмін інформацією (документами) між частинами (підрозділами) військ НАТО. Основними нормативними документами цього напрямку є наступні: STANAG 2199 COMMAND AND CONTROL OF ALLIED LAND FORCES; STANAG 7149 NATO MESSAGE CATALOGUE - APP-11; FM 6-99 US ARMY REPORT AND MESSAGE FORMATS.

В рамках наукового супроводження створення автоматизованої системи управління тактичної ланки Сухопутних військ Науковим центром Сухопутних військ проводяться дослідження щодо формування каталогу формалізованих документів частин (підрозділів) Сухопутних військ, адаптованих до стандартів НАТО. Крім розробок самих формалізованих документів, проводиться визначення, на яких етапах роботи командирів ці документи розробляються. Це дає можливість їх інтеграції в єдину систему підтримки прийняття рішень (СППР), як функціональну складову автоматизованої системи управління Сухопутних військ. Основою для формування такої СППР є формалізація алгоритмів (порядку) роботи командирів, а саме процесу прийняття воєнних рішень MDMP (military decision-making process), для якого програмно формується ієрархічна структура. Верхнім рівнем в цю структуру входять відомі сім етапів (кроків) MDMP (перший рівень ієрархії), з відповідними підетапами (другий рівень ієрархії), задачами, які виконуються на цих підетапах (третій рівень ієрархії), і діями командирів (четвертий рівень ієрархії). Серед етапів MDMP верхній рівень ієрархії алгоритмів роботи складають наступні: отримання завдання, аналіз завдання, розробка ймовірних варіантів дій, аналіз ймовірних варіантів дій, порівняння ймовірних варіантів дій, обрання варіанту дій, опрацювання планів та наказів.

Зазначена ієрархічна структура, яка детально визначає алгоритми роботи командирів при прийнятті рішень на ведення бойових дій, доповнюється додатковим функціоналом, а саме: електронними формами бойових документів, інформаційними та інформаційно-розрахунковими задачами, довідниковими даними, що використовуються на відповідних етапах роботи, підказками щодо порядку відпрацювання окремих задач командирів (на базі вимог та рекомендацій відповідних розділів стандартів НАТО).

Серед бойових документів, адаптованих до стандартів НАТО, найбільшу актуальність для впровадження мають: OPLAN – оперативний план або OPORD – наказ; WARNO – попереднє бойове розпорядження; FRAGO – уточнюючий наказ.

Лаврут О. О., Лаврут Т. В., Богуцький С. М.

НАВЧАЛЬНО-МАТЕРІАЛЬНА БАЗА ЯК СКЛАДОВА ПРОЦЕСУ УСПІШНОЇ ПІДГОТОВКИ КАДРІВ

Як зазначено у «Візії Генерального штабу ЗС України щодо розвитку Збройних Сил України на найближчі 10 років»: місія ЗС України – оборона України, захист її суверенітету, територіальної цілісності та недоторканості. Основою цього може стати лише професійна, висококваліфікована армія. Одним з основних пріоритетів розвитку Збройних Сил України є «високий рівень професійної підготовки особового складу».

Якісно, відповідно до вимог сьогодення і стандартів НАТО, підготувати еліту Українського війська можна лише швидко змінивши підходи та бачення викладання дисциплін. Одним із найважливіших аспектів цього процесу є удосконалення навчально-матеріальної бази кафедр. Сьогодні система зв'язку й автоматизації Збройних Сил України переведена на цифрові засоби, що дозволило забезпечувати виконання першо-

чергових завдань з управління військами. Враховуючи це, викладачам кафедри довелося швидко модернізувати навчально-матеріальну базу кафедри та вести пошук нових інноваційних рішень у підходах і методиці викладання дисципліни.

На кафедрі тактики створено інноваційний навчально-тренувальний комплекс «Експлуатація сучасних цифрових засобів зв'язку». Комплекс розміщено у двох класах і об'єднано в єдину мережу, що дозволяє під час вивчення дисципліни використовувати його для моделювання процесу обміну інформацією між посадовими особами старшого штабу та підпорядкованих і приданих підрозділів.

Для цього в одному класі обладнано наступні робочі місця:

- командно-спостережний пункт роти (КСП), який включає: автоматизовані робочі місця (АРМ) посадових осіб; ретранслятор Либідь К-2РТД; станцію супутникового зв'язку Tooway; автомобільну радіостанцію DM4600; телекомунікаційний комплект (ТК-1) та DSL модем, які дозволяють об'єднати в єдину мережу автоматизовані робочі місця посадових осіб роти та мережу старшого штабу;
- робочі місця, згідно штату роти, а саме: робочі місця командирів взводів, відділень та командирів приданих підрозділів (мінометної батареї); робочі місця командирів бойових машин (БТР, БМП, танка); робочі місця спостережних постів та вогневих позицій; окрема радіомережа розвідки.

Командний пункт управління старшого штабу розміщено в іншому класі. Його склад:

- АРМ старшого командира; АРМ начальника штабу; ретранслятор Либідь К-2РТД; станція супутникового зв'язку Tooway; телекомунікаційний комплект (ТК-1) та DSL модем, які дозволяють об'єднати в єдину мережу автоматизовані робочі місця посадових осіб керівного складу вищого штабу та підпорядкованих підрозділів, а також цифрові портативні та переносні радіостанції;
- приданий старшому штабу танковий підрозділ у вигляді стендового демонстраційно-навчального комплексу «Цифрова система зв'язку Aselsan 6680-IP».

Інноваційний навчально-тренувальний комплекс дозволяє формувати у курсантів знання, уміння та навички, за допомогою яких вони будуть спроможні виконувати службово-бойові функції та завдання щодо управління підпорядкованими і приданими підрозділами та вогнем під час виконання покладених завдань у різних видах бою, використовувати штатні засоби зв'язку, що перебувають на озброєнні в підрозділах Сухопутних військ ЗС України.

Лаврут О. О., Федін О. В., Вірко Є. В.

ІНТЕГРАЦІЯ КОМАНДНО-ШТАБНИХ МАШИН В ЄДИНУ АВТОМАТИЗОВАНУ СИСТЕМУ УПРАВЛІННЯ ПІДРОЗДІЛАМИ СУХОПУТНИХ ВІЙСЬК ЗБРОЙНИХ СИЛ УКРАЇНИ

Командно-штабна машина (КШМ) є однією з підсистем системи управління Сухопутних військ (СВ) Збройних Сил (ЗС) України, яку слід інтегрувати у перспективну Єдину автоматизовану систему управління (ЄАСУ) ЗС України. Пріоритетність розвитку цього напряму підтверджується «Візією Генерального штабу ЗС України щодо розвитку Збройних Сил України на найближчі 10 років» та основними положеннями «Стратегічного оборонного бюлетеню України», в якому зазначено, що створення ефективної системи оперативного управління, зв'язку, розвідки та спостереження (C4ISR), яка б відповідала стандартам НАТО є першочерговою задачею.

Сумісність засобів зв'язку та автоматизації КШМ при взаємодії із іншими АСУ має забезпечуватися дотриманням декількох основних вимог:

- технічна сумісність засобів зв'язку та автоматизації КШМ повинна забезпечуватись єдністю протоколів обміну фізичного, канального, мережного, транспортного та

інших рівнів (якщо обрана модель мережної взаємодії передбачає наявність таких рівнів), пов'язаних безпосередньо із роботою технічних засобів;

- програмна сумісність засобів зв'язку та автоматизації КШМ має забезпечуватись вибором єдиної операційної системи та уніфікації загального програмного забезпечення;
- інформаційна сумісність засобів зв'язку та автоматизації КШМ мусить забезпечуватись єдністю протоколів обміну, які використовуються програмним забезпеченням, єдиним способом організації інформаційного забезпечення, в тому числі єдністю схем баз даних, форм бойових документів, а також вибором єдиної платформи геоінформаційної підсистеми. Для забезпечення інформаційної сумісності засобів зв'язку та автоматизації КШМ має відповідати вимогам системи стандартів НАТО і програми забезпечення сумісності MULTILATERAL INTEROPERABILITY PROGRAMME;
- організаційна сумісність засобів зв'язку та автоматизації КШМ повинна забезпечуватись єдністю вимог керівних документів, що регламентують роботу всіх її складових елементів і взаємодію з іншими АСУ, та забезпечують узгодженість дій посадових осіб, які задіяні в роботі з АСУ;
- метрологічна сумісність засобів зв'язку та автоматизації КШМ.

В цьому напрямі командування ЗС України проводиться планомірна робота. Так у кінці 2019 року на озброєння Збройних Сил України прийнята КШМ К-1450-01. Однак, постачання зазначеного зразка у частини та підрозділи Сухопутних військ масово ще не розпочато. Дана КШМ оснащена сучасними засобами зв'язку та телекомунікацій, які використовуються країнами-членами НАТО: радіо, проводовими, супутниковими, транкінговими тощо.

Таким чином, використання новітніх розробок, сучасних технологій, засобів зв'язку та телекомунікацій в нових КШМ дасть змогу забезпечити вимоги щодо інтеграції їх в ЄАСУ.

Олійник С. Е., Опалинський В. Б.

КІБЕРБЕЗПЕКА

Протягом останніх років все ширше використання перспективних ІТ-технологій зумовило не лише численні переваги, а й цілу низку проблем. Зокрема, істотно підвищився рівень інформаційного негативного впливу на процеси збереження та розповсюдження інформації, зросла чисельність нових загроз інформаційній безпеці, таких як нові форми кібератак. При цьому в комп'ютерних системах зберігаються і обробляються великі обсяги облікової інформації, будь-який збій може привести до надмірних витрат, недостатніх доходів, втрати активів, санкцій тощо. Тому головним пріоритетом захисту облікової інформації є розроблення заходів, спрямованих на збереження інформації, що міститься у комп'ютерних базах. Виділяють такі дві категорії загроз комп'ютерним інформаційним системам, як активні і пасивні. Активні загрози включають комп'ютерне шахрайство та комп'ютерний саботаж. Пасивні загрози – це помилки системи (пошкодження окремих компонентів обладнання або програмного забезпечення). Досліди вказують, що 45% причин загроз становлять навмисні дії.

У зв'язку з тим, що останнім часом збільшується кількість незаконних фінансових операцій, крадіжок та шахрайства в мережі Інтернет, несанкціонованого використання чи модифікації програмного забезпечення, під час оцінки надійності систем інформаційної безпеки мають бути змінені пріоритети від забезпечення традиційної інформаційної безпеки до кібербезпеки. Питання кібербезпеки зачіпає інтереси не лише державних інституцій, а і приватного сектору та громадянського суспільства. Під захистом облікової інформації розуміється стан її захищеності від випадкових або навмисних впливів природного або штучного характеру, що можуть привести до нанесення шкоди власникам або користувачам цієї інформації. Якщо розглядати це поняття без конкре-

тики, то можна говорити про інформаційну безпеку загалом. Однак коли захист інформації стосується забезпечення безпеки інформаційних баз даних, а також різних програм, що входять у комп'ютерні мережі, виникає необхідність визначити співвідношення між інформаційною безпекою та кібербезпекою. Науковий погляд на сутність кібербезпеки означає наступальні дії, тобто кібербезпека відрізняється від традиційної інформаційної безпеки тим, що вона включає застосування практичних дій і засобів для атаки супротивників. Під час розмежуванняпонять «кібербезпека» та «інформаційна безпека» загрози кібербезпеці визначаються в уразливості об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, а також у фізичній і моральній застарілості системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

На відміну від інформаційної безпеки мова йде не про інформацію взагалі, а про ту інформацію, яка циркулює в кіберпросторі і становить важливу частину її змісту. Зрозуміло, що втрата інформації, яка зберігається в окремому комп'ютері і є важливою для користувача цього комп'ютера, не може розглядатися як загроза кібербезпеці. Однак захист інформації потрібно передбачувати, виходячи із цінності інформації не для себе, а для зловмисників, які будують відносини винятково на грошовій основі. Привабливою може бути інформація управлінського обліку, яка містить комерційну таємницю. Кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача. Відповідно кібербезпека – це деякий стан системи, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах.

Проблему кіберзлочинності загострює відставання нормативного регулювання цієї сфери в Україні від розвитку нових інформаційних технологій. У національній стратегії кібербезпеки України розкривається поняття забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів. На жаль, кіберзлочинність постійно вдосконалюється і йде в ногу з технологіями. Це ускладнює виявлення та протидію зазначеним протиправним діям. Тому варто усвідомити, що проблема кібербезпеки – це проблема не лише загально-державного рівня, а кожного окремо взятого користувача.

Більшість засобів захисту реалізуються у вигляді програм або пакетів програм, що розширюють можливості стандартних операційних систем, а також систем керування базами даних. Основним способом попередження кіберзагроз є впровадження послідовних рівнів заходів контролю за доступом до сайту, системи та файлів, що дає власникам можливості розмежування доступу до функцій та файлів, до окремих ділянок обліку, встановлення паролів користувачів. Крім застосування засобів захисту, що вбудовуються у програмне забезпечення, повинна бути передбачена низка адміністративних заходів, наприклад, стеження за відсутністю підслуховуючих пристроїв у комп'ютерних мережах тощо. При цьому важливими складниками захисту є компетентність та суворе виконання зобов'язань щодо гарантій дотримання необхідних правил безпеки персоналу, від коректності дій якого залежить рівень кібербезпеки.

До некомпетентних дій персоналу, які є загрозою втрати інформації, відносяться: встановлення неліцензійного програмного забезпечення; роботу з конфіденційними документами у місцях публічного доступу; відкриття на своєму комп'ютері файлів, надісланих електронною поштою або програмами миттєвого обміну повідомленнями від невідомих адресатів; використання паролів «за замовчуванням», створення простих паролів або небажання змінювати паролі протягом тривалого часу, «запам'ятовування» пароля у вікнах уведення, особливо на комп'ютерах для публічного доступу; повідом-

лення по телефону будь-яких даних про обліковий запис, логіни, паролі; нецільове використання мережевих ресурсів.

Очевидно, що об'єктом зацікавленості злочинців була і завжди буде приватна інформація, витоки якої здійснюють під час використання соціальних мереж через такі канали, як персональні комп'ютери, ноутбуки, смартфони, а тому користувачавам необхідно прописувати правила користування цією інформацією і стежити за безумовним їх виконанням. Зрозуміло, що неможливо досягти стовідсоткової безпеки захисту облікових даних. Проте індивідуальна відповідальність кожного користувача є найпершим і найпростішим фактором, який сприяє захисту цінної облікової інформації. Таким чином, повинна бути створена програма визначених дій, спрямованих на створення кіберзахисту облікової інформації, сфера застосування якого поширюється на людські ресурси і не обмежується винятково технологічними аспектами.

Загалом управління кібербезпекою повинно передбачати створення або спеціальної служби із забезпечення кібербезпеки облікової інформації, або введення посади спеціаліста з кібербезпеки, Ці функції також можуть бути покладені на системних адміністраторів, адміністраторів комп'ютерних мереж, менеджерів систем з інформаційної безпеки, аналітиків систем забезпечення кібербезпеки.

Таким чином, серед можливих шляхів підвищення ефективності заходів кібернетичного захисту можуть бути: налагодження ефективної системи кіберзахисту об'єктів з урахуванням їх категорій за ступенем уразливості; підвищення ефективності інформаційно-аналітичної роботи суб'єктів інформаційної безпеки; створення та постійне оновлення бази даних порушників і порушень, у тому числі кіберзлочинців; створення системи раннього виявлення інформаційних небезпек. Крім того, необхідно створити умови для дотримання режиму експертного контролю та нерозповсюдження несертифікованих програмно-апаратних засобів і систем, комп'ютерної техніки, оперативного реагування на інциденти, які пов'зані з виведенням із ладу інформаційно-технологічних систем, а також налагодження каналів формального та неформального обміну інформацією стосовно загроз комп'ютерної злочинності та кібертероризму.

Опалинський В. Б., Олійник С. Е.

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ

Сучасні зміни та перетворення, які відбуваються в Україні, поступово торкаються усіх сфер життєдіяльності суспільства: економічної, політичної, соціальної, духовної та інших. Особливої уваги заслуговує соціальна сфера, адже механізми реалізації соціальної політики і рівень соціального захисту населення нашої країни потребують змін. Мова йде про встановлення взаємодії і взаємної відповідальності між людиною та державними інститутами, зокрема, органами правопорядку.

Особливої актуальності проблеми формування ефективної комунікації між поліцією та населенням набули у зв'язку з останніми подіями, які відбулись в Україні під час Революції гідності. Інформаційне забезпечення правоохоронної діяльності відкриває нові можливості для попередження злочинності та сприяють ефективному і точному прийняттю рішень з метою розкриття злочинів.

Важливим аспектом цього питання є часткова втрата професійного складу правоохоронних органів у ході проведення реформування правоохоронної сфери. Так, після подій Євромайдану та Революції Гідності суспільство було охоплене негативним ставленням до правоохоронної системи загалом, що зумовило звільнення більшості досвідчених, висококваліфікованих працівників, а стаж роботи працюючих нині кадрів є неприпустимо низький. Така ситуація, безумовно, чинить негативний вплив на стан про-

тидії злочинності в умовах погіршення кримінологічної обстановки в нашій державі, оскільки відбулася втрата вагомої частини негласних джерел інформації, які забрали з собою звільнені працівники.

Для належної реалізації правоохоронними органами своїх функцій необхідно:

- вдосконалювати нормативно-правову базу інформаційного забезпечення правоохоронних органів і інформаційного забезпечення в цілому;
- створити єдину базу даних, яка б містила усю необхідну інформацію;
- застосовувати новітні засоби обробки інформації в оперативно-розшуковій та довідковій роботі;
- готувати працівників, які повинні достатньо володіти знаннями, вміннями та навичками застосування інформаційних технологій;
- постійно підвищувати кваліфікацію працівників інформаційних підрозділів та інших служб із загальної інформаційної культури, комп'ютерної підготовки, а також інформаційної безпеки;
- підвищувати рівень забезпечення всіх галузевих підрозділів сучасною потужною комп'ютерною технікою, ліцензійним стандартним та прикладним програмним забезпеченням;
- створити комплексну дієву систему інформаційної безпеки правоохоронних органів, в межах якої повинні бути визначені загальні положення, цілі, принципи та напрями запровадження, а також підтримка надійної системи інформаційної безпеки правоохоронних органів України.

Виконання вище зазначених заходів наддасть можливість привести у відповідність інформаційно-аналітичні системи правоохоронних органів, забезпечити єдність системи інформаційного законодавства та здійснювати фінансову підтримку правоохоронних органів з метою забезпечення високотехнологічного озброєння, створити спеціальні курси для працівників правоохоронних органів, з метою підвищення кадрового потенціалу.

Пащетник О. Д., Живчук В. Л., Поліщук Л. І.

ОБҐРУНТУВАННЯ СКЛАДУ ТА СТРУКТУРИ МЕРЕЖЕЦЕНТРИЧНОЇ ОНТОЛОГІЧНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ КОМАНДИРІВ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ

Система підтримки прийняття рішення (СППР) призначена для інформаційної та інтелектуальної підтримки командирів частин (підрозділів) за рахунок ефективної передачі, обробки, відображення та зберігання необхідної інформації засобами інформаційного та програмно-математичного забезпечення.

Впорядкування та ефективне використання необхідної інформації для підготовки і ведення бойових дій командирами тактичної ланки управління можливе за умов побудови онтології предметної області впорядкованих та структурованих знань, формально представлених на базі певної концептуалізації. Онтологія для СППР автоматизованої системи управління військами (АСУВ) будується на основі знань, формалізованих у бойових статутах і інших керівних документах із врахуванням стандартів НАТО (MDMP – The Military Decision-Making Process), а також програмної реалізації моделей, методів та алгоритмів функціонування окремих модулів СППР. Впровадження онтологічного підходу для організації інформаційного впливу автоматизованих систем в роботу командирів підвищить їх інформаційну обізнаність, дозволить в більш короткі терміни приймати обґрунтовані рішення на підготовку та ведення бойових дій. Таким чином, в роботі СППР розглядається як програмно-математичне та інформаційне забезпечення (ПМтаІЗ) для формування мережецентричної онтологічної СППР командирів тактичної ланки управління Сухопутних військ (СВ) Збройних Сил (ЗС) України.

При створенні програмної системи онтологічної моделі СППР запропоновано використовувати модульний підхід: всі функціональність моделі розділена на модулі; для кожного модуля описаний інтерфейс, який він повинен реалізувати; розширення функціональності відбувається шляхом додавання нового модуля до системи. Даний підхід дозволяє розробити набір базових модулів, що використовуються в будь-якій онтологічній моделі незалежно від предметної області. Функціональне доповнення через додавання нових модулів дозволяє адаптувати ядро мережецентричної онтологічної моделі до конкретної предметної області.

До складу програмного інтерфейсу для роботи з такою онтологією входить: модуль ПМтаІЗ за напрямком обміну інформацією (приймання-передача, обробка і зберігання команд, сигналів, розпоряджень, бойових документів); модуль ПМтаІЗ за напрямком обробки та зберігання інформації (електронний документообіг, ведення баз даних, обробка і зберігання даних поточної обстановки); модуль ПМтаІЗ за інформаційно-розрахунковим напрямком (організація управління, взаємодії та рекогносцировки на місцевості; збір, обробка та облік даних про свої війська, противника та фізико-географічні умови; оцінка обстановки; підтримка вироблення замислу; планування бою (бойових дій); планування матеріально-технічного забезпечення ін.); модуль ПМтаІЗ за напрямком картографічної підтримки (вирішення геоінформаційних завдань); модуль ПМтаІЗ за напрямком навігаційної підтримки (безперервне визначення значень навігаційних параметрів наземних рухомих об’єктів).

В рамках проведення досліджень розроблено прототип ПМтаІЗ автоматизованих робочих місць мережецентричної онтологічної СППР командирів тактичної ланки управління СВ ЗС України, як функціональної складової (підсистеми) автоматизованої системи управління тактичної ланки Сухопутних військ ЗС України.

Олійник С. Е., Опалинський В. Б.

КІБЕРБЕЗПЕКА В УМОВАХ ТА ВИКЛИКАХ СЬОГОДЕННЯ

Протягом останніх років все ширше використання перспективних ІТ-технологій зумовило не лише численні переваги, а й цілу низку проблем. Зокрема, істотно підвищився рівень інформаційного негативного впливу на процеси збереження та розповсюдження інформації, зросла чисельність нових загроз інформаційній безпеці, таких як нові форми кібератак. При цьому в комп’ютерних системах зберігаються і обробляються великі обсяги облікової інформації, будь-який збій може привести до надмірних витрат, недостатніх доходів, втрати активів, санкцій тощо. Тому головним пріоритетом захисту облікової інформації є розроблення заходів, спрямованих на збереження інформації, що міститься у комп’ютерних базах. Виділяють дві категорії загроз комп’ютерним інформаційним системам: активні та пасивні. Активні загрози включають комп’ютерне шахрайство та комп’ютерний саботаж. Пасивні загрози – помилки системи (пошкодження окремих компонентів обладнання або програмного забезпечення). Досліди вказують, що 45% причин загроз становлять навмисні дії.

У зв’язку з тим, що останнім часом збільшується кількість незаконних фінансових операцій, крадіжок та шахрайства в мережі Інтернет, несанкціонованого використання чи модифікації програмного забезпечення, під час оцінки надійності систем інформаційної безпеки мають бути змінені пріоритети від забезпечення традиційної інформаційної безпеки до кібербезпеки. Питання кібербезпеки зачіпає інтереси не лише державних інституцій, а і приватного сектору та громадянського суспільства. Зрозуміло, що втрата інформації, яка зберігається в окремому комп’ютері і є важливою для користувача цього комп’ютера, не може розглядатися як загроза кібербезпеці. Однак захист інформації потрібно передбачувати, виходячи із цінності інформації не для себе, а для

зловмисників, які будують відносини винятково на грошовій основі. Тому проблема кібербезпеки – це проблема не лише загально-державного рівня, а кожного окремо взятого користувача. Відповідно повинна бути створена програма визначених дій, спрямованих на створення кіберзахисту облікової інформації, сфера застосування якого поширюється на людські ресурси і не обмежується винятково технологічними аспектами. Загалом управління кібербезпекою повинно передбачати створення або спеціальної служби із забезпечення кібербезпеки облікової інформації, або введення посади спеціаліста з кібербезпеки. Ці функції також можуть бути покладені на системних адміністраторів, адміністраторів комп'ютерних мереж, менеджерів систем з інформаційної безпеки, аналітиків систем забезпечення кібербезпеки.

Таким чином, серед можливих шляхів підвищення ефективності заходів кібернетичного захисту можуть бути: налагодження ефективної системи кіберзахисту об'єктів з урахуванням їх категорій за ступенем уразливості; підвищення ефективності інформаційно-аналітичної роботи суб'єктів інформаційної безпеки; створення та постійне оновлення бази даних порушників і порушень, у тому числі кіберзлочинців; створення системи раннього виявлення інформаційних небезпек. Крім того, необхідно створити умови для дотримання режиму експертного контролю та нерозповсюдження несертифікованих програмно-апаратних засобів і систем, комп'ютерної техніки, оперативного реагування на інциденти, які пов'зані з виведенням із ладу інформаційно-технологічних систем, а також налагодження каналів формального та неформального обміну інформацією стосовно загроз комп'ютерної злочинності та кібертероризму. Загалом такий підхід забезпечить зниження кіберзагроз як для власників особистої інформації так і для кібербезпеки в цілому в Україні. Це особливо актаульно під час військової агресіїї та політичного тиску з боку Російської федерації.

Правдивець О. М., Лаврут Т. В., Родзяк І. П.

ПОРЯДОК ВІДПРАЦЮВАННЯ МЕТОДИКИ РОЗРОБКИ НОРМАТИВІВ З ОЦІНКИ ІНДИВІДУАЛЬНОЇ ПІДГОТОВКИ ОПЕРАТОРІВ РАЙОННИХ ВІЙСЬКОВИХ КОМІСАРІАТІВ ЗІ СТВОРЕННЯ (РЕДАГУВАННЯ) ОБЛІКОВИХ ЗАПИСІВ ВІЙСЬКОВОЗОБОВ`ЯЗАНИХ

У системі повсякденної діяльності обласних та районних військових комісаріатів Збройних Сил України активно та широко використовуються методи практичного навчання працівників та структурних підрозділів, які засновані на використанні нормативів експлуатації програмного забезпечення. Нормативи дозволяють встановлювати єдині та об'єктивні підходи до визначення рівня навченості та підготовки військовослужбовців, працівників і підрозділів районних та обласних військових комісаріатів, щодо експлуатації автоматизованої системи Єдиного державного реєстру військовозобов'язаних в частині, що стосується удосконалення професійної підготовки операторів ЄДРВ районних військових комісаріатів, а також розробки Програми підготовки адміністраторів ЄДРВ рівня обласних військових комісаріатів оперативних командувань.

Актуальність роботи обумовлена необхідністю розроблення (уточнення) нормативів програмного забезпечення для операторів військових комісаріатів. У зв'язку з цим автори пропонують розкрити порядок відпрацювання Методики розробки одиночного нормативу з оцінки індивідуальної підготовки операторів військових комісаріатів зі створення (редагування) облікових записів військовозобов`язаних.

Оцінювання практичних навичок індивідуальної підготовки фахівців визначених військово-облікових спеціальностей (ВОС) Сухопутних військ Збройних Сил України з оволодіння ними відповідними зразками озброєння і військової техніки (ОВТ) здійснюється відповідно до Збірника нормативів з бойової підготовки Сухопутних військ

Збройних Сил України шляхом виконання нормативів. Нормативи дозволяють встановлювати єдині та об'єктивні підходи до визначення рівня навченості та підготовки військовослужбовців щодо правильної та ефективної експлуатації ОВТ відповідно до отриманої ними ВОС.

У зв'язку з цим, виникла необхідність подальшого дослідження, щодо вирішення актуального наукового завдання, яке полягає в порядку опрацюванні методики розробки одиночного нормативу з оцінки індивідуальної підготовки операторів районних (міських) військових комісаріатів (Р(М)ВК).

Відповідно до Методики підготовки операторів Єдиного державного реєстру військовозобов'язаних для районних (міських) військових комісаріатів, яка реалізована в Стандарті індивідуальної підготовки СТІ 049А.45Л рівень індивідуальної підготовки оператора оцінюється за двома складовими, а саме за рівнем теоретичних знань та рівнем практичних навичок.

У ході розроблення та складання нормативів з оцінки індивідуальної підготовки операторів Р(М)ВК, як правило вирішуються два основних завдання:

1. Визначається перелік нормативів (з назвою кожного нормативу, встановленими відліками їх початку та кінця, а також змістом робіт, що підлягають виконанню).

2. Визначаються показники і критерії оцінки виконання нормативів.

Автори, для створення Методики підготовки операторів Єдиного державного реєстру військовозобов'язаних для районних (міських) військових комісаріатів, застосували наступні шляхи вирішення наукового завдання.

Пропонується завдання щодо визначення переліку нормативів бойової підготовки вирішувати методами мережевого планування і управління, а для циклічних процесів – шляхом розробки моделей потокового виробництва. Використання цих математичних методів дозволяє представити процеси підготовки та виконання завдань особовим складом і підрозділами, як єдиний нерозривний комплекс взаємопов'язаних операцій, а особовий склад, що бере участь у цих процесах, як ланки єдиної складної системи.

Застосування мережевих моделей дає змогу отримати логіко-математичний опис процесу виконання завдання та алгоритмізувати розрахунок його основних показників.

Визначення переліку нормативів індивідуальної підготовки операторів Р(М)ВК в ході розроблення та складання нормативів пропонується здійснюється наступним чином:

1-й крок. Визначається сукупність усіх операцій (елементарних робіт), що входять до процесу виконання завдання, їх зміст та послідовність виконання.

2-й крок. Будується мережева модель процесу виконання завдання та здійснюється її оптимізація за кількістю операцій.

3-й крок. Визначається критичний, підкритичний та інші шляхи мережевої моделі.

4-й крок. З операцій процесу виконання завдання формуються нормативи роботи за чотирма групами пріоритету. При цьому виключаються операції, які не можуть бути виконані автономно.

Під час визначення переліку показники і критеріїв оцінки виконання нормативів враховуються:

- кількість помилок, допущених під час виконання нормативу;
- збільшення часу від табличного (умовного) внаслідок необхідності виправлення допущеної помилки (час затримки);
- рівень досягнення необхідного результату (певного ступеню ефективності кінцевого результату) під час виконання нормативу.

У свою чергу, кількісний показник виконання нормативу – час, визначається одним з наступних способів.

Перший спосіб визначення часових критеріїв оцінки нормативу застосовується для визначення простих і незначних за тривалістю виконання нормативів (тих, що вимірюються секундами або одиницями хвилин).

Отже, визначивши один з нормативів (базовий), можна також визначити й усі інші.

Другий спосіб визначення часових критеріїв оцінки нормативу заснований на методах мережевого планування і управління.

Другий з розглянутих способів визначення часових критеріїв оцінки нормативу, який базується на методах мережевого планування і управління, крім усього вказує на два основних шляхи можливого скорочення часу його виконання, зокрема:

1. Підвищення виучки та професійної підготовки операторів.

2. Зміни характеру та технології процесів, що складають норматив.

Результати, що були отримані в ході її відпрацювання використані під час розроблення одиночного нормативу з оцінки підготовки операторів Р(М)ВК та внесено до Збірнику нормативів бойової підготовки Сухопутних військ Збройних Сил України.

Запропонована методика може вважається універсальною

Результати досліджень були враховані під час безпосередньої роботи операторів Р(М)ВК при виконанні завдань по створенню бази даних Єдиного державного реєстру призовників, військовозобов'язаних солдатів, сержантів і офіцерів запасу, внесення до нього відповідних змін.

Доцільно враховувати їх під час відпрацюванню одиночних нормативів для операторів, які обслуговують існуючі програмні забезпечення по веденню обліку і Методики та одиночні нормативи для яких не розроблені.

Кухарська Л. В., Шкіцькій Д. В.

КОСМІЧНА РОЗВІДКА В ЗБРОЙНИХ КОНФЛІКТАХ СУЧАСНОСТІ

Найхарактернішою рисою збройної боротьби сучасності можна вважати широкомасштабне використання космічних систем (наземних та орбітальних сегментів) для ведення розвідки, передачу даних, управління військами та зброєю в умовах реального часу.

Використання космічних систем стали основним джерелом для вирішення завдань інформаційного забезпечення збройних сил у провідних країнах світу.

Активне застосування космічних апаратів дистанційного зондування Землі подвійного призначення з розрізненою здатністю в кілька десятків сантиметрів – це не тільки інструмент здійснення розвідки сучасними збройними силами, але і необхідний елемент єдиної автоматизованої системи управління військами (силами).

На основі аналізу можливостей сучасних та перспективних космічних апаратів і світового досвіду використання космічного простору дозволяє всі завдання його використання в інтересах збройних сил поділити на три основні групи:

- забезпечення бойової діяльності збройних сил (всебічне інформаційне забезпечення, а саме виявлення ранніх ознак підготовки противника до війни, встановлення факту (початку) нападу, забезпечення розвідувальними даними командування збройними силами, контроль результатів ракетних ударів, навігаційне, гідрометеорологічне та топогеодезичне забезпечення операцій військ (сил), оперативне спостереження за обстановкою в районі бойових дій, контроль радіаційної обстановки і вирішення інших завдань забезпечення бойових дій);
- забезпечення управління та зв'язку (централізація бойового управління військами і зброєю, забезпечення збройних сил до тактичної ланки включно космічним зв'язком та розвідувальними даними, що значною мірою підвищує надійність управління військами в будь-яких умовах оперативно-стратегічної обстановки);
- ведення воєнних дій в космосі (радіоелектронне подавлення космічних засобів управління силами і засобами противника, активний вплив на космічне та геофізичне середовище, розвідку космічного простору і видачу цілевказівок наземним бойовим засобам, створення сприятливих умов для виконання завдань своїми космічними силами і засобами, іншими видами збройних сил).

Вище зазначене вимагає побудови в Міністерстві оборони України та Збройних Силах України дієздатної та надійної системи забезпечення військ (сил) космічною інформацією в реальному часі.

УДК 316.42.752

Горлинський В. В, Ананьїн В. О.

ЗНАЧУЩІСТЬ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ ФАХІВЦІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ ДЕРЖАВИ

Якісні зміни в сучасному інформаційно-комунікаційному просторі, що відбуваються завдяки розвитку інформаційних технологій, значною мірою впливають на спрямованість і якість підготовки фахівців сектору безпеки і оборони держави. Комунікаційна складова стає одним із найважливіших елементів національної безпеки України. Від обсягу, швидкості та якості обробки інформації залежить ефективність управлінських рішень у сфері безпеки і оборони держави. Комунікаційні технологій підвищують ефективність сил оборони, якісно перетворюють управління технічними засобами і озброєнням.

Але, поряд із зазначеним, потрібно зауважити, що розвиток цифрового світу зумовив і виникнення нових небезпек в інформаційно-комунікативному просторі, а глобалізація світу стала чинником інтернаціоналізації кіберзлочинності. Утворення в інформаційному просторі якісно нового сектору, зумовило необхідність розробки и впровадження нормативних стандартів із захисту національних інтересів України в кіберпросторі. З метою створення умов для безпечного функціонування кіберпростору, спочатку було прийнято Стратегію кібербезпеки України, а в 2017 році Закон «Про основні засади забезпечення кібербезпеки України». У документах було визначено правове поле розгортання відносин, що функціонують у кіберпросторі, введено принципові положення, поняття і норми, що регулюють правові відносини у цій сфері. Це, також, зумовлює необхідність відповідних змін у навчанні, включення нових понять, термінів, значень, компетентностей і настанов в систему освітніх знань фахівців сектору безпеки і оборони держави, що сприяють успішному виконанню професійних завдань у умовах розвитку сучасних інформаційних технологій.

Аналіз освіти як чинника безпеки сучасного суспільства здійснено у працях вітчизняних дослідників В. Андрущенка, В. Ананьїна, М. Згуровського, О. Данільяна, В. Кременя, М. Михальченка, В. Огнев'юка, Г. Почепцова, М. Панова, О. Пучкова, О. Сосніна, А. Старіша, В. Толубки, М. Швеця та інших науковців. Згідно з дослідженнями, однім з головних завдань освіти постає формування у майбутнього фахівця не тільки професійних знань і навичок, але і превентивного мислення, антикризової поведінки, відповідальності за можливі наслідки прийнятих рішень.

Отже, проблема поєднання інформаційних і новітніх гуманітарних технологій виводить на проблематику безпеки і технологічних ризиків, з'ясування моральних регулятивів службової і професійної діяльності, базисних цінностей підготовки фахівців сектору безпеки і оборони держави. Значущість інформаційного впливу на підготовку фахівців і професійну діяльність в сфері захисту національних інтересів держави посилюється, завдяки поєднанню сучасних інформаційних технологій з гуманітарними технологіями, спрямованими на маніпулювання колективною свідомістю.

Взаємодія нанонаук, генної інженерії, інформаційних і новітніх гуманітарних технологій, на кшталт чипування людини або нейролінгвістичного програмування, все більш радикально змінює людину, трансформуючи її власно людську природу, попереджують аналітики. Неконтрольований вплив сучасного інформаційного середовища на свідомість фахівців, діяльність яких пов'язана із захистом національних інтересів України,

вплив зовнішньої інформаційної експансії, внаслідок якої, формується мережна залежність, можуть мати негативні наслідки в їх професійній справі. Сучасні можливості інформаційних технологій, що забезпечують доступність і великі обсяги інформації, з одного боку, і неусвідомлена спрямованість людини на опанування нею, з іншого, можуть сприяти формуванню поверхневого, безсистемного знання, коли втрачається зв'язок між отриманим знанням і майбутньою професійною діяльністю, загублюється цінність і значущість знання, пов'язаного із захистом національних інтересів України.

Сучасні глобальні зміни, що супроводжуються підвищенням ризикогенності професійної діяльності, поряд із зазначеним, зумовлюють необхідність переосмислення значущості власно безпекової складової у підготовці фахівців до діяльності в непередбачуваних ситуаціях підвищеного ризику. Потреба у впровадженні в систему підготовки фахівців сектору безпеки і оборони держави, поряд із спеціальними знаннями, загальнотеоретичних знань про безпеку, з відповідною кореляцією світоглядних настанов зумовлена, також, посиленням проявів інформаційного тероризму в світі та Україні, зростанням масштабів гуманітарних і техногенних катастроф, проявами соціальної девіації. Актуальність постановки цього питання, в цей важкий для України час військових, політичних і соціально-економічних випробувань, є очевидною. Сучасна військова освіта постає одним з провідних чинників безпеки українського суспільства, а її якість, згідно з «Національною доктриною розвитку освіти», визначається як передумова національної безпеки України.

Перелічені чинники надають підстави зробити висновок, що підготовка фахівців сектору безпеки і оборони держави, має ґрунтуватися на системи базових професійних і гуманітарних знань, соціальних і професійних цінностей, моральних і правових засад, психологічних настанов, впровадження яких, має сприяти формуванню професійних і соціальних особистісних якостей, що відповідають сучасним вимогам професії і потребам часу. Результати підготовки фахівців мають відображуватись у відповідних компетентностях, що відповідають вимогам професійної діяльності в сфері забезпечення національної безпеки в умовах швидких змін інформаційно-комунікативних технологій, зростаючих ризиків і небезпек, які припускають спроможність фахівця приймати ефективні, відповідальні професійні і управлінські рішення в непередбачуваних умовах зростання ризику, враховуючи їх можливі соціальні наслідки.

Згідно з окресленими компетентностями, у контексті адаптації до безпекових потреб, важливим завданням підготовки фахівців є формування таких здатностей, як комплексна (професійна, інформаційна, інтелектуальна, моральна, психологічна) готовність фахівця до професійній діяльності в умовах інформаційних ризиків, воєнних, техногенних і гуманітарних загроз; прогнозування, попередження і подолання імовірних небезпек у професійній діяльності; здійснення самостійного, адекватного і відповідального вибору в прийнятті рішень у непередбачуваних, екстремальних ситуаціях, пов'язаних із захистом національних інтересів держави; критична оцінка і врахування можливості небезпечних наслідків власної діяльності й прийнятих рішень; самостійний пошук і відпрацювання інформаційних джерел для систематичного оновлення власних знань з питань безпеки професійної діяльності з метою загальнотеоретичного і професійного самовдосконалення.

Отже розвиток комунікаційних систем і технологій у сучасному небезпечному світі, потребує впровадження у систему підготовки фахівців сектору безпеки і оборони держави, поряд із професійними знаннями, відповідної складової системи безпекових компетентностей і здатностей, превентивного мислення, антикризової поведінки, відповідальності за можливі наслідки прийнятих рішень, що мають сприяти успішному виконанню професійних завдань в складних умовах підвищеного ризику професійної діяльності в сфері захисту національних інтересів України.

УДК 519.72 : 624.028 (075)

Лівенцев С. П., Павлов В. П.,Василюк Ю. С.

МАТЕМАТИЧНА МОДЕЛЬ ПРОЦЕСУ ФУНКЦІОНУВАННЯ БЛОКУ ЗАХИСТУ ВІД ЗАВАД БЕЗПРОВОДОВОЇ СИСТЕМИ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В даний час проблема забезпечення завадозахищеності безпроводових систем спеціального призначення є досить актуальною. Розвиток систем радіоелектронного придушення та їх широке застосування в сучасних бойових діях вимагають розробки нових ефективних алгоритмів та способів захисту від завад. З кожним новим поколінням радіозасобів наростає складність функцій, компонентів і правил проектування їх архітектури. Більш за все перспективні багаторежимні радіозасоби (РЗ) зажадають радіотерміналів і базових станцій, що мають високу пристосованість до навколишнього середовища з погляду характеристик радіоканалу, протоколів доступу, швидкостей передачі даних, попереднього і післякорекції, виправлення помилок, випромінюваної потужності й призначених для користувача характеристик.

В провідних країнах світу перспективним напрямком створення радіозасобів є технологія програмно-керованих радіостанцій (ПРС), що використовує стандартні апаратні засоби для виконання функцій під управлінням програмного забезпечення.

Тому метою роботи є розробка та удосконалення методів і засобів математичного та комп'ютерного моделювання, обчислювальних методів, призначених для використання при всебічному дослідженні і створенні об'єктів та систем технічного призначення, що дозволяє істотно скоротити об'єм експериментальних досліджень або повністю їх виключити. Це дає можливість значно зменшити витрати матеріальних ресурсів, грошових коштів і часу на створення та вдосконалення виробів.

Для реалізації процедур демодуляції, декодування та адаптивного управління, з метою усунення апріорної невизначеності пропонується алгоритм визначення апріорних відомостей, які зводяться до знання (часткового знання) законів розподілу ймовірностей та розрахунку функцій правдоподібності прийнятих даних.

З метою визначення невідомих апріорних розподілів прийнятої інформації запропоноване задавання емпіричних відомостей, які отримуються з аналізу прийнятої певної тестової послідовності, що вимагає застосування додаткового каналу передачі. За результатами аналізу прийнятої інформації формуються оцінки середнього значення невизначеності інформації та відбувається мінімізація цих оцінок вибором правил рішення за допомогою методів адаптивного управління.

Запропоновано новий підхід до використання результатів декодування турбокодів як додаткової інформації для оцінки достовірності інформації у вигляді змін знаку апріорної-апостеріорної інформації, на підставі якого вдосконалено метод оцінювання достовірності інформації в частині представлення способу оцінювання каналу на основі формалізованого опису декодування турбокодів та використання для цього щільності розподілу нормалізованих значень кількості змін знаку апріорної-апостеріорної інформації декодера турбокоду, що зменшує апріорну невизначеність і істотно підвищує точність оцінки заданої та сталої достовірності в процесах адаптації завадостійких кодерів при відсутності додаткового тестового каналу.

Розроблено імітаційну модель процесу функціонування безпроводової системи передачі даних, яка включає векторну модель дискретно-неперервного каналу з врахуванням впливу навмисних завад. Запропонована імітаційна модель враховує методи та способи об’єднання компонентних кодів, властивості середовища поширення та має можливість в широких межах змінювати параметри кодів (поліноми, розмір кадру, типи перемежувачів, кількість компонентних кодів, структури конкатенації кодів, кількість

ітерацій декодування, алгоритми декодування і інші параметри) для отримання статистичних характеристик з метою вдосконалення існуючих та перспективних інформаційних технологій.

УДК 519.72 : 624.028 (075)

Лівенцев С. П., Павлов В. П., Василюк Ю. С.

ЗАСТОСУВАННЯ АЛГОРИТМІВ СЛІПОЇ ОБРОБКИ ОЦІНЮВАННЯ СКАЛЯРНИХ ТА ВЕКТОРНИХ КАНАЛІВ ЗІ СТРУКТУРНИМИ ЗАВАДАМИ

Підвищення достовірності інформаційного обміну в системах спеціального зв'язку може бути забезпечене шляхом застосування потужного завадостійкого кодування – турбокодів. Одним з методів підвищення достовірності прийняття рішень по надійності декодування символів (біт) в турбокодах може бути ідентифікація та оцінювання каналу. У скалярному каналі, тобто в каналі з одним входом і виходом, алгоритми сліпої ідентифікації, як правило, вимагають деякої статистичної вибірки інформаційних блоків на виході каналу для побудови оцінки, тобто необхідні нові методи оцінювання.

Сліпа обробка (*blind signal processing*) – це нова технологія цифрової обробки сигналів, яка отримала свій розвиток протягом останніх років. У загальному вигляді завдання сліпої обробки можна сформулювати як цифрову обробку невідомих сигналів, що пройшли лінійний канал з невідомими характеристиками на фоні адитивних шумів. Під ідентифікованістю системи наосліп розуміється можливість відновлення імпульсної характеристики системи з точністю до комплексного множника тільки по вихідних сигналах.

У загальному випадку для стаціонарного гауссівського входу ідентифікація неможлива. Якісно, без прив'язки до конкретного методу ідентифікації і властивостей каналу, для отримання сліпої оцінки в скалярному каналі потрібна інформаційна послідовність, довжина якої зазвичай на два порядки перевищує довжину каналу. При цьому якість оцінки наближається до оцінки за тестовим сигналом.

Запропоновано підхід до синтезу алгоритмів сліпої ідентифікації на основі поліноміальних статистик, який дозволяє за єдиним алгоритмом синтезувати різні методи сліпої ідентифікації для скалярних каналів зі стаціонарним і нестаціонарним входом та різних розподілах вхідних символів. На відміну від підходу на основі поліспектрів в даному випадку може бути знижена невизначеність вибору набору кумулянтних функцій в процедурі синтезу алгоритму.

Використання статистик 2-го порядку для сліпої ідентифікації скалярного каналу можливе в цілому для нестаціонарної моделі вхідного сигналу і в частковому випадку періодично-корельованого (циклостаціонарного) сигналу.

Використовуючи поліноміальні статистики, розв'язок задачі сліпої ідентифікації зводиться до задачі розв'язання систем поліноміальних рівнянь від багатьох змінних. Даний підхід є узагальненням підходу, заснованого на використанні поліспектрів (методи статистик високого порядку), відомих в теорії зв'язку. Даний підхід може бути узагальнений і на випадок векторного каналу.

Модель векторного каналу використовується для опису рознесеного прийому (в просторі або в часі). Умови ідентифікації векторного каналу можуть бути сформульовані в рамках детермінованої моделі, тобто сліпа ідентифікація здійснюється по одній реалізації, також як і при використанні тестового сигналу. При цьому співвідношення довжин каналу та інформаційної послідовності становить приблизно один порядок, що дозволяє використовувати ці технології в каналах з швидкими завмираннями.

Можливість статистичної сліпої ідентифікації каналу за моментними функціями випадкового процесу 2-го порядку на виході каналу забезпечується наданням в загально-

му випадку стаціонарному інформаційному сигналу додаткових нестаціонарних властивостей, що сприяють подальшій сліпій ідентифікації. При цьому модель періодично корельованого процесу на вході є окремим випадком для загальної нестаціонарної моделі просторово-часового каналу.

При застосуванні методу сліпої ідентифікації оцінка імпульсної характеристики може далі використовуватися для оцінки інформаційної послідовності, тобто є першим етапом сліпого вирівнювання, яке може бути використане для підвищення достовірності прийняття рішення під час декодування турбокодів.

УДК 621.396.6

Сакович Л. М., Василюк Ю. С.

МЕТОД БАГАТОРІВНЕВОЇ СТРУКТУРИЗАЦІЇ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ ПРИ ЇХ ПРОЕКТУВАННІ

В теперішній час теоретичні та прикладні питання скорочення часу без втрати якості ремонту складних технічних об’єктів достатньо глибоко і широко досліджені в наукових працях провідних вітчизняних і зарубіжних авторів, серед яких Жердєв Н. К., Кононов В. Б., Креденцер Б. П., Ксёнз С. П., Мозгалевський А. В. та багато інших.

Однак, в відомих роботах при рішенні задач підвищення ефективності діагностичного забезпечення (ДЗ) поточного ремонту (ПР) радіоелектронних засобів (РЕЗ) не повністю враховані особливості їх схемної та конструктивної побудови, що зумовлені наявністю різних видів надлишковості. Під діагностичним забезпеченням розуміють комплекс взаємопов’язаних правил, методів, алгоритмів та засобів, необхідних для проведення діагностування радіоелектронних засобів на всіх етапах їх життєвого циклу. Надлишковість – це додаткові засоби й (або) можливості більш ніж необхідні для виконання об’єктом заданих функцій. Розрізняють конструктивну, часову, структурну, функціональну та інформаційну надлишковість.

В тезах доповіді на основі комплексного використання всіх виявлених видів надлишковості розкрито метод багаторівневої структуризації РЕЗ при їх проектуванні згідно з вимогами до ремонтопридатності.

Метод призначений для наукового обґрунтування рекомендацій з проектування перспективних зразків РЕЗ з метою забезпечення заданого рівня ремонтопридатності при реалізації ПР у ремонтних органах (РО) агрегатним методом.

Сутність методу полягає у визначенні числа складових елементів у конструкції РЕЗ, що забезпечує задане значення середнього часу відновлення при обмеженнях на кваліфікацію фахівців і технологічне оснащення РО, на основі комплексного використання всіх виявлених видів надлишковості РЕЗ та отриманих нових функціональних залежностей характеристик ДЗ від керованих змінних.

Вихідні дані для використання методу одержують після аналізу умов ПР, матеріально-технічної бази та штатного розпису ремонтного підрозділу, принципової електричної схеми виробу.

Метод є основою аналітичних й алгоритмічних засобів розробки рекомендацій з компонування перспективних зразків РЕЗ із урахуванням вимог до рівня їхньої ремонтопридатності за умови реалізації ПР обслуговуючим персоналом або РО. Його доцільно використати при розробці нової редакції вимог до ремонтопридатності РЕЗ, яку модернізують та розробляють, а також у проектних організаціях при розробці перспективних зразків РЕЗ для забезпечення необхідного значення середнього часу відновлення при ПР.

Наукова новизна методу полягає в комплексному використанні всіх виявлених видів надлишковості РЕЗ при розробці ДЗ на основі вперше отриманих функціональних залежностей кількісної оцінки впливу компонування виробу на показники ремонтопридатності.

Яровий В. С., Радзівілов Г. Д., Гришина Н. С.

ОБГРУНТУВАННЯ НЕОБХІДНОСТІ РОЗРОБКИ МЕТОДИКИ ДІАГНОСТУВАННЯ ВТОРИННИХ ДЖЕРЕЛ ЖИВЛЕННЯ ВІЙСЬКОВОЇ ТЕХНІКИ ЗВ'ЯЗКУ В ДИНАМІЧНОМУ РЕЖИМІ

Сучасна техніка зв'язку характеризується своєю багатофункціональністю і складністю побудови, яка обумовлена об'ємом і характером покладених на неї завдань за допомогою використання різних технічних пристроїв, які у своєму складі мають один із найважливіших елементів – вторинні джерела електроживлення (ВДЕЖ).

Аналіз розвитку військової техніки зв'язку (ВТЗ), як в Україні, так і за її межами, показує, що покращення тактико-технічних та експлуатаційних характеристик досягається, як правило, схемним і конструктивним ускладненням ВТЗ, що призводить до зниження їх надійності. Виявлені протиріччя можливо усунути за рахунок покращення ремонтоздатності, також за рахунок раціонального компонування ВТЗ, якісного діагностичного забезпечення, під яким необхідно розуміти комплекс взаємозалежних правил, методів, алгоритмів і засобів, що необхідні для здійснення діагностування ВТЗ на всіх етапах життєвого циклу. В рамках діагностичного аспекту надійності повинна вирішуватися задача визначення технічного стану об'єктів (зразків, виробів, пристроїв) ВТЗ, тобто організації перевірки справності, працездатності, правильності функціонування елементів, ключовими з яких є ВДЕЖ.

Актуальність завдання технічного діагностування ВДЕЖ визначається наступними обставинами:

- кількістю ВДЕЖ в сучасній ВТЗ, що складають 10% від її об'єму;
- великими працевтратами на діагностування ВДЕЖ (до 70% від загального часу на відновлення), а також високою вартістю відновлювальних робіт (до 50% від вартості життєвого циклу виробу).

Аналіз контролю діагностування ВДЕЖ показує, що якість визначення технічного стану ВДЕЖ безпосередньо на об'єктах ВТЗ достатньо низька. Наприклад, при виникненні збоїв у ВДЕЖ в динамічному режимі сучасні засоби контролю не визначають причину цих збоїв. В результаті цього знижується коефіцієнт готовності ВТЗ.

Як показав досвід, під час експлуатації ВДЕЖ в ВТЗ працюють в таких умовах, коли навантаження змінюється у великих межах. Ці динамічні зміни навантаження приводять до збоїв в роботі ВДЕЖ, навіть в тих випадках, коли результати діагностики в статичному режимі можуть бути позитивними.

Існуючі системи діагностування, іншими словами контролю технічного стану виробу, можуть забезпечувати необхідний середній час відновлення при заданих економічних витратах (10-15% від вартості контролюємого ВДЕЖ) та необхідну ефективність контролю.

Отже, необхідність розробки такої методики діагностування, яка б дозволяла забезпечити необхідну ефективність цієї діагностики в динамічному режимі, є більш ніж актуальною.

Для того, щоб отримати задану достовірність параметрів, отриманих внаслідок діагностики, необхідно правильно визначити усі ознаки, які характеризують справний або несправний стан ВДЕЖ; вибрати узагальнені параметри, які однозначно визначають ці ознаки; знайти співвідношення між точністю вимірювань параметрів, що контролюються та допусків на ці параметри.

Зубков А. М., Цицик М. В., Красник Я. В., Мартиненко С. А.

АДАПТИВНА СИСТЕМА МНОГОСПЕКТРАЛЬНОГО ЛОКАЦІЙНОГО МОНІТОРИНГУ ОХОРОНЯЄМОЇ ЗОНИ

Моніторинг локаційними методами в інтересах вирішення загальнотехгічних і спеціальних завдань являється одним із актуальних напрямків розвитку інформаційних технологій. Для отримання локаційної інформації застосовуються активні, пасивні і напівактивні сенсори різних дільниць спектру електромагнітних хвиль: радіо, інфрачервоного і оптичного діапазонів. Із-за суттєвої різниці вказаних сенсорів по дальності дії, інформативності, завадозахищеності запропоновані оптимальні алгоритми комплексування локаційних каналів спостереження з різними фізичними сенсорами в рамках інтегрованої многоспектральної системи моніторингу. При цьому реалізуються переваги парціальних спектральних каналів: фотоконтрасного – висока кутова роздільна здатність; інфрачервоного (теплового) – висока кутова роздільна здатність, цілодобовість; радіолокаційного – цілодобовість, всепогодність, висока роздільна здатність по дальності і доплерівській частоті в активному режимі роботи.

Необхідно відмітити, що в теоретичному аспекті відкритим залишається питання оцінки приросту ефективності многоспектральної системи моніторингу, а в прикладному аспекті – інженерний синтез структури і алгоритмів роботи такої системи в ціле фонової обстановки, що динамічно змінюється.

Приріст ефективності мультиспекрального моніторингу може бути визначений через інформативність мультиспекрального зображення об’єкту (сцени) спостереження. Але запропонований раніше підхід до оцінки інформативності мультиспекрального відео зображення через дивергенцію Кульбака-Лейблера не може бути використаний стосовно мультиспектральних систем моніторингу із значним рознесенням парціальних каналів по частоті, оскільки на практиці застосовуються різні системи координат сформованих зображень (радіолокаційне зображення – в координатах “радіолокаційний контраст” – дальність, або доплерівська частота; оптичне (теплове) зображення – в координатах “оптичний (тепловий) контраст – азимут, кут місця”).

Пропонується для оцінки ефективності багатоспектрального моніторингу використовувати повний об’єм отриманої інформації по Шеннону (гіперспектральний куб інформації) з врахуванням специфіки формування парціальних зображень в фотоконтрастному і тепловому каналах:

- залежність енергетики каналу від стану приземний шару атмосфери (ніч, гідро метеори, пилюка, дим);
- втрати лінійної роздільної здатності по кутових координатах із збільшенням дальності до ділянки спостереження земної поверзні;
- неможливості використання в фотоконтрасному каналі на граничних дальностях спостереження кольорового контрасту (ціль спостерігається на “сірому” фоні).

Аналітично повну інформативність многоспектрального зображення запропоновано оцінювати виразом:

$$I = \frac{1}{D^2}\left(\frac{L_\alpha L_\varepsilon}{\gamma_\phi \mathrm{tg}^2 \Delta\theta_\phi} + \frac{L_\alpha L_\varepsilon}{\gamma_T \mathrm{tg}^2 \Delta\theta_T}\right) + \frac{L_D}{\Delta D} + \frac{\Delta F_\partial}{\Delta F}, \qquad (1)$$

де:, L_α, L_ε, L_D – лінійні розміри спостережуваного об’єкта по азимуту, куту місця і дальності, відповідно; γ_ϕ, γ_T, $\Delta\theta_\phi$, $\Delta\theta_T$ – коефіцієнти прозорості атмосфери і кутова роздільна здатність фотоконтрастного і теплового каналів, відповідно; ΔD, ΔF – роздільна здатність радіолокаційного каналу по дальності і допплерівській частоті; ΔF_∂ – ефективна ширина допплерівського спектра.

Бачимо, що для об'єктів, що спостерігаються, компоненти інформативності зв'язані з парціальними спектральними каналами, являються функціями дальності, що монотонно зменшуються. Не складно показати, що швидкість зменшення інформативності для фотоконтрастних і теплових каналів становить:

$$\frac{\partial I_{\phi,T}}{\partial D} = -\frac{2L_\alpha L_\varepsilon}{\gamma_{\phi,T}\,\mathrm{tg}^2\Delta\theta_{\phi,T}} D^{-3}, \qquad (2)$$

водночас для радіолокаційного каналу;

$$\frac{\partial I_P}{\partial D} = -\frac{2L_D C}{\Delta D \ln 2} D^{-1}. \qquad (3)$$

Аналіз виразів (1) – (3) показує, що наявність радіолокаційного каналу, як цілодобового, всепогодного з максимальними дальністю дії і "полем зору" в системі моніторінгу являється обов'язковим для:

- компенсації зменшення інформативності фотоконтрастного і теплового каналів при збільшенні дальності до об'єкту (ділянки), що спостерігається – див. вираз (2);
- "прицілювання" вузьконаправлених фото і теплового каналів при широкій кутовій зоні спостереження.

Важливо відмітити, що фундаментальний розрив в значеннях кутової роздільної здатності фото (теплового) каналів і радіолокаційного при обмежених розмірах апертур антен (об'єктивів) може бути ліквідований тільки при використанні в останнім мікрохвильового (зокрема міліметрового) діапазону електромагнітних хвиль.

З точки зору практичної реалізації потенціальних можливостей багатоспектрального моніторингу по дальності, інформативності і завадозахищеності найбільший інтерес становить ситуація ціле фонової обстановки, що динамічно змінюється (день, ніч, наявність метеоопадів або завад штучного походження).

Найвища ефективність може бути досягнута при перебудові передавальних функцій парціальних спектральних каналів в відповідності з адаптивним алгоритмом їх ранжування. Для цього введемо наступні практично виправдані передумови:

1. Ранжування парціальних спектральних каналів по пріоритетності, незалежно від завдань дистанційного моніторингу (виявлення, розпізнавання, вимір координат) проводиться на етапі виявлення.

2. Технічним еквівалентом методу максимуму правдоподібності являється метод максимального відношення сигнал/завада (ОСП) на виході каналу спостереження.

3. Апріорі завжди можна налагодити парціальний спектральний канал на максимальне відношення сигнал/завада для деякого усереднення для цього каналу фоноцільової обстановки.

4. Динамічні діапазони приймальних трактів парціальних спектральних каналів забезпечують лінійну обробку вхідної адитивної суміші сигнал + завада.

Тоді оптимальний алгоритм виявлення для трьох спектральної системи моніторингу приймає вигляд:

$$\sum_{k=1}^{3} \frac{1}{\sigma_k^2} \sum_{i=1}^{n_k} x_{ki} a_k \geq A, \qquad (4)$$

де: $x_{ki} = a_{ki} + b_{ki}$ – дискретна часова реалізація процесу на вході парціального спектрального каналу; a_{ki} – корисна компонента адаптивної суміші сигнал + шум; b_{ki} – шумова компонента; σ_k^2 – дисперсія завади на вході парціального спектрального каналу; n_k – об'єм дискретної часової вибірки; А – поріг, значення якого визначається потрібною імовірністю хибної тривоги при заданій вірогідності правильного виявлення для системи моніторинга в цілому.

Бачимо, що ефективність виявлення являється функцією ОСП $\frac{a_k}{\sigma_k^2}$. В припущенні, що парціальні спектральні канали нерівноцінні по ефективності для випадку $\frac{a_1}{\sigma_1^2} > \frac{a_2}{\sigma_2^2} > \frac{a_3}{\sigma_3^2}$ можна записати систему нерівностей

$$\left.\begin{aligned} &\frac{1}{\sigma_1^2}\sum_{i=1}^{n_1} x_{1i}a_{1i} > A_1 = A, \\ &A_1 \geq \frac{1}{\sigma_2^2}\sum_{i=1}^{n_2} x_{2i}a_{2i} > A_2, \\ &A_2 \geq \frac{1}{\sigma_3^2}\sum_{i=1}^{n_3} x_{3i}a_{3i} > A_3. \end{aligned}\right\} \qquad (5)$$

Система нерівностей (5) визначає оптимальний алгоритм роботи аналізатора завадової обстановки для багатоспектральної системи моніторингу. Фізична суть алгоритму – вибір серед парціальних спектральних каналів каналу з найвищим вихідним відношенням сигнал/завада і використання його в якості ведучого (опорного).

Алгоритм (5) розповсюджується на всі етапи моніторингу: розпізнавання, вимірювання (оцінка) координат.

Таким чином:

1. Розглянуто питання аналітичного опису інформативності багатоспектрального моніторингу.

2. Запропоновані алгоритми адаптації системи багатоспектрального моніторингу під цілефонову обстановку, що динамічно змінюється.

Красник Я. В., Зубков А. М., Юнда В. А., Мартиненко С. А.

ЗАСТОСУВАННЯ ПРИНЦИПІВ БАГАТОСПЕКТРАЛЬНОГО МОНІТОРИНГУ ДЛЯ САМОНАВЕДЕННЯ РАКЕТНОГО ОЗБРОЄННЯ

Фізичним джерелом інформації про ціль для формування команд самонаведення є поля різноманітних ділянок спектру електромагнітних хвиль (ЕМХ), розсіяні або випромінені ціллю. При наведенні на наземну ціль цим полям є супутні поля, які розсіяні або випромінені ділянками місцевості що оточують ціль (фоном). Основні характеристики каналу самонаведення ракети (дальність, точність, динаміка) визначаються позитивним енергетичним співвідношенням інтенсивності полів цілі і фону (цілефоновим контрастом).

Фізичними факторами, які визначають потужність сигналу і фону на вході головки самонаведення (ГСН) ракети є електродинамічні властивості матеріалу конструкції цілі і ділянки місцевості, яка безпосередньо оточує ціль (електропровідність, діелектрична проникність, комплексний коефіцієнт втрат). Одночасно енергетика сигналу цілі і фону визначається траєкторією польоту ракети на ділянці самонаведення, затуханням ЕМХ, які відбиті або випромінені ціллю на траєкторії “ракета-ціль”. Незалежно від ділянки спектру ЕМХ, що використовується, під цілефоновим контрастом розуміємо співвідношення

$$Э = \frac{P_ц}{P_ф}, \qquad (1)$$

де $P_ц$, $P_ф$ – потужність сигналів цілі і фону, відповідно.

В активному радіолокаційному каналі енергетика сигналу цілі визначається ефективною поверхнею розсіювання (ЕПР) цілі

$$\sigma_{\text{ц}} = 4\pi r_{\text{ц}}^2 \frac{\Pi_2}{\Pi_1}, \tag{2}$$

де Π_1, Π_2 – щільності потоку потужності зондуючого сигналу і ехо-сигналу; $r_{\text{ц}}$ – відстань “ракета-ціль”.

Оскільки ЕПР цілі залежить від ракурса підльоту ракети при розрахунках вводять поняття середньої ЕПР

$$\overline{\sigma}_{\text{ц}} = AS_{\text{ц}}, \tag{3}$$

де A – коефіцієнт пропорціональності, пов’язаний з властивостями відбиття матеріалу конструкції; $S_{\text{ц}}$ – метрична площа проекції цілі на картинну площу (перпендикулярну лінії візірування цілі).

Для імпульсних зондуючих сигналів середня ЕПР фону визначається

$$\overline{\sigma}_{\text{ф}} = \frac{1}{2}\rho_M r_{ц} \Delta\theta_{\alpha} c\tau_{u} \text{tg}\varepsilon, \tag{4}$$

де $r_{ц}$ – поточна дальність цілі; $\rho_{\text{м}}$ – коефіцієнт відбиття від місцевості; $\Delta\Theta_{\alpha}$ – ширина основного пелюстка діаграми направленості антени ГСН в курсовій площині наведення ракети; ε – кут наведення в площині тангажу; τ_u – тривалість зондуючого імпульсу; c – швидкість світла.

Тоді цілефоновий контраст в радіолокаційному каналі

$$\text{Э} = \frac{\overline{\sigma}_{\text{ц}}}{\overline{\sigma}_{\text{ф}}} = f\left(\rho_{м}, r_{ц}, \varepsilon\right). \tag{5}$$

Для теплового каналу енергетика сигналу цілі визначається формулою Релея-Джинса

$$B_f = \frac{2kT}{\lambda^2}, \tag{6}$$

де $B_f = \frac{d\,\Pi_f}{d\,\Omega}$ [$\text{В}_{\text{т}}/\text{м}^2\cdot$Гц$\cdot$Стр] – “яскравість” цілі, Π_f – спектральна густина потоку потужності теплового випромінювання проекції цілі на “картинну площину”; Ω – кут проекції тіла цілі на цю площину; k=1,38 10^{-23} Дж/К$^{\circ}$ – постійна Больцмана; T – термодинамічна температура цілі.

На практиці замість термодинамічної (дійсної) температури T доцільно використовувати відносну (яскравісну або радіояскравісну) температуру $T_{\text{я}} < T$, яка згідно закону Кірхгофа пропорційна термодинамічній

$$T_{Я} = \nu T, \tag{7}$$

де ν – коефіцієнт поглинання матеріалу конструкції цілі.

Тоді для теплового каналу по аналогії з (3) можна записати

$$B_f = BS_{ц}, \tag{8}$$

де B – коефіцієнт пропорціональності, який пов’язаний з поглинаючими властивостями матеріалу конструкції цілі.

Відома фундаментальна залежність

$$\nu = 1 - \rho, \tag{9}$$

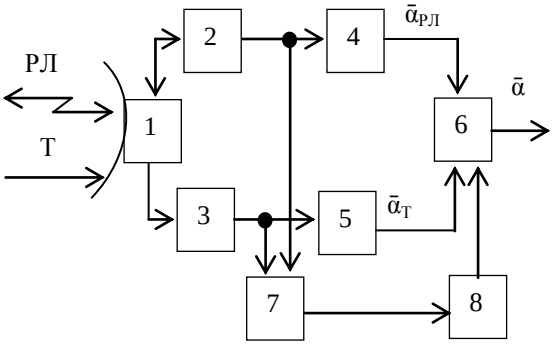
де ρ – коефіцієнт відбиття матеріалу конструкції цілі.

Ця обставина з урахуванням виразів (3) і (8) дозволяє розглядати активні радіолокаційні і теплові зображення цілі як “позитив” і “негатив” відповідно.

Вищеперераховане дає підставу стверджувати, що єдиним ефективним шляхом забезпечення інваріантності характеристик контура самонаведення ракети до знаку цілефонового контрасту є застосування мультиспектральної ГСН, координатор цілі (КЦ) якої утримує в крайньому разі два парціальних спектральних канала – радіолокаційний і тепловий (радіотепловий).

Ключовим схемоконструкторським завданням є забезпечення взаємоюстірованої в просторі і взаємосинхронної по часу роботи парціальних спектральних каналів. На

практиці це досягається єдиною електродинамічною схемою діаграмоутворення. Структурна схема КЦ, нечутливого до знаку цілефонового контрасту, представлена на рис. 1 (в α-площині самонаведення).



1 – єдиний діаграмоутворюючий пристрій радіолокаційного (РЛ) і теплового (Т) каналів;
2 – прийомопередавач РЛ каналу;
3 – приймач Т каналу;
4, 5 – пеленгатори РЛ і Т каналів відповідно;
6 – блок формування мультиспектральної оцінки;
7 – аналізатор цілефонового контрасту;
8 – блок формування вагових коефіцієнтів пеленгаторів $G_{РЛ}$, $G_{Т}$

Рисунок 1 – Загальна структурна схема КЦ, нечутливого до знаку цілефонового контрасту

Алгоритм роботи блоку формування мультиспектральної оцінки

$$\hat{\alpha} = G_{РЛ}\hat{\alpha}_{РЛ} + G_T\hat{\alpha}_T, \tag{10}$$

де $\hat{\alpha}_{РЛ}$, $\hat{\alpha}_T$ – парціальні оцінки кутової координати цілі; $G_{РЛ}, G_T \in [0;1]$ – вагові коефіцієнти, що формуються на основі аналізу цілефонового контрасту.

На етапах створення і відпрацювання ракетного озброєння важливу роль має методологія моделювання цілефонової обстановки (ЦФО). Стосовно багатоспектрального моніторингу вона включає:

- методику аналітичного представлення полів, які формуються елементами формоутворюючої поверхні цілі в парціальних каналах;
- методику трансформації візуальної моделі спостерігаємої цілі в математичну модель формування напруженості (інтенсивності) електромагнітного поля в "картинній площині" спостереження з урахуванням впливу атмосфери;
- формування діаграм зворотного розсіювання (ДЗР) цілей в радіолокаційному каналі, який володіє цілодобовістю, всепогідністю і найбільшою дальністю дії.

Поле цілі, що спостерігається, є суперпозицією напруженостей (для когерентного випадку) або інтенсивностей (для некогерентного випадку) полів, які формуються елементами формоутворюючої поверхні цілі

$$E(x,y,z) = \sum_{n=1}^{N} \frac{A}{R_n^2}\delta_n(a_n,\beta_n,\lambda)\exp[2\mu R_n + i(2kR_n - \omega t)], \tag{11}$$

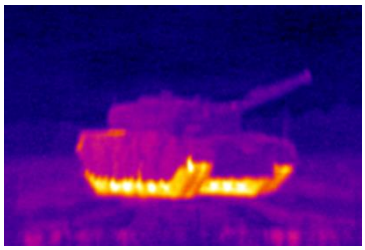
$$I = \sum_{n=1}^{N} I_n \exp[\mu(\lambda)R_n], \tag{12}$$

де δ_n – ДЗР елемента цілі; A – амплітуда зондуючого сигналу; μ – коефіцієнт прозорості атмосфери; k – хвильове число; ω – кругова частота зондуючого сигналу; I_n – інтенсивність випромінювання n-го елемента цілі (ефективна температура); R_n – похила дальність до елемента формоутворюючої поверхні цілі.

На рис. 2 представлені парціальні зображення типового наземного об'єкта – в тепловому і фотоконтрастному каналах в "картинній площині", в радіолокаційному каналі дальністний "портрет".

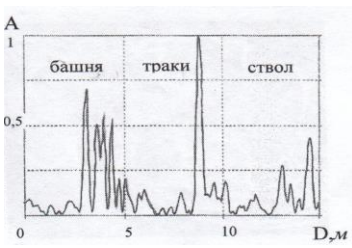
Загальну ідею моделювання цілефонової обстановки ілюструє рис. 3.

Опорним є оптичне зображення в центрі рис. 3, елементи якого конвертуються в полігональну модель у вигляді кінцевої сукупності елементарних відбивачів (випромінювачів) з визначеним набором електродинамічних особливостей.



а) тепловий канал

б) фотоконтрастний канал



в) радіолокаційний канал

Рисунок 2 – Парціальне зображення типового наземного об’єкту

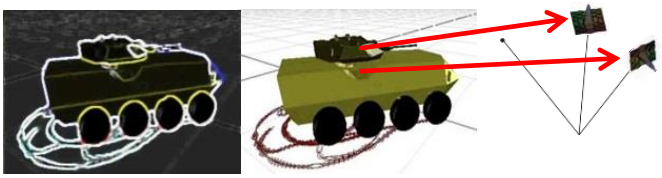
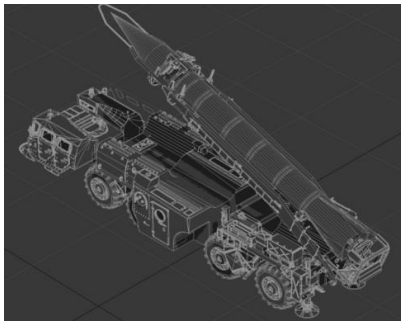


Рисунок 3 – Моделювання цілефонової обстановки

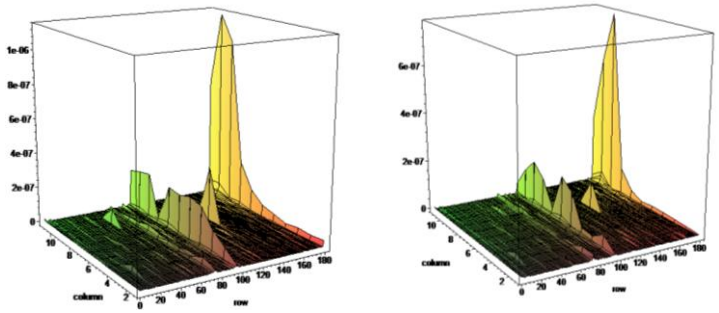
На наступному етапі полігональна модель імпортується в 3D модель цілі у вигляді трикутних примітивів, які орієнтовані у просторі і утримують всю інформацію про матеріал формоутворюючої поверхні (коефіцієнт відбиття, коефіцієнт поглинання і ін.). Фінішними етапами є:

- формування розподілень напруженості (інтенсивності) електромагнітного поля в “картинній площині” спостереження з урахуванням впливу атмосфери;
- формуванням ДЗР об’єкта, що спостерігається, шляхом зміни точки спостереження.

Оскільки радіолокаційний канал в багатоспектральній системі спостереження є базовим було виконано моделювання ДЗР типових наземних об’єктів (залізничний міст, ракетна пускова установка, вертоліт) в діапазонах радіочастот 35 ГЦ і 95 Гц на відстанях 1000 м при кутах візування по тангажу 75-85 кут. град, по рисканню 0-180 кут. град, характерних для ділянки самонаведення ракет. На рис. 4 в якості ілюстрації представлені полігональна модель ракетної пускової установки і її ДЗР на частотах 35 Гц, 95 Гц. На ДЗР чітко проявляються характерні конструктивні елементи цілі.



а) частота 35 ГГц



б) частота 95 ГГц

Рисунок 4 – Полігональна модель пускової установки, її ДЗР

В середовищі Maple 15 створені масиви даних з кроком 1 кут. градус і отримані матриці розміром 181×11, які можуть бути використані для обґрунтування структури і характеристик систем мультиспектрального моніторингу.

Таким чином:

1. Інваріантність характеристик самонаведення ракет до величини і знаку цілефонового контрасту об’єктів, що спостерігаються, забезпечується шляхом мультиспектральної обробки сигналів, що приймаються, по розробленому адаптивному алгоритму.
2. Усі елементи адаптивної мультиспектральної системи самонаведення допускають технічну реалізацію.

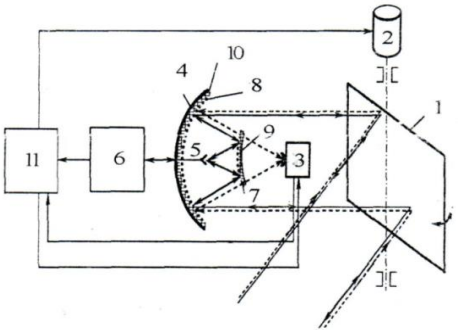
3. Розроблена методологія моделювання багатоспектральної цілефонової обстановки, яка забезпечує на початкових етапах проектування оцінку енергетичних і точністних характеристик системи самонаведення.

Д'яков А. В., Зубков А. М., Щерба А. А., Петлюк І. В.

ПРИЛАДНЕ ОСНАЩЕННЯ БАГАТОСПЕКТРАЛЬНОГО ЛОКАЦІЙНОГО МОНІТОРИНГУ

Методом максимуму правдоподібності синтезовано оптимальні алгоритми багатоспектральної обробки локаційних сигналів для всіх етапів дистанційного моніторингу – виявлення, вимірювання координат та розпізнавання об'єктів. Вказані алгоритми інваріантні до методу локації (активна, пасивна, напівактивна) та фізичному принципу побудови сенсору – радіо, оптичний, тепловий. Оптимізація побудови багатоспектральної апаратури дистанційного моніторингу із врахуванням важливого практичного обмеження – мінімізація ваго-габаритних характеристик, яке є ключовим для бортової апаратури мобільних об'єктів, безсумнівно представляє науково-практичний інтерес. При цьому, комплексування каналів спостереження, що передбачає інформативне поєднання на виході каналів, не дозволяє досягнути визначеної мети внаслідок відсутності просторового взаємоюстування та часової синхронізації парціальних каналів.

Підґрунтям методики інтеграції парціальних спектральних каналів локаційного спостереження є можливість поєднання апертурних частин радіо- і теплового каналів в рамках єдиної конструкції на основі принципів метричної оптики. Інтегрована радіотеплова система представлена на рис. 1. Радіолокаційний канал працює в міліметровому діапазоні (ММД) з міркувань мінімізації вагогабаритних характеристик із збереженням високої кутової роздільної здатності.



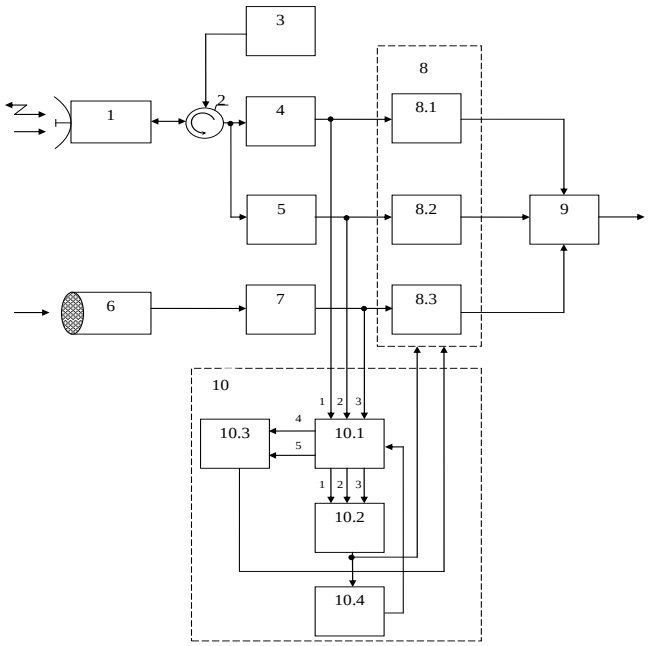
1 – плоске скануюче дзеркало;
2 – управляючий електропривод;
3 – приймач теплового випромінювання ІЧ діапазону;
4 – параболічне дзеркало;
5 – багатомодовий випромінювач ММД;
6 – когерентно-імпульсний приймач-передавач;
7, 8 – печатні поляризаційні фільтри;
9 – гіперболічна підкладка;
10 – параболічна підкладка;
11 – блок управління, обробки і синхронізації

Рисунок 1 – Інтегрована радіотеплова оглядова система

Розвитком системи є доповнення її когерентно-імпульсною РЛС формування радіолокаційних зображень (РЛЗ) – елемент 6 на рис. 1. РЛЗ уявляє собою "дальністний портрет" об'єкту, що спостерігається. В цьому випадку у блоці 11 формується трьохвимірне зображення об'єкту, що спостерігається, з врахуванням " портрету" цілі в "картинній" (такою що перпендикулярна лінії візування цілі) площині, отриманого за рахунок високої кутової роздільної здатності приймача теплового випромінювання інфрачервоного (ІЧ) діапазону.

Принциповим питанням локаційного моніторингу є забезпечення інваріантності характеристик виявлення, вимірювання координат та розпізнавання до параметрів цілефонового контрасту (ЦФК).

Кількісно ЦФК характеризується відношенням сигнал/завада+внутрішній шум (ОСПШ) на вході відповідного парціального каналу. Розроблена методика адаптації багатоспектральної локаційної системи до величини і знаку ЦФК. Структурна схема двоспектрального виявляча наземних об'єктів з адаптацією до ЦФК представлена на рис. 2.

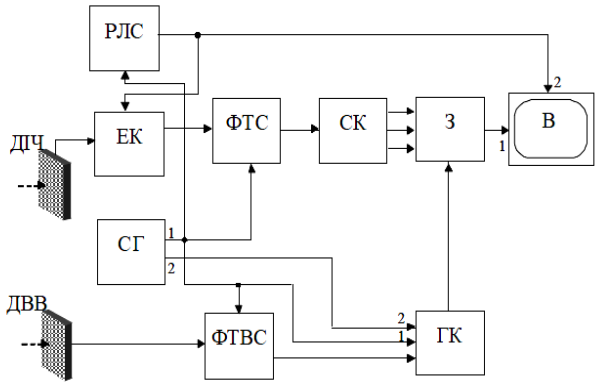


1 – антена РЛ каналу;
2 – циркулятор розв'язки "прийом-передача";
3 – передавач РЛ каналу;
4,5 – приймачи активного і радіометричних каналів;
6, 7 – об'єктів та приймач ІЧ каналу;
8 – керовані ключі;
9 – блок виявлення;
10 – аналізатор завадової обстановки;
10.1 – керований комутатор;
10.2, 10.3 – блок вибору сигналу по максимуму;
10.4 – блок керування комутаторами

Рисунок 2 – Двоспектральний виявляч

Слід відмітити, що активний радіолокаційний канал – з однієї сторони, та радіометричний з інфрачервоним (тепловим) каналом – з другої сторони, з позиції формування РЛЗ можуть розглядатися як "позитив" і "негатив". Фізично це поясняється теми обставинами, що в активному радіолокаційному каналі джерелом інформації про спостережний об'єкт є розсіяний металевою формоутворювальною поверхнею сигнал, а в тепловому (радіотепловому) каналі джерелом є випроменені нагрітим фізичним тілом сигнали, які характеризують діелектричний матеріал.

Подальшим розвитком практики багатоспектрального моніторингу є розробка системи для визначення фізичних характеристик спостережних об'єктів. Спосіб визначення теплофізичних характеристик об'єктів при дистанційному моніторингу та систему для його реалізації ілюструє рис. 3.



ДІЧ – детектор інфрачервоного випромінювання;
ДВВ – детектор видимого випромінювання;
ЕК – електронний ключ;
СГ – синхрогенератор;
ФТС – формувач тепловізійного сигналу;
ФТВС – формувач телевізійного сигналу;
СК – синтезатор кольору;
З – змішувач;
В – кольоровий монітор;
ГК – генератор контурів

Рисунок 3 – Структура системи визначення теплофізичних характеристик об'єктів

Призначення каналів: інфрачервоний – аналіз розподілення теплового контрасту на поверхні об'єкту, який спостерігається; телевізійний – формування контуру об'єкту в "картинній" площині; радіолокаційний – формування зображення об'єкту у розрізі.

Ключовим елементом системи моніторингу є багатоспектральний обтікач. Основні вимоги до якого: низькі втрати у всіх діапазонах; міцність конструкції; можливість серійного виробництва.

В табл. 1 представлено на рівні переваг та недоліків основні фізичні характеристики матеріалів, придатних для моно і багатоспектральних обтікачів. Якісна оцінка парамет-

рів по п’ятибальній шкалі (за виключенням питомої ваги) представлена в круглих скобках. Пріоритет належить кварцу і алмазу. Але технологічні труднощі отримання обтікачів значних розмірів і висока вартість стимулює до пошуку матеріалів обтікачів з полімерних і композитних матеріалів.

Таблиця 1

Порівняльні фізичні характеристики матеріалів обтікача

Матеріал обтікача	Питома вага (г/см^3)	Діелектрична проникність	Тангенс втрат /35ГГц	Прозорість в ІЧ діапазоні	Міцність при зсуві (psi)	Твердість по Кнушу (кг/мм^2)	Макс. короткочасний нагрів, град С^0
Багатоспектральні (ММД+ІЧ)							
Сульфід цинку ZNS	4,05	8,35 (3)	0,0024 (4)	(5)	18 (3)	350 (3)	370 (3)
Селенід цинку ZnSe	5,16	8,98 (2)	0,0017 (4)	(5)	8 (2)	150 (3)	315 (3)
Шпінель $MgAl_2O_4$	3,68	9,19 (3)	0,0002 (5)	(4)	28 (3)	1650 (5)	980 (5)
Кварц SiO_2	2,20	3,75 (5)	0,0004 (5)	(3)	8 (2)	600 (4)	1100 (5)
Нітрид кремнію Si_3N_4	3,18	6,1 (4)	0,0006 (5)	(2)	90 (5)	2200 (5)	1500 (5)
Алмаз С	3,52	5,7 (4)	<0,0004 (4)	(2)	400 (5)	8800 (5)	1900 (5)

Виходячи із вищесказаного можна зробити наступні висновки:

1. На сьогодні існує науково-технологічний доробок для практичного впровадження методів багатоспектрального моніторингу для вирішення широкого кола загальнотехнічних та спеціальних задач.

2. Відпрацьовано питання технічної реалізації систем дистанційного моніторингу та їх складових частин

УДК. 538.3

Софієнко І. І., Василюк Ю. С., Зінченко Я. В.

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ЕКРАННИХ КОНСТРУКЦІЙ ІЗ СУЧАСНИХ БУДІВЕЛЬНИХ МАТЕРІАЛІВ

На сьогоднішній день одним з основних видів пасивного технічного захисту інформації є екранування електромагнітних хвиль. Перелік будівельних матеріалів, що ефективно екранує електромагнітні поля широкого діапазону частот, обмежений. Так, дослідження показують, що такі будівельні матеріали як цегла, бетон, шлакоблоки в тім або іншому ступені послабляють електромагнітну енергію. Істотно більш ефективним для захисту інформації, завдяки підвищеній електропровідності, є мінерал шунгіт і будівельні матеріали на основі шунгітових порід: цегла, розчин для кладки, конструкційний бетон, штукатурна мастика. З метою підвищення екранування недавно створений новий клас будівельних матеріалів – радіоекрануючі магнезіально-шунгітові сухі будівельні суміші (МШБС). Радіоекрануючі суміші призначені для облаштування підлоги й оштукатурювання стін. До складу сумішей, що випускаються, входять натуральні компоненти, такі як шунгіт (наповнювач), магнезит (в’яжуче) і бішофіт (затверджувач). На

сьогоднішній день екрануючі властивості матеріалів на основі шунгітових порід мало вивчені: є лише часткові результати експериментальних досліджень окремих зразків при нормальному падінні плоских електромагнітних хвиль.

В доповіді приведені екрануючі властивості матеріалів на основі шунгіта при проходженні різних типів інформаційних електромагнітних полів розсіювання й виявлення найнебезпечніших каналів витоку інформації при використанні шунгітових конструкцій. Результати проведених розрахунків підтверджують, що електропровідність МШБС практично визначається електропровідністю шунгіта, який входить до його складу. Магнезіально-шунгітовий будівельний матеріал володіє переважно радіопоглинаючими властивостями. Переваги споруд на основі магнезіально-шунгітових будівельних матеріалів полягають у тому що, в них суміщаються не тільки екрануючі, але й конструкційні властивості, що дозволяє створювати спеціальні будівельні конструкції із застосуванням традиційних будівельних технологій. Традиційні матеріали (цегла, розчин для кладки, конструкційний бетон), які мають такий же коефіцієнт екранування, що й «Альфапол ШТ-1» повинні мати в кілька разів більшу товщину покриття в порівнянні із МШБС. Внаслідок цього, екранування традиційними будівельними матеріалами громіздке, при їх використанні важко забезпечити герметичність екрана. МШБС є немагнітними матеріалами, не знижують природне магнітне поле Землі. Поєднання в одній споруді конструкційних і екрануючих властивостей значно знижує терміни введення таких екранованих приміщень в експлуатацію. Екрануючі штукатурні суміші наносяться по звичайній будівельній технології. МШБС не містять цементу, мають ряд позитивних будівельних властивостей, таких як безпильність, маслобензостійкість, морозовитривалість, пожежобезпечність, висока адгезія з різними матеріалами, у тому числі з металом. МШБС задовольняють основним гігієнічним вимогам: не виділяють небезпечних газів і запахів, відповідають першому класу по радіаційній безпеці.

Яновський П. О.,. Луценко О. К., Целіщев І. О.

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СИСТЕМІ ОХОРОНИ ПРАВОПОРЯДКУ

Прискорення науково-технічного прогресу в умовах сучасної глобалізації світових процесів розглядається як основний резерв підвищення ефективності функціонування нашого суспільства. У поліпшенні життєвого рівня громадян, стабільності економічного розвитку держави одне із провідних місць посідає інформатизація суспільства і виробничих процесів. В результаті кропіткої роботи в цьому напрямку здійснюється розробка і впровадження в економічні і суспільні відносини автоматизованих систем управління (АСУ) різного спрямування. Досвід експлуатації наявних на даний момент часу автоматизованих систем показує, що вони є ефективним засобом поліпшення організації управління підприємств різних галузей економіки, підвищення ефективності їх функціонування та забезпечення високого матеріального і фінансового рівня населення.

На сучасному етапі розвитку інформаційного суспільства визначна роль належить інформаційним технологіям, стратегічне значення яких неухильно підвищується, в тому числі і й сфері забезпечення правопорядку. Про це свідчать дані за період з 1995 р. до 2018 р. про рівень злочинності в Україні, за яким визначають комфорт і якість життя в різних регіонах держави. Найбільша кількість злочинів (на 10000 осіб) відбувається у Запорізький області та в містах Києві та Севастополі, рівень злочинності по Україні в цілому за період більше ніж 20 років не зменшився. За величиною рівня злочинності області відрізняються одна від одної. Простежується тенденція до збільшення кількості злочинів у східних областях у порівнянні із західними. Характерним є те, що рівень злочинності дуже значний у містах з великою кількістю населення: в Києві, Харкові,

Одесі, Миколаєві та Львові. Крім того, значний рівень злочинності характерний областям, які межують із непідконтрольною територією ОРДЛО. Лише в м. Дніпро спостерігається тенденція до зменшення кількості злочинів.

Природно, як свідчать результати статистичних даних, на кількість правопорушень впливає рівень економічного розвитку різних регіонів держави, а отже і добробут населення. Крім того, має місце зв'язок між рівнем доходу і рівнем злочинності. Виявилося в областях із меншим рівнем доходу людей відповідно менший рівень правопорушень. Суттєве скорочення кількості здійснених злочинів в останні роки в Луганській та Донецькій областях пояснюється збільшенням кількості правоохоронців та посиленням контролю з їх боку за цивільним населенням.

З метою зниження рівня злочинності в регіонах і великих містах України важливо удосконалювати і розвивати існуючі інформаційні технології (ІТ) для зберігання, оброблення і поширення повної, достовірної і своєчасної інформації про переміщення (внутрішня і зовнішня міграція) осіб не лише в східних областях держави, а і по всій Україні для всіх працівників системи правопорядку. Сучасні інформаційні технології в системі правопорядку повинні враховувати новітні досягнення і вимоги до їх розробки. Вони повинні створювати інформацію нової якості про стан об’єкта (переміщеної особи) з врахуванням його динаміки в часі. ІТ повинна надавати інформацію такого рівня, який буде забезпечувати об’єктивну оцінку і встановлення ступеня її придатності в підтримці необхідного рішення, що сприятиме формуванню по Україні комфортного для населення правопорядку.

Розвиток ІТ слід здійснювати завдяки розширенню доступу до них громадян, що буде забезпечувати більш високий рівень комунікації поліцейських з населенням для проведення сумісної роботи по попередженню злочинності, що підвищуватиме довіру в суспільстві до правоохоронних органів і зміцнюватиме їх авторитет.

Кульбашевський В. А., Яновський П. О., Малиш А. Г.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В БОРОТЬБІ З РЕЙДЕРСТВОМ

Важливий принцип функціонування системи правопорядку щодо захисту прав громадян є публічність в її діяльності та наукова організація роботи із постійним залученням громадян, що ґрунтується на широкому використанні сучасних методів побудови інформаційних систем (ІС). Сучасні ІС складних соціально-економічних процесів дають можливість всебічно врахувати наявні елементи випадковості в їх протіканні, сприяють виявленню системних закономірностей, врахування яких забезпечує реалізацію ефективних режимів їх функціонування.

Використання інформаційних технологій (ІТ) в правоохоронній сфері держави в значному ступені надає можливість враховувати вплив на рівень злочинності багатьох важливих факторів: значне зубожіння населення, зростання рівня безробіття, відсутність економічного розвитку в суспільстві, посилення культурної деградації людей, довготривала війна з Росією на сході нашої держави, постійне зростання корупції на всіх рівнях влади, відхід в державі від системних моральних принципів та інше. Важливим є ще те, що в державі влада не проявляє ініціативи проведення системної роботи з комплексного вирішення нагальних проблем всього суспільства. Тому ситуація із зниженням рівня злочинності в Україні за роки незалежності, як свідчать дані державної статистики, не покращується.

В Україні щорічно кількість рейдерських захоплень зростає, що порушує принципи вільного суспільства і, особливо, законне право громадянина на власність. Відповідно до статистичних даних Генеральної прокуратури України із 2014 р. кількість рейдерських за-

хоплень в державі щорічно збільшується. Найбільша їх кількість була в 2017 р. – 414 захоплень, найменша в 2014 р. – 234 захоплення. Дані ГПУ свідчать, що найбільша їх кількість за останні 5 років сталася в Києві і Київській області (397 захоплень), на другому місці Дніпропетровська (133) і Львівська (104) області, найменша у Сумській області. До 50 захоплень було зафіксовано у 13 областях, і до 100 захоплень у 9 областях.

Слід відзначити, що реальна статистика, як правило, відрізняється від статистичних даних ГПУ тому, що через корупцію, як вважають українські юристи, по рейдерським захопленням переважно кримінальні провадження не порушуються. Порушення здійснюється по іншим статтям кримінального кодексу: хуліганство, самоуправство, незаконне поводження із зброєю та інше. Як свідчить практика, рейдерство пов'язано із діями реєстраторів або судовими рішеннями через зміну майнових прав, складу засновників або керівників підприємств. Для наведення належного порядку в захисті прав громадян на власність необхідно:

- створити по регіонам держави прозорі ІС з можливістю доступу до їх роботи громадян;
- передбачити в кожній ІС можливість реєструвати всі випадки рейдерства та інші порушення закону не лише представниками правоохоронних органів, а і громадянами, громадськими організаціями;
- в ІС необхідно оприлюднювати звіти посадових осіб правоохоронних органів по кожному випадку рейдерства з детальними доказами при відхиленні кримінального провадження;
- підвищити відповідальність працівників правоохоронних органів при фіксації в ІС деталей досудового розслідування, усунувши їх корегування в процесі дослідження справи і не кваліфікаційні дії в роботі сторони звинувачення щодо збирання доказів з метою зміцнення доказової бази для обвинувачення під час судових засідань та винесення справедливих вироків.

Плужніков Б. О., Яновський П. О., Марценюк С. О.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЗАБЕЗПЕЧЕННІ ДІЯЛЬНОСТІ СИЛОВИХ СТРУКТУР ВЕЛИКОГО МІСТА

З розвитком суспільно-економічних процесів в умовах розбудови ринкових перетворень в Україні протягом трансформаційного періоду рівень злочинності по країні в цілому і по регіонах суттєво не зменшився. Це стосується як областей, так і міст і поселень. Східним областям держави притаманний більший рівень злочинності, ніж на заході України. В західних областях кількість правопорушень на 10000 осіб, як правило, не перевищує 100, а в східних – перебільшує 100, а інколи – більше 200 злочинів (Запорізька область). У великих містах (Київ, Харків, Одеса, Миколаїв, Львів) рівень злочинності більший, ніж у малих та середніх містах. Найбільшою кількістю правопорушень характеризується місто Київ, що пояснюється не лише великою кількістю населення, а і наявністю у жителів міста значної кількості переваг соціально – економічного характеру, що вимагає особливої уваги щодо розвитку і впровадження сучасних інформаційних технологій для підтримки своєчасного і якісного прийняття рішення працівниками правоохоронних органів (ІТПР).

Більш широке використання ІТПР в управлінні правоохоронних систем у великих містах держави сприяє створенню більш комфортних умов життя нашого населення. Мета використання ІТПР – пошук шляхів найбільш ефективного управління складною динамічною проблемою правового життєзабезпечення суспільства. Динамічність системи в суспільстві означає наявність постійних змін її параметрів в часі і в просторі в кількісному і якісному вимірі, спроможність її складових і в цілому до змін свого стану і розвитку.

Аналіз результатів статистичних даних по адміністративних районах м. Києва свідчить, що райони мають суттєві відмінності не лише за кількістю населення, а і відрізняються кількістю скоєних правопорушень, яка залежить від наявності об'єктів, де здійснюється більшість порушень закону (вокзалу, ринку та інші). Як правило, для міста характерні такі правопорушення: крадіжки, пограбування, шахрайство, хуліганство, хабарництво. Найпоширенішими є майнові злочини (крадіжки). В середньому за рік в місті буває 30-35 тисяч крадіжок і пограбувань. По адміністративним районам міста кількість крадіжок і пограбувань за рік розподіляється таким чином: із 10 районів в одному районі скоїться більше 4 тисяч; в чотирьох районах – більше 3 тисяч; в трьох районах – більше 2 тисяч і в двох районах – трохи більше 1 тисячі правопорушень.

Такий нерівномірний розподіл правопорушень між районами одного великого міста свідчить, що правоохоронні системи районів мають відмінності в побудові баз даних та їх опрацюванні. Структура їх повинна враховувати реальну динаміку правопорушень і в кожному районі необхідно реалізовуватися свої інформаційні технології ІТПР з врахуванням оперативної динаміки правопорушень. Такі технології мусять базуватися на нових методах збирання і аналізу інформації, які зараз розробляються в нашій державі і набувають свого поширення. Враховуючи ту обставину, що сучасними інформаційними технологіями в теперішній час оснащується і кримінальне середовище, важливо, використовуючи ІТПР, упроваджувати потужні інформаційно-пошукові системи. Також необхідно, щоб впроваджувані ІТПР спрощували інформаційно-аналітичну роботу, прискорювали проведення і підвищували її якість, здійснювали систематизацію та аналіз великого обсягу інформації, допомагали проводити пошуки альтернативних рішень, швидко та об'єктивно оцінювати ситуацію і приймати обґрунтовані рішення.

Яременко В. В., Яновський П. О., Фомуляєв А. В.

ОСОБЛИВОСТІ ІНФОРМАТИЗАЦІЇ ПРАВОВОГО ПРОЦЕСУ В БОРОТЬБІ З НЕЗАКОННИМ ЗАВОЛОДІННЯМ АВТОМОБІЛІВ

Для управління будь-яким процесом потрібно реалізувати велику швидкість і високу точність розрахунків його параметрів, завдяки чому можна обґрунтувати раціональну організацію роботи і досягти високі результати в діяльності органу. Крім того, для отримання належного рівня результативності в роботі певної правоохоронної структури слід використовувати сучасні інформаційні технології (ІТ) для прогнозування характеру протікання оперативного процесу в найближчому майбутньому та здійснювати якісне планування роботи його підрозділів і співробітників. Тому рівень сучасних ІТ повинен бути таким, щоб сприяв швидкому виявленню, якісному розслідуванню конкретних злочинів і попередженню та недопущенню правопорушень.

В умовах переходу нашого суспільства на ринкові відносини змінюється структура і характер правопорушень, що значно ускладнює роботу оперативних працівників та слідчого апарату. Тому постало питання про застосування ІТ в оперативно-розшуковій і слідчій роботі для активізації вирішення проблем в правоохоронній діяльності. Як свідчать результати аналізу даних Національної поліції України, протягом 2018 року в державі було зафіксовано 4092 випадки незаконного заволодіння автомобілями. Як правило, викрадають дешеві автомобілі моделей ВАЗ і Daewoo та дорогі німецькі і японські машини марки Toyota, Mercedes і Honda. В порівнянні з 2017 роком в 2018 році було викрадено на 592 автомобіля менше. У великих містах покращення з викраденням автомобілів не спостерігається. Найгірший стан з викраденням автомобілів має місце в м. Києві (у 2018 р. на столицю припало 25% випадків від загальної кількості по державі). Найбільшою проблемою для нашої столиці є недостатня кількість спеціальних майданчиків для паркування, що змушує власників порушувати встановлені правила.

Слід відзначити, що показник розкриття таких злочинів знаходиться на дуже низькому рівні в Україні в цілому. Так, на початку 2019 року було знайдено 766 автомобілів, а повернуто власникам лише 250 (32,6% від загальної кількості).

Причини викрадення автомобілів, що слідує із реальних даних, у великих містах: встановлення власниками на свої авто спрощених систем сигналізації та їх безпечність; розвиненість дорожньої інфраструктури з великою кількістю в русі автомобілів та зручністю швидко покинути місце злочину; великі неохороняємі стоянки біля торговельно-розважальних центрів і біля багатоповерхівок – місць проживання власників; відсутність паркувальних майданчиків і відеоспостереження; бездіяльність правоохоронних структур і органів влади.

Для суттєвого покращення ситуації із викраденням автомобілів потрібна співпраця власників, правоохоронних структур і органів державної влади. Тому, як вважають експерти, ефективно проблему захисту власних автомобілів в державі можна вирішити комплексно за участю всіх співучасників експлуатації автотранспорту: власників, правоохоронців і органів державної влади, що дасть змогу реалізувати багаторівневу систему захисту. Особливо слід звернути увагу на впровадження в практику удосконалених ІТ, більш складних в порівнянні з існуючими. Мається на увазі впровадження в ІТ такого програмного забезпечення з обладнанням автомобілів, яке б забезпечувало одночасне надходження сигналів в правоохоронні органи і власнику у випадку незаконного проникнення крадія в чужий автомобіль. Сучасний рівень електронної техніки і програмних продуктів не визиває ніяких складнощів в реалізації такого рішення.

Ткаченко В. А., Яновський П. О., Іващенко Т. М.

АСПЕКТИ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПРАВООХОРОННИХ ОРГАНІВ У ГАЛУЗІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Прискорення слідчо-пошукових дій органами правопорядку з якісним результатом можливо завдяки використанню сучасних інформаційних технологій (ІТ), які повинні враховувати постійні зміни як в кримінальному середовищі, так і удосконалення правового поля держави, тенденції та пріоритети подальшого розвитку законодавства у відповідності з державним курсом до ринкової економіки і європейської інтеграції. Враховуючи ту обставину, що рівень злочинності в Україні за роки незалежності не покращується, необхідно, щоб система підготовки фахівців для органів правопорядку могла забезпечувати формування методичної і організаційної основи також у галузі інформаційних технологій.

Система підготовки фахівців повинна враховувати складові компетентностей майбутнього працівника, що надасть йому можливість успішно працювати в різних підрозділах правопорядку. Досягнення його готовності до практичної діяльності забезпечується наданням йому якісної характеристики широкого спектру особливостей не лише професійної юридичної підготовки спеціаліста, а і знань інформаційних технологій. Тим більше, відомо, як свідчить реальна практика правоохоронної системи, навичками інформаційно-аналітичної роботи повинні володіти не лише співробітники спеціальних правоохоронних підрозділів, а й усі без винятку працівники, які займаються оперативно – розшуковою роботою.

Використання нових технічних засобів і технологій кримінальними особами підвищує рівень їх кримінальної діяльності, що спонукає нас до розробки більш ефективних методів збирання й аналізу великого обсягу інформації, нових спеціальних технічних засобів з розширеними можливостями. Також вже розпочато впровадження аналітичної моделі поліцейської діяльності, проводяться різноманітні операції і розслідування лише

на підставі оперативно-аналітичної інформації, здійснюється оснащення спеціальних підрозділів комплексами комп'ютерної і аналітичної роботи.

Але наявність недоліків в системі запобігання злочинів вимагає реалізувати якісно нові підходи до підготовки фахівців для правоохоронної системи з використанням сучасних інформаційних технологій, врахувавши наступне:

- підготовка фахівців повинна ґрунтуватися на реалізації системного підходу, завдяки якому забезпечувалась би збалансованість рівня роботи правоохоронної системи в цілому і кримінального середовища, а в результаті мало б місце випередження в діяльності виконання правоохоронцями всіх технологічних, технічних, інформаційних, правових і оперативно – розшукових заходів з високою результативністю їх роботи;
- використовувані в практиці і підготовці фахівців і узгоджені із законодавчим полем ІТ повинні повністю виключати незаконні втручання в роботу правоохоронних органів сторонніх осіб;
- підготовка фахівців має забезпечувати високий рівень знань не лише правового напряму, а і технічного та інформаційного, тому що на даний час створюються спеціальні комплекси для аналітичної і комп'ютерної розвідки і здійснюється оснащення ними спеціальних підрозділів поліції;
- спорядити технічними засобами і забезпечити доступ до баз даних МВС та інших державних органів незалежно від місця перебування співробітників для виявлення схожих злочинів та взаємодію між різними оперативними відділеннями МВС міста для ідентифікації схожих злочинів, що допоможе в їх швидкому розкритті.

Яновський П. О., Яновська Т. Г., Маліновський А. В.

КОМПРОМІСНЕ УПРАВЛІННЯ ЛОГІСТИЧНОЮ ЛАНКОЮ «ПРАВОПОРЯДОК - ТОРГІВЛЯ» В ПРИМІСЬКИХ ЗОНАХ ВЕЛИКИХ МІСТ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Відсутність координації діяльності різних підприємств, органів влади і великого бізнесу не забезпечує досягнення найкращого результату для держави і наших громадян та великого успіху в забезпеченні соціальної стабільності. Так, при вирішенні важливої задачі для населення, яке проживає у невеличких містечках і селах (ОТГ), тобто в приміських зонах міст, практично не відпрацьовується взаємодія правоохоронних органів із організаціями сфери обслуговування (торгівлею). Вивчення цієї проблеми та її вирішення особливо загострюється в сучасних умовах підвищеного безробіття в сільській місцевості, вимушених щоденних поїздок жителів приміських дільниць на роботу транспортом у великі міста.

Результати проведеного анкетування людей свідчить, що кожна людина із передмісць в місті заробляє щомісяця в середньому 11 тис. грн. Зрозуміло, що якась частина цих коштів витрачається по місцю роботи, а більша їх частина – за місцем проживання сімей (в сільській місцевості), в межах від 38% до 82% – тобто в середньому 60%.

Для економічного піднесення сільських регіонів необхідно забезпечити взаємодію місцевих органів державної влади, правоохоронних органів, місцевих структур з надання населенню сервісних послуг завдяки побудові і реалізації систем компромісного управління системами правопорядку і торгівлі, що забезпечить сталий і поступальний розвиток передмість великих міст, розвиток їх інфраструктури, якісне надання всього комплексу сервісних послуг населенню, в тому числі і безпеки та збереження особистого майна громадян та матеріальних цінностей підприємств торгівлі. При відпрацюванні систем компромісного управління в конкретній ОТГ логістичною ланкою «Правопорядок – Торгівля» слід розробити і впровадити комплексну інформаційну технологію (КІТ), яка буде забезпечувати ефективну взаємодію взаємозалежних підсистем: правоо-

хоронних органів і торгівлі. Така система повинна накопичувати інформацію в повному обсязі функціонування кожної з них.

Довготривала криза змінила структуру населення і товарів в сільських закладах торгівлі. В сільській місцевості весь товарообіг поділяється в залежності від ціни товару і характеру його споживання по двум періодам – зимовий та літній. Набір товарів, як слідує із даних роботи підприємств торгівлі, відрізняється в літній і зимовий період року. Взимку більшим попитом користуються горілчані вироби та м'ясні продукти, влітку – одяг, взуття та слабоалкогольні напої. Такі товари представляють найбільшу цінність для певної категорії громадян. Завдяки довготривалій кризі в державі пройшло велике розшарування в ОТГ населення. Катастрофічне безробіття, особливо в сільській місцевості вплинуло на появу особливої групи людей, які потенційно спрямовують свої дії на порушення закону. До них легко приєднуються особи із міста, які звільнилися з закладів позбавлення волі і лишаються без роботи. Об'єктами їх злочинних дій є магазини в сільській місцевості, у яких часто відсутня візуальна охорона та надійна сигналізація.

Для зниження кількості правопорушень в ОТГ необхідно впроваджувати сучасні інформаційні технології (ІТ) в правоохоронних структурах із обов'язковим наданням їм автоматично інформації щодо структури товарів від закладів торгівлі. З використанням такої інформації система буде допомагати в формуванні відповідних рекомендацій правоохоронцям щодо прийняття необхідних рішень з метою попередження правопорушень.

УДК 621.391

Lysechko V., Yanina Yu.

PROCEDURE FOR DETERMINATION OF SUBCARRIER FREQUENCIES` POSITIONS

This research is aimed at solving the problem of increasing the frequency resource utilization in the cognitive radio network. To solve this problem, it is proposed to use the method of determining the coincidence of frequency subcarriers based on the method QOFDM.

The principle of zero orthogonal access at subcarrier frequencies is based on the principle of zero orthogonality between frequency positions. One of the problems in signal generation using the proposed method of quasiorthogonal access at subcarrier frequencies - Quasiorthogonal frequency-division multiplexing (QOFDM) – is the task of determining the frequency positions that coincided when paired comparisons of frequency plans. Due to the large number of subcarrier frequencies in each band of the ensemble, these frequencies can overlap, so, obviously, certain positions of the subcarrier frequencies may coincide.

It is necessary to determine the places of coincidence of frequency positions between different signals of the same ensemble, which coincided when comparing frequency plans with each other.

The coincidence coefficient is defined as the integral over the interval of the frequency band F_i to F_j of the product of the *i-th* and *j-th* frequency plans with a sampling step Δ_j. The coefficient of coincidence will be calculated by the formula (1):

$$B_{ij}(\Delta f) = \int_{F_1}^{F_2} S_i(\Delta f_i) \cdot S_j(\Delta f_i - \Delta_j) d\Delta f, \quad (1)$$

where Δ_j - the sampling frequency step in the *j-th* frequency plan.

The following condition (2) must be fulfilled:

$$B_{ij}(\Delta f) \le \frac{1}{\sqrt{N_i \cdot N_j}}, \quad (2)$$

Consider the method of determining the location of the coincidence of frequency positions in different ensemble signals.

Matched frequency positions are determined in pairs by expression (3):

$$F_{ij} = \sum_{k=1}^{n_i} \Delta f_{ik} = \sum_{m=1}^{n_j} \Delta f_{jm}, \quad (3)$$

where F_{ij} – the frequency position that coincided with the pairwise comparison of the *i-th* and *j-th* frequency plans;

k – the number of subcarriers in the *i-th* frequency plan;

m – the number of subcarriers in the *j-th* frequency plan;

$\sum_{k=1}^{n_i} \Delta f_{ik}$ – the sum of the frequency intervals of the *i-th* frequency plan to the subcarrier, which coincided with the subcarrier *j-th* frequency plan;

$\sum_{m=1}^{n_j} \Delta f_{jk}$ – the sum of the frequency intervals of the *j*-th frequency plan to the subcarrier, which coincided with the subcarrier *i-th* frequency plan.

The system of equations (4) must be solved for four signals.

Frequency positions will coincide when the equations are the same.Let $k = a$ and $m = b$.Then the expression (4) for the paired plans will look like (5):

$$\begin{cases} F_{12} = \sum_{k=1}^{n_i} \Delta f_{1k} = \sum_{m=1}^{n_2} \Delta f_{2m}, \\ F_{13} = \sum_{k=1}^{n_i} \Delta f_{1k} = \sum_{m=1}^{n_3} \Delta f_{3m}, \\ F_{14} = \sum_{k=1}^{n_i} \Delta f_{1k} = \sum_{m=1}^{n_4} \Delta f_{4m}, \\ F_{23} = \sum_{k=1}^{n_2} \Delta f_{2k} = \sum_{m=1}^{n_3} \Delta f_{3m}, \\ F_{24} = \sum_{k=1}^{n_2} \Delta f_{2k} = \sum_{m=1}^{n_4} \Delta f_{4m}, \\ F_{34} = \sum_{k=1}^{n_3} \Delta f_{3k} = \sum_{m=1}^{n_4} \Delta f_{4m}. \end{cases} \quad (4)$$

$$\begin{cases} a \cdot \Delta f_{1a} = b \cdot \Delta f_{2b} = F_{12}, \\ a \cdot \Delta f_{1a} = b \cdot \Delta f_{3b} = F_{13}, \\ a \cdot \Delta f_{1a} = b \cdot \Delta f_{4b} = F_{14}, \\ a \cdot \Delta f_{2a} = b \cdot \Delta f_{3b} = F_{23}, \\ a \cdot \Delta f_{2a} = b \cdot \Delta f_{4b} = F_{24}, \\ a \cdot \Delta f_{3a} = b \cdot \Delta f_{4b} = F_{34}. \end{cases} \quad (5)$$

From expression (5) we express the numbers of coincident frequency subcarriers a of the first frequency plan in the pair being compared – expression (6) and coincident frequency subcarriers b of another frequency plan in a pair that is compared (7):

$$\begin{cases} a = \frac{b \cdot \Delta f_{2b}}{\Delta f_{1a}}, \\ a = \frac{b \cdot \Delta f_{3b}}{\Delta f_{1a}}, \\ a = \frac{b \cdot \Delta f_{4b}}{\Delta f_{1a}}, \\ a = \frac{b \cdot \Delta f_{3b}}{\Delta f_{2a}}, \\ a = \frac{b \cdot \Delta f_{4b}}{\Delta f_{2a}}, \\ a = \frac{b \cdot \Delta f_{4b}}{\Delta f_{3a}}. \end{cases} \quad (6)$$

$$\begin{cases} b = \frac{a \cdot \Delta f_{1a}}{\Delta f_{2b}}, \\ b = \frac{a \cdot \Delta f_{1a}}{\Delta f_{3b}}, \\ b = \frac{a \cdot \Delta f_{1a}}{\Delta f_{4b}}, \\ b = \frac{a \cdot \Delta f_{2a}}{\Delta f_{3b}}, \\ b = \frac{a \cdot \Delta f_{2a}}{\Delta f_{4b}}, \\ b = \frac{a \cdot \Delta f_{3a}}{\Delta f_{4b}}. \end{cases} \quad (7)$$

This way you can determine the frequency positions that match the different signals.

To illustrate the operability of the proposed method, an example is presented, which presents the simulation results for which 50 frequency plans included in the signal ensemble were selected. The calculations were performed with the values of the bandwidth parameter ΔF = 15 MHz and 20 MHz with the subchannel width Δs = 15 kHz. The number of frequency subcarriers varies from 23 to 512. The frequency plans are paired in comparison.

Thus, the value of the correlation coefficient r_{ij} of the two compared frequency plans was calculated. On the basis of the obtained results, those frequency plans that gave the worst values in the calculation of the correlation coefficient, namely r_{ij}> 0,1, were removed.

In Figure 1, the correlation coefficient does not exceed the allowable value. This is achieved by removing frequency plans from the ensemble.

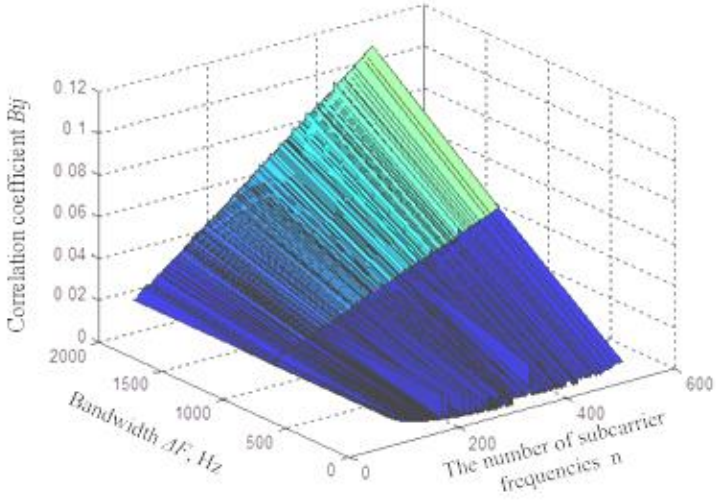


Figure 1 – Graph of correlation coefficient of pairwise comparison of frequency plans on the number of frequency subcarriers and on the bandwidth ΔF = 20 MHz before removal of frequency plans from the ensemble

Thus, we can conclude that the minimum similarity of the two compared plans is achieved when the value of the bandwidth ΔF = 20 MHz. The method of determining the frequency positions that coincide when paired comparing frequency plans allows to simplify the process of formation of frequency plans and to reduce the level of intra-system interference that occur when multiple users use the same frequency bands in cognitive radio systems. This makes it possible to increase the capacity of the cognitive radio network.

Безкоровайний В. В., Сотник С. В.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ РЕІНЖИНІРИНГУ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Швидкі зміни умов функціонування сучасних організаційних, технічних і організаційно-технічних об'єктів, що використовуються у різних сферах людської діяльності, приводять до необхідності відповідних змін в їхніх структурах і системах керування ними. Основу систем керування такими об'єктами складають комп'ютерні мережі, на базі яких реалізуються функції автоматизації на різних рівнях керування [1]. Задачі реінжинірингу мереж пов'язані з суттєвою зміною множин та (або) характеристик користувачів, розширенням множини функціональних задач, удосконаленням елементної бази й (або) технологій реалізації функцій системи керування, які роблять існуючі варіанти їх організації малоефективними або неприйнятними. Корпоративні комп'ютерні мережі являють собою територіально (просторово) розподілені об'єкти, рішення з реін-

жинірингу для яких визначаються за результатами розв'язання комплексу задач їх структурної, топологічної, параметричної та технологічної оптимізації.

На першому етапі створюється загальний формалізований опис мережі, який відображає взаємозалежність між функціональним ефектом від реінжинірингу та витрачених на нього ресурсів (витрат) $Q = F(C)$, де Q і C приведені скалярні оцінки ефекту і витрат; F – оператор, що відображає стратегію використання ресурсів (варіант реінжинірингу). Вибір стратегії здійснюється з урахуванням мети реінжинірингу, характеристик існуючої мережі та наявних ресурсів за результатами системологічного аналізу проблеми. На цьому етапі задача пошуку найкращого варіанту побудови мережі серед допустимих $s^o \in S*$ подається в узагальненій формі [2]:

$$s^o = arg \underset{Q,C,F}{opt} \Theta(Q, C, F), \quad (1)$$

де $opt\,\Theta$ – оператор, що відображає обраний критерій ефективності реінжинірингу.

З урахуванням встановлених обмежень на показники необхідного ефекту від реінжинірингу мережі $Q(s) \geq Q*$ або допустимих витрат $C(s) \geq C*$ задача (1) деталізується та може бути подана у такій формі:

$$s^o = arg \max_{s \in S*}(Q(s)/C(s) : Q(s) \geq Q*,\ C(s) \leq C*). \quad (2)$$

Частковими, широко поширеними на практиці випадками задачі (2), є задачі вибору варіанту $s^o \in S*$, що максимізує ефект від реінжинірингу в умовах обмежень на витрати ресурсів $C(s) \geq C*$ або мінімізує витрати на досягнення необхідного ефекту $Q(s) \geq Q*$.

За результатами системологічного аналізу проблеми встановлюється структура технології реінжинірингу мережі [3]:

$$CirDes = <Tasks, InDat, Res, DesDec, ProcDec>, \quad (3)$$

$$Tasks = \{Task_i\},\ i = \overline{1,6}, \quad (4)$$

де $Tasks = \{Task_i\},\ i = \overline{1,6}$ – упорядкована множина задач визначення принципів побудови мережі, оптимізації структури, топології, параметрів елементів і зв'язків, технології функціонування, оцінки ефективності і вибору найкращого варіанту реінжинірингу $s^o \in S*$; $InDat$ – множина вхідних даних задач; Res – множина обмежень задач; $DesDec$ – множина проектних рішень; $ProcDec$ – відображення у вигляді проектної процедури (методу розв'язання), що ставить у відповідність кожній парі $< InDat_i, Res_i >$ непусту підмножину $DesDec_i, i = \overline{1,6}$.

З точки зору інформаційних технологій кожна з задач є перетворювачем вхідних даних у вихідні $Task_i : InDat_i \rightarrow OutDat_i,\ i = \overline{1,6}$.

Упорядкована множина задач (4) вважається повністю розв'язною, якщо для всіх задач $Tasks = \{Task_i\}$ існують проектні процедури $ProcDec_i,\ i = \overline{1,6}$ і кожен розв'язок є єдиним $\left|ProcDec_i(< InDat_i, Res_i >)\right| = 1,\ i = \overline{1,6}$.

При цьому слід враховувати характерні особливості технології реінжинірингу корпоративних комп'ютерних мереж: тісний взаємозв'язок задач структурної, топологічної, параметричної, технологічної оптимізації, що вимагає їх спільного розв'язання; комбінаторний характер більшості задач; необхідність розв'язання задач великої розмірності; наявність в постановках задач важко формалізованих чинників; високу динамічність або невизначеність вихідних даних; широкий діапазон умов розв'язання практичних задач.

Тісний взаємозв'язок і неповна інформаційна визначеність задач за вихідними даними і обмеженнями обумовлює ітераційний характер методів і процедур реінжинірингу, що забезпечує можливість розв'язання всього комплексу задач $\{Task_i\},\ i = \overline{1,6}$ за входами.

Висока складність методів розв’язання задач проблеми (вирішальних процедур), обумовлена їх комбінаторним характером, і широкий діапазон умов їх розв’язання вимагають використання множини методів, що мають суттєво різні показники складності і точності. Це забезпечить можливість розв'язання всієї множини задач (4) за ресурсами.

Для більш повного використання досвіду проектувальників і врахування важко формалізованих чинників технології оптимізації мереж доцільно будувати на основі інтерактивних (людино-машинних) процедур, що включає взаємодоповнюючі процедури автоматичного й інтелектуального аналізу та синтезу.

На всіх етапах проектування доцільно використовувати прийоми, що знижують трудомісткість розв'язання задач оптимізації. З цією метою можуть бути використані різного роду евристики, що враховують специфіку задачі реінжинірингу, проектні рішення, отримані за допомогою «швидких» (наближених) методів, формальні або експертні оцінки.

З урахуванням особливостей задач і вимог до процедур їх розв’язання, а також аксіом системного проектування метод формування проектних рішень з реінжинірингу корпоративних комп’ютерних мереж пропонується будувати на основі ітераційних логічних схем. При цьому для кожної з задач технології має існувати множина математичних моделей, методів і алгоритмів їхнього дослідження різних рівнів деталізації, точності та складності. Відібрані (розроблені) математичні моделі, методи й алгоритми утворюють відкритий банк засобів, узгоджених за змінними та параметрами задач реінжинірингу. Це дозволяє у залежності від постановки задачі, особливостей мережі, наявних часових і обчислювальних ресурсів обирати ланцюжки ефективних засобів в межах запропонованої інформаційної технології реінжинірингу.

Список використаних джерел

1. Nesterenko, S. A. Costs evaluation methodic of energy efficient computer network reengineering [Text] / S. A. Nesterenko, J. S. Nesterenko // Праці Одеського політехнічного університету. – 2016. – Вип. 2 (49). – С. 70-75.

2. Бескоровайный, В. В. Разработка системологической модели проблемы структурно-топологического реинжиниринга систем крупномасштабного мониторинга [Текст] / В. В. Бескоровайный, К. Е. Подоляка // Восточно-Европейский журнал передовых технологий. – 2015. – №3(75). – С. 37-42.

3. Тимченко, А. А. Основи системного проектування та аналізу складних об'єктів: У 2-х кн. Кн. 1. Основи САПР та системного проектування складних об'єктів [Текст] / За ред. В. І. Бикова. – К.: Либідь, 2000. – 272 с.

УДК 519.816; 004.415.2

Перетятко М. В., Широкопетлєва М. С.

ВИКОРИСТАННЯ МЕТОДУ ЗВАЖЕНОЇ СУМИ ПРИ РЕАЛІЗАЦІЇ ПРОГРАМНОЇ СИСТЕМИ ПІДБОРУ РОБОЧИХ МІСЦЬ

На сьогоднішній день в багатьох галузях науки і техніки для прийняття рішень використовується багатокритеріальний аналіз та методи оптимізації, що дозволяють оцінити, певним чином диференціювати усі можливі рішення та отримати серед них найбільш ефективні для подальшого впровадження і використання [1, 2].

Для дослідження в рамках даної роботи було обрано задачу ранжування робочих місць на підставі вподобань користувачау відповідності до індивідуальних потреб (потреб в обладнанні, бажаних предметах, які надаються на робочому місці), встановленої важливості задоволення кожної потреби для цього користувача, та ступенем задоволення цих потреб кожним вільним робочим місцем.

Багатокритеріальний аналіз пропонує ряд методів для знаходження оптимальних рішень, серед яких можна виокремити найчастіше використовувану групу методів – методи скаляризації [3]. Сенс таких методів полягає в тому, що векторна цільова функція задачі багатокритеріальної оптимізації перетворюється в функцію зі скалярним значенням і вся задача багатокритеріальної оптимізації зводиться до задачі оптимізації з однією скалярною функцією [4, 5]. Прикладом такого методу є метод зваженої суми, саме його було обрано для вирішення досліджуваної задачі аналізу та підбору найбільш відповідних робочих місць.

Метод зважених сум полягає в наступному: на вхід подаються набір критеріїв для дослідження та додатній ваговий коефіцієнт кожного критерію(важливість), при застосуванні методу оцінка кожного критерію (ступінь вираженості) $c_i^T x$ множиться на ваговий коефіцієнт λ_i, всі k зважених критеріїв додаються один до одного та складають цільову функцію $\lambda^T Cx$(функцію, створену зваженою сумою) [6, 7]. Переваги методу зважених сум наступні:

- порівняна простота;
- можливість використання за відсутності кількісних критеріїв оцінки варіантів або складності їх отримання;
- результат не обмежується тільки найкращим варіантом, а включає ранжування за ступенем привабливості всіх досліджуваних варіантів.

Найбільшу роль у виборі методу для поставленої задачі зіграла саме можливість ранжування усіх доступних робочих місць, що складає вичерпне рішення та дозволяє, за потреби, обрати не лише найбільш відповідне місце, тобто представляє клієнту повний результат з можливістю власного незалежного вибору місця.

У поставленій для дослідження задачі критеріями виступають елементи обладнання робочого місця, а ваговими коефіцієнтами – оцінки важливості кожного елементу, виставлені користувачем. Кожне робоче місце аналізується на ступінь вираженості того чи іншого обладнання (наприклад, якщо користувач обрав критерієм наявність двох комп'ютерів, то якщо на робочому місці є лише один комп'ютер – ступінь вираженості дорівнює 0,5), отримані ступені вираженості множаться на відповідні вагові коефіцієнти важливості, всі отримані числа додаються між собою – таким чином для кожного робочого місця розраховується зважена сума критеріїв. Підраховані зважені суми порівнюються з ідеальним випадком, при якому всі елементи робочого місця присутні в потрібному обсязі, розраховується відсоток кожної зваженої суми по відношенню до ідеальної – це і є коефіцієнт відповідності робочого місця. Результатом застосування методу є повний список доступних робочих місць з відповідними коефіцієнтами відповідності.

Для впровадження рішення даної задачі було розроблено програмну систему, яка складається з серверної частини (технологія .NET Core, СКБД MS SQL), веб-клієнта (фреймворк Angular 8) та мобільного за стосунку (фреймворк Xamarin), дозволяє користувачам в інтерактивному режимі додавати бажане обладнання та інше устаткування робочого місця та оцінювати важливість кожного обраного елементу (за п'ятибальною шкалою). Для пошуку найбільш відповідного вільного робочого місця необхідно обрати будівлі (офіси). Результати представляються у вигляді ранжованого списку робочих місць із підрахованим коефіцієнтом відповідності для користувача. Після цього користувач може самостійно обрати собі робоче місце за вказаними параметрами. Розроблений програмний продукт був успішно протестований на різних наборах даних, він коректно працює та має перспективи у подальшому використанні.

Отже, в результаті проведених досліджень для рішення задачі підбору робочих місць на підставі вподобань користувача було обрано метод багатокритеріального аналізу, який найкраще враховує особливості поставленої задачі– метод зваженої суми, була знайдена відповідність між даними задачі та вхідними даними методу зважених сум і було вдало застосовано цей метод. Також метод вирішення задачі було вдало втілено в програмному забезпеченні, яке на даний момент є повністю готовим до використання.

Список використаних джерел

1. Лотов А. В. Многокритериальные задачи принятия решений. Метод достижимых целей / А. В. Лотов, И. И. Поспелова. – М.: МАКС Пресс, 2008. – 197 с.
2. Айзерман М. А. Выбор вариантов. Основы теории / М. А. Айзерман, Ф. Т. Алескеров – М. : Наука, 1990. – 237 с.
3. Дубов Ю. А. Многокритериальные модели формирования и выбора вариантов систем / Ю. А.Дубов, С. И.Травкин, В. Н. Якимец – М. : Наука, 1986. – 296 с.
4. Кини Р. Л. Принятие решений при многих критериях: предпочтения и замещения / Р. Л.Кини, Х. Райфа – М : Радио и связь, 1981. – 560 с.
5. Грешилов А. А. Математические методы принятия решений / А. А. Грешилов. – М. : Издательство МГТУ им. Н. Э. Баумана, 2014. – 648с.
6. Березовский Б. А. Задача наилучшего выбора / Б. А. Березовский, А. В. Гнедин – М. : Наука, 1984. – 196 с.
7. Бомас В. В., Судаков В. А., Афонин К. А. Поддержка принятия многокритериальных решений по предпочтениям пользователя. СППР DSB/UTES / В. В. Бомас, В. А. Судаков, К. А. Афонин. – М. : МАИ,2006. – 172 с.

УДК 358.119.1+007 + 357.3 + 355.692.32

Черноног О. О., Козубцов І. М., Жовтун А. А. Радченко М. М.

ДОСВІД ФОРМУВАННЯ ТАКТИКО-ТЕХНІЧНИХ ВИМОГ ДО КОМПЛЕКСІВ (ЗРАЗКІВ) КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ЗБРОЙНИХ СИЛ

Постановка завдання. Формування оперативно-тактичних вимог (ОТВ) та тактико-технічних вимог (ТТВ) та загальних вимог (ЗВ) до комплексів (зразків) озброєння і військової техніки Збройних сил України (ЗСУ) має дуже важливе значення під час розробки (модернізації) створення нових зразків. При цьому на етапі проектування, виникає необхідність в обґрунтуванні, ТТВ до комплексів (зразків) кібернетичної безпеки ЗСУ.

Аналіз досліджень і публікацій. Аналізуючи наукові роботи [1–4] можна встановити, що їх автори використовують різні підходи до розробки та формування ОТВ і ТТВ до озброєння та військової техніки.

Мета доповіді. Мета доповіді полягає розглянути особливості та практичний підхід до формування ТТВ до комплексів (зразків) кібернетичної безпеки ЗС.

Результат дослідження. Рішення цієї практичної проблеми вбачається наступним чином. На сьогодні керівним документом, який регламентує порядок розробки оперативно-тактичних (оперативно-стратегічних) вимог до системи та військової техніки, є «Організаційно-методичні рекомендації з формування оперативно-стратегічних і оперативно-тактичних вимог до перспективних зразків (комплексів, систем) озброєння та військової техніки» [5]. При розробці ТТВ на комплекси кібернетичної безпеки виникли складнощі із обранням структури ТТВ, оскільки в методичних рекомендаціях [5] структура ТТВ не визначена.

Таким чином, виникала необхідність у виборі логічної структури ТТВ. Виходячи з вище розглянутого нами рекомендується обрати з ГОСТ В 15.201-83 [6] за основу ТТВ наступну структуру розділів, а саме:

1 Тактико-технічні вимоги за призначення

1.1 Загальні вимоги до щодо призначення

1.2 Тактико-технічні завдання, які покладаються на виконання

1.2.1 Головні тактико-технічні завдання, які покладаються на виконання:

1.2.2 Спеціальні тактико-технічні завдання, які покладаються на виконання

1.2.3 Тактико-технічні (бойові) можливості
1.2.4 Тактичні об’єкти (цілі) дій
1.2.5 Тактичні вимоги щодо взаємодії з системами управління
1.3 Технічні вимоги до складу обладнання
1.3.1 Склад обладнання комплексу
1.4 Тактико-технічні вимоги до зразка

Розділ повинен складатися з наступних підрозділів:

- вимоги до радіоелектронного захисту;
- вимоги до живучості і стійкості до зовнішніх дій;
- вимоги до надійності;
- вимоги до ергономіки і технічної естетики;
- вимоги до експлуатації, зручності технічного обслуговування, ремонту і зберігання;
- вимоги до транспортабельності;
- вимоги до безпеки;
- вимоги до забезпечення збереження державної і військової таємниці;
- вимоги до стандартизації і уніфікації;
- вимоги до технологічності;
- конструктивні вимоги.

При необхідності припускаємо вводити і інші підрозділи.

Вимоги в кожному підрозділі розташовують залежно від ступеня їх важливості і характеру, формулюють чітко, виключаючи можливість їх неоднозначного тлумачення.

Вимоги підрозділів задають з урахуванням вимог по забезпеченню збереження державної таємниці.

Номінальні значення величин, що визначають вимоги і тактико-технічні (технічні) характеристики зразка приводять з допустимими відхиленнями або приводять їх найбільші або найменші допустимі значення. Статистичні параметри встановлюють з вказівкою рівня довірчої вірогідності, якому відповідає дане значення параметра.

Для наступного маневрування у тих випадках, коли вимоги по якому-небудь розділу, підрозділу не пред'являються, то після найменування розділу, вписують «не передбачені» або «не пред'являються».

Висновки. Авторами запропоновано рішення практичної задачі з обґрунтування структури ТТВ до комплексів (зразків) озброєння і військової техніки в частині, що стосується кібернетичної безпеки. Дане рішення не суперечить логіці побудови нормативним документам, а навпаки уніфіковує типові рішення. Доцільно доповнити відповідним розділом існуючу регламентуючу базу України в частині, що стосується кібернетичної безпеки.

Список використаних джерел

1. Гриб Д. А. Системно-концептуальні основи і елементи методології формування оперативно-тактичних і тактико-технічних вимог, що пред'являються до перспективних зразків озброєння і військової техніки та зразків, що модернізуються / Д. А. Гриб, Б. О. Демідов, М. В. Науменко // Системи озброєння і військова техніка. – Х.: ХУПС, 2009. – Вип. 2 (18). – С. 65-73.

2. Демідов Б. О. Системна методологія обґрунтування, формування та реалізації оперативно-тактичних і тактико-технічних вимог до зразків (комплексів, систем) озброєння та військової техніки / Б. О. Демідов, М. І. Луханін, М. В. Науменко // Наука і оборона. – К.: Техніка, 2011. – №1. – С. 45-50.

3. Родін І. О. Методика визначення тактико-технічних вимог до комплексів подвійного призначення на базі автономних підводних апаратів / І. О. Родін, Р. В. Вакар // Збірник наукових праць НУК. – 2012. – № 5-6. – С. 33-36.

4. Шишанов М. О. Методологія обґрунтування тактико-технічних вимог до технічних засобів відновлення / М. О. Шишанов, А. В. Гуляєв, О. В. Зубарєв, М. М. Шевцов //

Озброєння та військова техніка. 2017. №2(14). – С. 80-83.

5. Організаційно-методичні рекомендації з формування оперативно-стратегічних і оперативно-тактичних вимог до перспективних зразків (комплексів, систем) озброєння та військової техніки. – Київ: Воєнно-наукове управління ГШ ЗСУ, 2009. – 11 с.

6. ГОСТ В 15.201-83 Тактико-техническое (техническое) задание на выполнение опытно-конструкторской работы.

УДК 358.119.1+007 + 357.3 + 355.692.32

Черноног О. О., Козубцова Л. М., Терещенко Т. П., Козубцов І. М.

ПРО МОЖЛИВІСТЬ РЕАЛІЗАЦІЇ КЕРІВНИЦТВА З КІБЕРБЕЗПЕКИ НА ЗАСАДАХ NIST SPECIAL PUBLICATION 800-53 REVISION 4

Постановка завдання. З інтенсифікацією впровадження у Збройних Силах України стандартів НАТО виникла необхідність вирішенні задачі з впровадження у підрозділах кібернетичної безпеки інформаційно-телекомунікаційної системи зв'язку методики аудиту кібернетичної безпеки.

Мета доповіді. Апробувати ідею можливості реалізації у керівництві з кібербезпеки для підрозділів силових відомств методики аудиту кібербезпеки на основі NIST Special Publication 800-53 Revision 4 [1].

Результат дослідження. Авторським колективом запропоновано в основу керівництва з кібербезпеки для підрозділів силових відомств методики аудиту кібербезпеки застосувати рекомендації до NIST Special Publication 800-53 Revision 4. На думку авторів розробки NIST він полегшує вибір методів та процедур оцінки кіберзахищеності (безпеки) інформаційної системи.

Методика аудиту інформаційної безпеки реалізується наступними кроками:

Крок 1. Категоризація інформаційної системи.

Крок 2. Вибір мір заходів кібербезпеки.

Крок 3. Процедури реалізації заходів кібербезпеки.

Крок 4. Перевірка реалізованості процедур відповідно визначених заходів кібербезпеки.

Крок 5. Надання дозволу на експлуатацію інформаційної системи.

Крок 6. Моніторинг, раптові перевірки інформаційної системи.

Слід відзначити, що в початковому вигляді [1] методика аудиту кібербезпеки інформаційної системи потребує істотного переосмислення окремих кроків, які з нашого погляду потребують. а в певних діях і переопрацювання. Таке рішення випливає з розуміння відсутності логічної ціпочки документів та ідеології на яку вона опирається.

Висновки. Таким чином, можна сформулювати наступні висновки:

- ідея застосування в основі аудиту кібербезпеки інформаційної системи Збройних Сил на основі NIST Special Publication 800-53 Revision 4 є новою;
- прямий переклад NIST Special Publication 800-53 Revision 4 з англійської мови на українську не забезпечує таке ж пряме і швидке запровадження у практику, оскільки існує принципова відмінність і розуміння сутності окремих процесів;
- потребує доопрацювання з урахуванням національних особливостей.

Список використаних джерел

1. NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organization. [Electronic resource] // National Institute of Standards and Technology NIST. - Access mode URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

УДК 358.119.1+007 + 357.3 + 355.692.32

Козубцова Л. М.

АПРОБАЦІЯ СТРУКТУРИ МЕТОДИКИ ДІАГНОСТУВАННЯ КІБЕРНЕТИЧНОЇ СТІЙКОСТІ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ В КІБЕРНЕТИЧНОМУ ПРОСТОРІ

Постановка завдання. У відповідно до мети, об’єкта, предмета дисертаційного дослідження визначено часткове наукове завдання, яке формується наступним чином: обґрунтувати структуру методики діагностування кібернетичної стійкості функціонування інформаційної системи спеціального призначення в кібернетичному просторі. Як відомо функціонування об'єктів критичної інформаційної інфраструктури в новому середовищі – кіберпросторі, породжує нові уразливості і загрози, і вимагає розробки нового інструментарію забезпечення стійкості функціонування в умовах комп'ютерних атак [1].

Мета доповіді. Апробувати структуру методики діагностування кібернетичної стійкості функціонування інформаційної системи спеціального призначення в кібернетичному просторі.

Результат дослідження. В дисертаційному досліджені запропоновано в основу структури методики діагностування кібернетичної стійкості функціонування інформаційної системи спеціального призначення в кібернетичному просторі, окремі етапи методики аудиту кібербезпеки рекомендовані в NIST Special Publication 800-53 Revision 4 [2]. Порівняльні відмінностей між існуючим та запропонованим підходом до побудови методики діагностування кібернетичної стійкого функціонування інформаційної системи спеціального призначення в кібернетичному подано в табл. 1.

Таблиця 1

Порівняльні відмінностей між існуючим та запропонованим підходом до побудови методики

Існуючий підхід		Запропонований підхід	
Етап 1.	Категоризація інформаційної системи.	Етап 1.	Реалізація заходів з категоріювання ІС на елементи та компоненти.
Етап 2.	Вибір мір заходів кібербезпеки.	Етап 2.	Вибір мір заходів кібербезпеки кожному елементу, компоненті ІС.
Етап 3.	Процедури реалізації заходів кібербезпеки.	Етап 3.	Процедури з реалізації заходів кібербезпеки.
Етап 4.	Перевірка реалізованості процедур відповідно визначених заходів кібербезпеки.	Етап 4.	Діагностування рівня реалізованості процедур відповідно до визначених заходів кібербезпеки для ІС.
-	-	Етап 5.	Розрахунок показника кібернетичної стійкості функціонування ІС в кібернетичному просторі.
Етап 5.	Надання дозволу на експлуатацію інформаційної системи.	Етап 6.	Надання рекомендацій щодо подальшої експлуатації ІС.
Етап 6.	Моніторинг, раптові перевірки інформаційної системи.	Етап 7.	Епізодичний раптовий моніторинг-перевірка ІС в межах етапів 4-6.

Слід відзначити, що в початковому вигляді [2] методика аудиту кібербезпеки інформаційної системи не придатна до застосування для інформаційних систем спеціального застосування. Тому в ході дисертаційного дослідження переосмислено окремі кроки (етапи).

На кроці 5 пропонується здійснювати розрахунок показника кібернетичної стійкості

функціонування ІС в кібернетичному просторі з використанням окремих ідей [2], а семе неохідності впровадження поняття кіберстійкості, як інтегрованого показника кіберживучості, кібернадійності та кіберзахищеності. Зазначимо, що на відміну від роботи [2] показник кіберзахищеності розраховується за раніше розробленим автором методиками [3; 4]

Таке рішення випливає з розуміння відсутності логічної послідовності документів та ідеології на яку вона опирається.

Висновки. Таким чином, можна сформулювати наступні висновки:

- ідея застосування в основі методики діагностування кібернетичної стійкого функціонування інформаційної системи спеціального призначення в кібернетичному просторі на основі NIST Special Publication 800-53 Revision 4 є новою, що і визначає новизну одержаного наукового результату в дисертації;
- в рамках удосконалення існуючої методики було запропоновано здійснювати розрахунок кіберстійкості, як інтегрованого показника кіберживучості, кібернадійності та кіберзахищеності. Необхідність введення нової властивості викликана новим середовищем функціонування інформаційної системи (кіберпростір), як наслідок появою нових вразливостей і загроз. Отриманий результат, відповідно до розробленої схеми дисертаційного дослідження, дозволяє однозначно дати оцінку стану безпеки ІС від комп'ютерних атак (деструктивних інформаційних дій).

Наукова новизна полягає в запропонуванні методики діагностування кібернетичної стійкості функціонування інформаційної системи спеціального призначення в кібернетичному просторі.

Перспектива подальших досліджень доцільно націліти на удосокналення математичного апарату розрахунку показників кіберживучості та кібернадійності інформаціної системи.

Список використаних джерел

1. Захарченко Р. И., Королев И. Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. – Т. 10. – № 2. – С. 52 – 61. doi 10.24411/2409-5419-2018-10041.

2. NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organization [Electronic resource] // National Institute of Standards and Technology NIST. - Access mode URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

3. Козубцова Л. М., Куцаєв В. В., Терещенко Т. П. Методика оцінки кібернетичної захищеності системи зв’язку організації // Сучасні інформаційні технології у сфері безпеки та оборони. – 2018. – №1 (31). – С. 43 – 46.

4. Куцаєв В. В., Радченко М. М., Козубцова Л. М., Терещенко Т. П. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв’язку // Збірник наукових праць ВІТІ. – К.: ВІТІ, 2018. – № 2. – С. 67 – 76.

УДК 004.49

Штонда Р. М., Куцаєв В. В., Терещенко Т. П.

DDOS-АТАКИ ЯК ЗАСОБИ ВПЛИВУ НА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

В даний час захист Веб-ресурсів інформаційно-телекомунікаційних систем військового призначення від DDoS-атак є найбільшою проблемною серед більшості завдань по забезпеченню безпеки кібернетичного простору. По результатам аналізу матеріалів, які опублікова-

ні в ряді видань, що стосуються безпеки Internet-ресурсів та кібернетичної безпеки, в останні роки спостерігається постійне збільшення кількості DDoS-атак, і збитків від них [1, 2].

Метою DDoS-атак є переповнення буфера атакованого комп'ютера, сервера інформаційно-телекомунікаційної системи в результаті чого вони перестають відповідати на будь-які запити і просто "виснуть". DDoS-атаки широко використовуються для отримання доступу до атакованих пристроїв і запуску на них коду. Також часто застосовуються недобросовісними конкурентами, оскільки DDoS-атака не є дорогим заходом, а ось усунення її наслідків може потребувати багато фінансів і часу.

Для того щоб уявити наскільки велику загрозу представляє DDoS-атака, слід зазначити, що таку атаку спроможний навіть провести старшокласник. Так вона за масштабом буде не значна, скоріше за все інформаційно-телекомунікаційні системи військового призначення вона атакувати не зможе, але кожна людина розуміє: що якщо чим більше відбувається таких DDoS-атак на певну інформаційно-телекомунікаційну систему тим більше ймовірностей, що до таких атак підключаться більш досвідчені зловмисники, які спроможні задати шкоди.

Переважно DDoS-атака може бути інструментом для проведення незаконних дій, наприклад, зловмисники можуть провести DDoS-атаку, як маневр який відволікає увагу під час проведення цільової кібернетичної атаки. Кібернетична атака в свою чергу може представляти серйозну загрозу інформаційно-телекомунікаційній системі військового призначення через складність виявлення та наслідки які вона спроможна заподіяти. В середньому, виявлення таких DDoS-атак відбувається через 200 днів після їх початку та не завжди закінчується позитивним результатом.

За звичай проведення DDoS-атаки залежить від можливостей зловмисника, але існують класичні види DDoS-трафіка, розглянемо їх:

- HTTP-запити, за допомогою таких запитів користувач працює в системі. Основою HTTP-запиту є HTTP-заголовок. Зловмисники мають такі заголовки, чим затрудняють виявлення таких атак;
- HTTP(S) GET-запит – метод, який знаходить інформацію в системі. HTTP(S) GET-флуд – метод DDoS-атаки, при якому особа яка атакує інформаційно-телекомунікаційну систему посилає потужний потік запитів до системи з цілю переповнення її ресурсів. Як результат інформаційно-телекомунікаційна система стає не працездатною;
- HTTP(S) POST-запит – метод, при якому дані розміщуються в тіло запитів для наступної обробки в інформаційно-телекомунікаційній системі. HTTP(S) POST-флуд – це тип DDoS-атаки, при якому кількість POST-запитів переповнюють інформаційно-телекомунікаційну систему так, що дана система не в стані відповісти на всі запити;
- також один із самих небезпечних методів – коли зловмисник відправляє підроблений ICMP-пакет в якому його адрес замінена на адресу об'єкта атаки. SYN-флуд та UDP-флуд.

На даний час зловмисники навчилися ускладнювати алгоритми атак разом з цим стали популярні бот-мережі, комбінація різноманітних методів атак, при цьому не завжди використовують максимальні свої можливості, їх можуть залишити для подальших атак на інформаційно-телекомунікаційну систему. На ринку України існує безліч засобів та систем, які мають експертні висновки та призначені для відбиття DDoS-атак.

Виділимо методи протидії DDoS-атакам навіть якщо в інформаційно-телекомунікаційній системі встановлені засоби та системи протидії DDoS-атакам а саме [3]:

- пошук фахівців по DDoS та подальше їх включення до штатів підрозділів;
- постійне підвищення кваліфікації особового складу підрозділів та навчання на курсах щодо захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах;
- побудова розподілених систем;
- використання систем та комплексів моніторингу;
- взаєморозуміння між керівництвом та підлеглими.

Існує безліч засобів, способів та методів протидії DDoS-атакам. Кожний з них має свої переваги, недоліки та особливості застосування. Але на даний час не існує доско-

налого засобу, способу чи методу протидії DDoS-атакам. Зловмисники з кожним днем удосконалюють свої вміння та навички щодо проведення таких атак. Теоретично хотілось б зазначити, що об'єднання способів, методів та уміле використання особовим складом підрозділів засобів протидії DDoS-атакам дасть можливість вчасно виявляти та протидіяти атакам із мінімальними втратами інформації, що циркулює в інформаційно-телекомунікаційних системах військового призначення. Ви не перший і не останній, хто зіткнеться з DDoS-атакою, і в ваших силах, керуючись своїми знаннями, звести наслідки атаки до мінімуму.

Список використаних джерел

1. Кібербезпека в інформаційному суспільстві інформаційно-аналітичний дайджест за 2018 рік. Науково-дослідний інститут інформатики і права Національної академії правових наук України, Національна бібліотека України імені В. І. Вернадського.

2. Кібербезпека в інформаційному суспільстві інформаційно-аналітичний дайджест за 2019 рік. Науково-дослідний інститут інформатики і права Національної академії правових наук України, Національна бібліотека України імені В. І. Вернадського.

3. Пеньков В. І. Методи та засоби протидії шкідливому програмному забезпеченню./ В. І. Пеньков, Р. М. Штонда, О. М. Гук, І. Р. Мальцева, Ю. О. Черниш // – К. НУОУ Сучасні інформаційні технології у сфері безпеки та оборони № 2(29), 2017. С. 58-64.

Коротченко Л. А, Радзівілов Г. Д.

ПРОБЛЕМНІ ПИТАННЯ ОРГАНІЗАЦІЇ ЗВ'ЯЗКУ З БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

В останні декілька років спостерігається зростаючий інтерес до безпілотних літальних апаратів (БПЛА), це обумовлено можливістю ефективно вирішувати за допомогою їх завдання як у військовій так і в цивільній сфері.

При розробці і в процесі експлуатації БПЛА виникають питання щодо організації зв'язку.

Основними такими питання при організації зв'язку між наземним пунктом управління (НПУ) і БПЛА, особливо на великих відстанях, є:

- відсутність прямої радіовидимості між НПУ і БПЛА, вплив рельєфу місцевості на дальність прямої радіовидимості;
- забезпечення електромагнітної сумісності радіоелектронного обладнання на БПЛА, обмеження потужності радіопередавальних пристроїв БПЛА;
- залежність діаграми направленості антенних систем, під час польоту БПЛА;
- зменшення якості радіолінії під час високошвидкісної передачі даних з БПЛА (відеоінформації);

Шляхами вирішення зазначених питань:

- збільшення висоти підйому антени НПУ і польоту БПЛА;
- оптимальне розміщення бортового обладнання та антен на БПЛА;
- використання в складі НПУ антен направленої дії;
- використання супутникових систем зв'язку;
- використання ретрансляційного обладнання.

Як правило, для організації зв'язку НПУ – БПЛА використовують два радіоканали:

- дуплексний: для прийому-передачі командно-телеметричної інформації;
- симплексний: для передачі корисної (фото-, відео-) інформації з БПЛА на НПУ.

Виходячи з їх призначення, до них висуваються різні вимоги. Так, щодо пропускної спроможності, радіоканал прийому-передачі командно-телеметричної інформації повинен бути не більше 256 кбіт/с; радіоканал передачі корисної інформації (цільове навантаження) не менше 5 Мбіт/с.

Для організації радіозв'язку прямої видимості широко застосовують антени направленої дії з активними фазовими антенними решітками (АФАР). Перевагами АФАР є, що при швидкому скануванні частот в широкому спектрі, можливо сформувати задану діаграму направленості. Це дасть можливість системі автоматичного керування (САК) НПУ постійно супроводжувати БПЛА в просторі і автоматично підналаштовуватись. Для підвищення швидкодії та динамічної точності САК діаграмою направленості АФАР пропонується покращити показники якості перехідних процесів. Для покращення показників запропоновано синтез розімкнутого зв'язку комбінованої системи та синтез диференціального зв'язку, що виконані у відповідності з умовами зменшення динамічної, середньоквадратичної помилки та підвищення швидкодії системи автоматичного керування. Результати досліджень можуть бути використані для оцінки показників під час побудови АФАР.

УДК 621.391

Штомпель М. А.

АНАЛІЗ ОСОБЛИВОСТЕЙ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ З КОМУТАЦІЄЮ ПАКЕТІВ

Необхідність впровадження сучасних інформаційних послуг призводить до широкого розповсюдження телекомунікаційних мереж з комутацією пакетів, що побудовані на основі стеку протоколів TCP/IP. При цьому постійно зростають вимоги щодо забезпечення рівня інформаційної безпеки у даних телекомунікаційних мережах.

Однією з актуальних задач при організації захищеної передачі даних у телекомунікаційних мережах на основі стеку протоколів TCP/IP є виявлення атак та запобігання їх впливу на працездатність мережі. Для цього використовуються системи виявлення вторгнень, які можна розділити на такі види:

- мережеві системи виявлення вторгнень, що розташовуються на межі двох мереж;
- системи виявлення вторгнень окремого вузла, що аналізують потік даних, який надходить на конкретний сервер;
- системи виявлення вторгнень хосту, що розгортаються на заданому хості мережі.

Ефективність систем виявлення вторгнень залежить від компонентного складу та технологій, що використовуються при їх технічній реалізації. При цьому ключову роль при побудові даних систем відіграє модуль виявлення атак, що може бути реалізований з використанням різних підходів та процедур.

Проведені дослідження показали, що перспективними є підходи до аналізу даних на основі експертної оцінки та машинного навчання. Показано, що для вирішення задачі виявлення атак можуть бути використані методи, що засновані на математичному апараті статистичного аналізу, кластерного аналізу, нейронних мереж, імунних мереж, опорних векторів, експертних систем та сигнатур.

Сутність методів виявлення вторгнень з використанням процедур статистичного аналізу полягає у порівнянні поточного стану телекомунікаційної мережі з набором ознак типового стану мережі. Розвиток даного підходу лежить в основі методів на основі кластерного аналізу, що передбачає розбиття ознак на окремі групи та визначення нетипових екземплярів, що признаються вторгненнями.

З іншого боку, у класі методів, що засновані на сигнатурах та експертних оцінках, здійснюється порівняння екземпляру з наявними прикладами та заданими правилами, що зберігаються у деякій базі знань.

Новітнім підходом до виявлення вторгнень у телекомунікаційних мережах є застосування методів, заснованих на принципах та процедурах машинного навчання. Наприклад,

методи на основі нейронних мереж передбачають можливість використання різних моделей мереж, таких як радіально-базисні мережі, рекурентні мережі, карт Кохонена тощо, для виявлення вторгнень шляхом проведення відповідного навчання мережі. Методи на основі імунних мереж передбачають формування антитіл за різними критеріями та створенні імунних детекторів для визначення вторгнень. У методах, що засновані на процедурі опорних векторів, здійснюється класифікація екземплярів шляхом застосування лінійно роздільних множин, побудованих з використанням відповідних правил.

За результатами аналізу визначено, що застосування технологій машинного навчання при реалізації модулю виявлення атак дозволяє отримати достатньо хороші показники ефективності. Перспективним напрямом подальших досліджень є отримання кількісних показників щодо обчислювальної складності технічної реалізації модулю виявлення атак на основі різних процедур машинного навчання.

УДК 621.396.4

Бойко В. Н.

ИСПОЛЬЗОВАНИЕ РАДИОТЕХНИЧЕСКИХ СИСТЕМ КОМАНДНО-ИЗМЕРИТЕЛЬНОГО КОМПЛЕКСА В ЗАДАЧАХ РАСПОЗНАВАНИЯ КОСМИЧЕСКИХ АППАРАТОВ

Использование наземных радиотехнических средств (НРТС) для контроля космической обстановки является одним из путей дальнейшего совершенствования комплекса обзора космического пространства. Применения НРТС в совокупности со средствами обработки информации позволяет расширить возможности комплекса.

Введение указанной информации в контур обработки системы контроля космической обстановки приводит к улучшению его характеристик. Действительно, получение фото- и радиоизображений космических объектов позволяет наиболее полно решать задачи идентификации космических аппаратов (КА). Методы получения изображений, являются наиболее информативными и обеспечивают наибольшую оперативность контроля в условиях значительной априорной неопределенности. Однако получение изображения при помощи наземных средств часто весьма затруднено или вообще невозможно. В такой ситуации особое значение приобретает использование наземных радиотехнических систем для приема и обработки радиосигналов идентифицируемых космических объектов.

Каждый тип космических объектов использует различные виды радиосигналов, структуры кодовых последовательностей, частоты излучения. Кроме того, характерные особенности каждого КА появляются на уровне вторичных признаков сигнала: формы фронтов и спадов огибающей дрейфа несущей частоты, глубины модуляции паразитных составляющих спектра и т.д. Выделение совокупности признаков и особенностей сигнала совместно с данными слежения за параметрами движения КА позволяют с высокой вероятностью поэкземплярно идентифицировать объекты в течение сравнительно небольшого интервала времени.

Тем не менее, возможности анализа радиосигналов космических аппаратов военного назначения ограничиваются временем, отводимым на информационный объем между бортами идентифицируемого космического объекта и наземной станции. Необходимо отметить, что такой анализ затрудняется в связи с проведением информационного обмена в области космического пространства в непосредственной близости от командно-измерительной системы. Поэтому излучения каналов информационного обмена идентифицируемых космических объектов, как правило, не попадают в зону радиовидимости НРТС.

Следовательно, наиболее реальным путем использования НРТС с целью получения информации для комплекса контроля космической обстановки является их работа с «молчащими» РТС.

Любой технически исправный КА, находящийся на орбите, является источником излучений, которые будем называть неконтролируемыми (НКИ). К таким излучениям относятся «просачивания» через антенно-фидерный тракт приемной антенны сигнал бортовых гетеродинов приемника, шумы переключений электронных и электронно-механических устройств, излучения, вызываемые работой бортовых ЭВМ, а также излучения по боковым лепесткам бортовых антенн, направленных в сторону спутников-ретрансляторов. Очевидно, что наиболее мощными будут излучения по боковым лепесткам передающих антенн и НКИ бортовых гетеродинов.

Применение НРТС является целесообразным лишь в том случае, если оно с достаточной степенью надежности за сравнительно небольшой интервал времени позволяет идентифицировать КА. Поэтому НРТС и приданные ей средства обеспечения должны удовлетворить следующим требованиям:

1) Временные затраты на выделение характерных признаков космического объекта должны быть существенно меньшими, чем при использовании КА-инспекторов и КА-наблюдателей.

2) Алгоритмы идентификации КА по НКИ с использованием наземных средств могут быть целесообразными и работоспособными в условиях, где другие средства неработоспособны.

3) Интегральные материальные затраты также должны быть сравнительно небольшими.

4) Тактико-технические характеристики НРТС должны обеспечивать прием весьма слабых сигналов НКИ в широком диапазоне.

5) Информационно-вычислительные средства, связанные с НРТС, могут обеспечить обработку поступающей информации в масштабе времени, близком к реальному.

6) Программное и алгоритмическое обеспечение вычислительного комплекса, работающего с НРТС, должно быть ориентировано на решение задач идентификации.

Заметим, что включение НРТС в комплекс контроля дает возможность применять меньшее количество КА–инспекторов, что в свою очередь, ведет к существенной экономии средств и разгрузке систем информационного обеспечения и управления КА.

Очевидно, что выполнение указанных требований приведет к улучшению таких системных показателей комплекса контроля космической обстановки, как оперативность и вероятность выполнения задачи. Получение количественных соотношений, определяющих влияние показателей системы на характеристики комплекса является весьма сложной задачей. Поэтому в качестве показателя оперативности идентификации и её качества следует использовать отношение временных интервалов идентификации с использованием НРТК к интервалам идентификации другими средствами и вероятность идентификации за фиксированное время, соответственно.

Специфические требования к НРТС вызывают необходимость использовать для задач идентификации уникальные, по современным понятиям, радиотехнические средства. Если бы таких средств не было, то материальные затраты на их создание сделали бы, по всей видимости, нецелесообразным применение НРТС для идентификации КА. Но в настоящее время созданы и функционируют средства, удовлетворяющие перечисленным требованиям. Этими системами являются радиотехнические станции информационно-вычислительные средства командно-измерительного комплекса.

Список использованных источников

1. Инженерный справочник по космической технике / Под ред. А. В. Солодова. – М. : Воениздат, 1969. – 696 с.

2. Справочник по радиолокации. Радиолокационные устройства и системы . Том 3 / Под ред. А. С. Виницкого. – М. : Сов. радио, 1978. – 528 с.

3. Космическое оружие: дилемма безопасности / Под ред. Е. П. Велихова, Р. З. Сагдеева, А. А. Кокошина. – М. : Мир, 1986. – 182 с.

4. Проектирование оптических систем / Под ред. Р. Шеннона. – М. : Мир, 1983. – 420с.

5. Радиосистемы межпланетных космических аппаратов / Под ред. А. С. Виницкого. – М. : Радио и связь, 1993. – 328 с.

6. Радиотехнические системы / Под ред. Ю. М. Казаринова. – М. : Высшая школа, 1990. – 496 с.

УДК 621.317

Бурцева В. В., Григорчук Р. В., Крихтін Ю. О.

РЕЗУЛЬТАТИ АНАЛІЗУ МОЖЛИВОСТІ ОНОВЛЕННЯ ПАРКУ ВИСОКОЧАСТОТНИХ ВОЛЬТМЕТРІВ

Серед ВЧ вольтметрів, які застосовуються у військових метрологічних лабораторіях, найбільшого поширення набули діодні компенсаційні вольтметри типу В3-49. Широкі частотний та динамічний діапазони дозволяють їх застосовувати під час проведення повірки (калібрування) електронних вольтметрів змінного струму, генераторів НЧ та ВЧ сигналів не тільки в стаціонарних умовах, але й на виїзді. Перевагою даних вольтметрів є те, що в діапазоні частот до 30 МГц точність вимірювання не залежить від частоти сигналу. Вольтметри, які мають достатню стабільність метрологічних характеристик, використовуються як робочі еталони 1-го або 2-го розряду з поправочними коефіцієнтами для компенсації систематичних похибок, обумовлених впливом частоти та рівня сигналу; інші – використовуються як робочі ЗВТ. На даний час більшість таких вольтметрів вичерпали свій ресурс та вважаються морально й фізично застарілими і потребують ремонту. Проте через відсутність комплектуючих (в першу чергу, ламп 6Д24Н) відновити їх на даний час неможливо.

Виходячи з цього, було проаналізовано сучасні ВЧ вольтметри іноземного виробництва, серед яких заслуговують особливої уваги одноканальні та двоканальні радіочастотні вольтметри Boonton серії 9240. Їх перевагою є малі споживча потужність, маса та габарити, що спрощує їх транспортування під час виконання робіт на виїзді. У ході аналізу з'ясовано, що сумарне значення відносної похибки вольтметра з ВЧ зондом 952001 (діапазон частот від 10 кГц до 1,2 ГГц) з урахуванням основної похибки, а також частотного та температурного ефектів складає: у діапазоні частот від 10 кГц до 100 МГц приблизно від 3 % до 5 %, у діапазоні частот від 100 МГц до 1 ГГц – від 5 % до 7 %, у діапазоні частот від 1 ГГц до 1,2 ГГц – від 9 % до 11 %. Конструктивна сумісність між вольтметром Boonton та вітчизняним ЗВТ, що підлягають повірці (калібруванню), забезпечується замовленням набору ЗІП (аксесуарів) 952063, до складу якого входять: ВЧ зонд 952001, адаптер 50 Ом BNC(F) 95200201B, подільник напруги 100:1 95200501A, накінечник для зонда 95200401A та кабель для зонда завдовжки 1,5 м.

Наприклад, на даний час відповідно до стандарту на методи і засоби повірки ВЧ генераторів ДСТУ ГОСТ 8.322:2008 вимоги до точності під час визначення опорної напруги ВЧ генераторів складають від 4 % до 6 % у діапазоні частот від 50 кГц до 30 МГц, на інших – не більше 10 %. Замість застарілих вольтметрів, які передбачено застосовувати згідно стандарту, пропонується використовувати вольтметр Boonton 9241 з ВЧ зондом 952001 для роботи в діапазоні частот від 10 кГц до 1,2 ГГц, точність якого цілком відповідає встановленим у стандарті нормам.

Результати аналізу метрологічних характеристик вольтметра Boonton 9241 з НЧ зондом 952064 (для роботи в діапазоні частот від 10 Гц до 100 МГц) показали, що мінімальне значення його сумарної похибки становить 6 %. Відповідно до вимог стандарту на

методи і засоби повірки НЧ генераторів ДСТУ ГОСТ 8.314:2008 необхідне співвідношення границь основної похибки вольтметра та генератора сигналів НЧ допускається не більше ніж 1:3. У разі використання вольтметра Boonton серії 9240 разом з НЧ зондом 952064 дане співвідношення не виконується.

З метою отримання висновків щодо інших можливих варіантів застосування вольтметрів Boonton серії 9240 пропонується провести декілька їх калібрувань протягом року для визначення поправочних коефіцієнтів та оцінити довгострокову нестабільність їх метрологічних характеристик.

Дуболазов Ю. О., Коротій О. О., Красинський С. В.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ОЦІНЮВАННІ МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ СКЛАДНИХ ТЕХНІЧНИХ ВИРОБІВ

В даний час оцінювання метрологічного забезпечення (МлЗ) складних технічних виробів (ТВ) здійснюється за допомогою науково-методичного апарату, розробленого за часів колишнього СРСР, який представляє собою в основному набір евристичних прийомів проведення оцінювання окремих показників МлЗ на різних етапах життєвого циклу виробів. Крім того, для процесу оцінювання МлЗ традиційними методами характерні великі тимчасові, трудові і фінансові витрати, зниження яких в умовах нинішньої економічної ситуації є одним із першочергових завдань. Удосконалення методичного апарату оцінювання МлЗ призводить, як правило, до неминучого його ускладнення і, як наслідок, до зростання всіх супутніх витрат.

Одним із шляхів вирішення даного протиріччя може бути залучення для вирішення завдань оцінювання МлЗ якісно нових засобів автоматизації та інформаційних технологій.

Як відомо, в будь-якій інформаційній технології (ІТ) виділяють три основні компоненти: обчислювальну середу (програмно-апаратний комплекс ІТ), виконавську середу (регламентовані функції користувачів ІТ) і методичну середу (опису дій при використанні ІТ в різних ситуаціях).

Обчислювальне середовище, в свою чергу, складається з операційних та інформаційних компонентів.

З аналізу структури компонентів інформаційних технологій слідує, що основним компонентом інформаційної технології оцінювання (ІТО) МлЗ досліджуваних зразків складних технічних виробів є інформаційне середовище ІТО, яке повинно формуватися з урахуванням можливостей і потреб методичного та виконавського середовищ.

Основна мета використання ІТ при оцінюванні МлЗ полягає в тому, щоб оперативно і в повному обсязі надати користувачеві сучасні методи і засоби синтезу-аналізу моделей МлЗ досліджуваних технічних виробів і забезпечити необхідну адекватність цих моделей реальним процесам. Основу синтезу моделей МлЗ повинна становити узагальнена інформаційна модель (УІМ) МлЗ технічного виробу. Мета розробки такої моделі полягає в тому, щоб визначити інформаційні потоки, виявити зв'язки між окремими завданнями, які вирішуються з оцінювання МлЗ, класифікувати джерела та споживачів інформації.

Відомо кілька визначень інформаційної моделі. Узагальнюючи конструктивні елементи кожного з цих визначень, під інформаційною моделлю МлЗ ТВ будемо розуміти різновид моделі, який виражає закономірності, притаманні МлЗ ТВ, за допомогою символьного опису того чи іншого виду, служить засобом взаємодії між метрологами і іншими фахівцями різного профілю, причетними до проектування, випробувань і експлуатації ТВ, і відображається в будь-яку інформаційну середу, підтримувану сучасними СУБД.

Наявність "системних" властивостей в МлЗ ТВ свідчить про те, що розробку УІМ МлЗ доцільно здійснювати в оболонці інформаційного середовища оцінювання МлЗ ТВ.

На основі аналізу МлЗ зразка ТВ як сукупності певних властивостей, в яких реалізовані задані вимоги до МлЗ зразка ТВ, який розробляється, пропонується представити УІМ і відповідну інформаційну середу оцінювання МлЗ зразка ТВ у вигляді, наведеному на рис. 1.

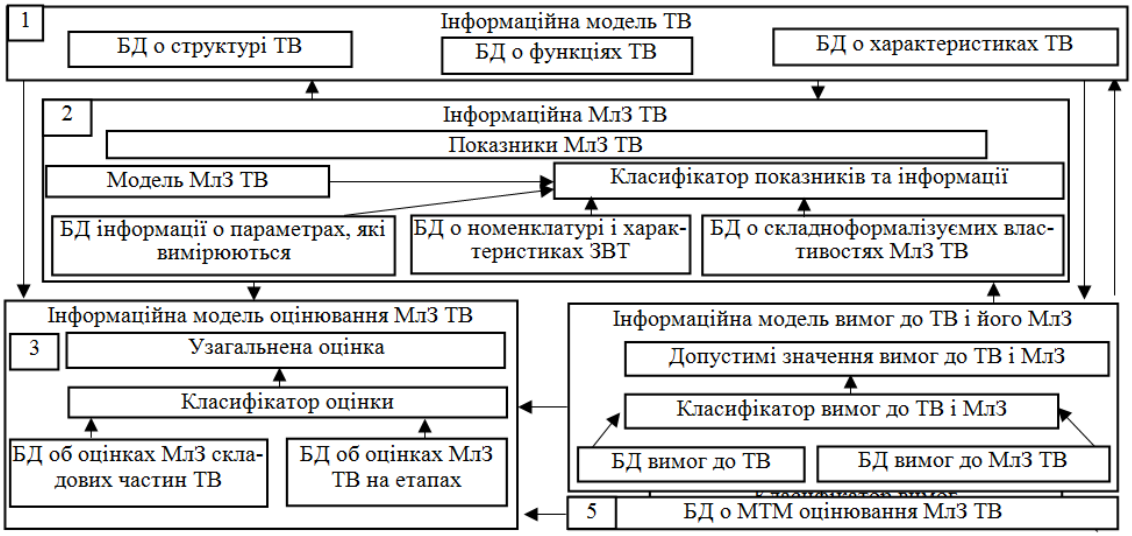


Рисунок 1 – Інформаційна середа оцінювання зразка ТВ

З наведеного рисунку слідує, що основними інформаційними технологічними модулями є бази даних вимірюваних параметрів, засобів вимірювальної техніки і інших властивостей ТВ, що визначають його "метрологічну досконалість". Класифікатори показників і оцінок є по суті методичними технологічними модулями (МТМ), які виконують функції отримання значень показників більш високого порядку, ніж вихідні. Функціональні залежності, використовувані при розрахунках, визначаються застосовуваними моделями МлЗ зразка ТВ.

Інформаційні технологічні модулі можуть використовуватися як автономно (припустимо, для вирішення окремих завдань оцінювання МлЗ ТВ), так і в складі різних інформаційних технологічних процесів або технологічних ліній (наприклад, військово-метрологічного супроводу зразків озброєння або проведення метрологічних експертиз).

Опис операцій з оцінювання окремих показників МлЗ та ефективності МлЗ ТВ в цілому закладаються в МТМ. Вибір дій передбачається у відповідних точках діалогу (меню), де здійснюються переходи між технологічними компонентами ІТО. Якщо в ІТО не пропонується використовувати інструментальні засоби експертних систем (що найчастіше і відбувається на початкових етапах формування ІТ), для отримання оцінки стану МлЗ доцільно застосовувати таблиці рішень.

Виконавську середу ІТО доцільно реалізовувати шляхом послідовного, еволюційного впровадження мережі автоматизованих робочих місць на всіх рівнях управління.

При цьому автоматизовані системи підтримки прийняття рішень при оцінюванні МлЗ займають проміжне положення між традиційними способами оцінювання МлЗ та ІТО.

Список використаних джерел

1. Нудьга А. П., Макаров О. В. Об опыте автоматизации оценивания метрологического обеспечения в процессе разработки сложных технических систем // Тез. докл. 1-го международного молодежного форума "Электроника и молодежь в XXI веке".

2. Морозов О. О. Формалізована модель системи метрологічного забезпечення. // Системи обробки інформації. – 2002. – № 6(22). – С. 100-105.

УДК 621.396

Кротов В. Д.

МЕТОД ПІДВИЩЕННЯ СТРУКТУРНО-ІНФОРМАЦІЙНОЇ ЗВ'ЯЗНОСТІ МОБІЛЬНИХ ВУЗЛІВ РАДІОМЕРЕЖ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ

Управління бойовими підрозділами в ході сучасних бойових дій вимагає повної поінформованості посадових осіб щодо ситуації, яка склалася на полі бою в той чи інший момент часу. Збір, обробка та відповідна реакція на таку інформації в тактичній ланці управління військами можливі лише шляхом використання сучасних мереж радіозв'язку, які можуть забезпечити зв'язок за принципом „у будь-якому місці, в будь-який час". Прикладом таких мереж є мобільні радіомережі (МРМ) класу MANET (Mobile Ad-Hoc Network), особливістю функціонування яких є мобільність всіх вузлів, а також здатність самоорганізовуватися в радіомережу без завчасно розгорнутої мережевої інфраструктури в умовах невизначеності (достовірна інформація про ситуацію на полі бою в момент розгортання відсутня).

У радіомережах тактичної ланки управління існує низка проблем, вивченню яких приділяється велика увага. Однією з таких проблем є проблема низької структурно-інформаційної зв'язності мобільних вузлів (рис.1). Структурна надійність сучасних мереж визначається наявністю або відсутністю справного шляху в заданому напрямку. Однак, наявність справного шляху ще не гарантує негайного встановлення з'єднання, оскільки елементи шляху можуть бути зайняті іншими абонентами для передачі або приймання інформації. Отже актуальною задачею у руслі створення ефективних телекомунікаційних технологій є оцінка надійності безпроводових мереж із урахуванням їх структурних і інформаційних характеристик. Отже, виникає необхідність розробки методу підвищення структурно-інформаційної зв'язності мобільних вузлів радіомереж тактичної ланки управління.

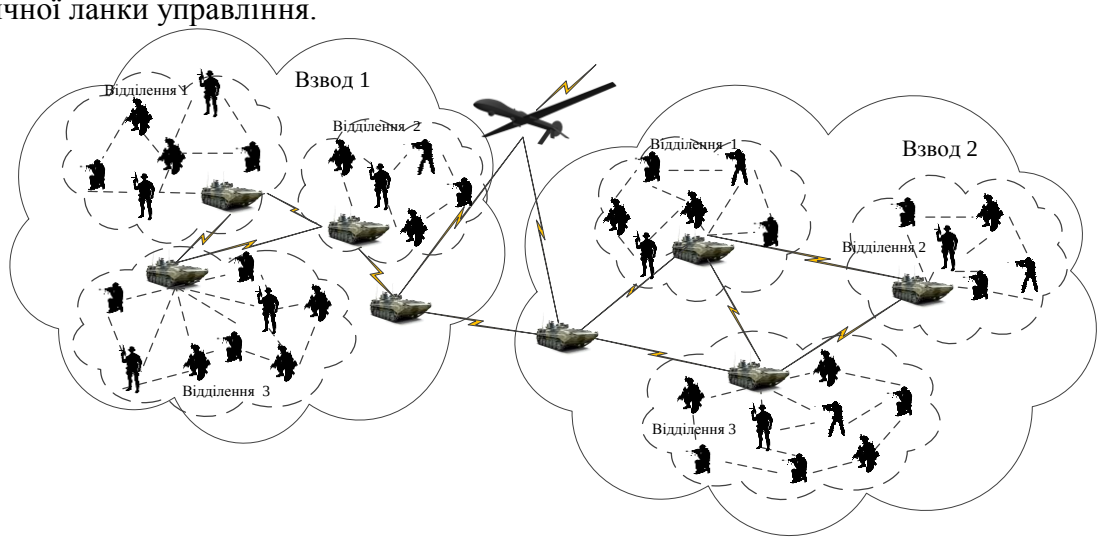


Рисунок 1 – Зони структурно-інформаційної зв'язності в тактичній ланці управління

Таким чином метою даної роботи є розробка методу підвищення структурно-інформаційної зв'язності мобільних вузлів радіомереж тактичної ланки управління в умовах постійної зміни структури та з урахуванням інформаційних характеристик мережі. Для досягнення поставленої мети передбачається вирішення наступних задач:

1. Обґрунтування показників для оцінки структурно-інформаційної надійності МРМ із урахуванням інформаційних характеристик мережі.
2. Систематизація існуючих методів та поєднання їх в єдиний оптимізований метод.
3. Програмна реалізація запропонованого алгоритму і аналіз отриманих результатів.

Структурно-інформаційну надійність будемо визначати як об’єктивну властивість мережі забезпечувати зв’язність абонентів із якістю надання послуг (QoS) не гірше заданої. При визначенні структурної надійності мережі будемо розглядати тільки вплив ліній зв’язку, вважаючи, що надійність вузлів дорівнює одиниці.

Справний стан лінії зв’язку може визначатися одним або декількома показниками якості надання послуг QoS. В залежності від типу трафіку пріоритетним показником QoS можуть бути різні параметри: гарантована достовірність (точність) передачі інформації, необхідна пропускна спроможність, час затримки передачі інформації та джиттер. Найважливішим із цих параметрів для більшості типів трафіку є необхідна гарантована достовірність передачі інформації.

Зазвичай структуру мережі можна представити у вигляді графу, що представляє собою сукупність послідовно або паралельно з’єднаних ребер (в даному випадку ненадійних ліній зв’язку). Практично будь-який граф двополюсної мережі можна перетворити на просте послідовне або паралельне з’єднання його елементів, наприклад, шляхом використання методу розкладання Шеннона-Мура. Однак критерій структурної зв’язності не може повністю характеризувати надійність зв’язку, оскільки він не враховує алгоритми функціонування мережі, зокрема, протокол множинного доступу, алгоритм обробки заявок на вузлах мережі, протокол маршрутизації, пропускні спроможності каналів та ін. Тому розглянемо можливість використання для оцінки надійності мережі критеріїв структурно-інформаційної та інформаційної зв’язностей, що характеризують якість обслуговування запитів в умовах ненадійності елементів.

При наявності потоку інформації між двома фіксованими вузлами мережі ймовірність структурно-інформаційної зв’язності між ними є ймовірність того, що в заданому інтервалі часу при надходженні чергового запиту на передачу інформації в процесі пошуку встановлення з’єднання знайдено принаймні один справний шлях між даними вузлами. Таким чином, критерій структурно-інформаційної зв’язності визначає потенційну надійність мережі та є верхньою межею ймовірності зв’язності між вузлами мережі. Однак, зв’язок між вузлами може бути невстановлений не тільки із-за порушення працездатності каналів, а також з причини відсутності вільних канальних ресурсів в даний момент часу.

У даній роботі пропонується метод колективної передачі інформації, спрямований на вирішення проблеми низької зв'язності в МРМ. Ідея даного методу полягає в тому, що близько розташовані один до одного вузли об'єднуються для синхронної передачі даних на інший вузол або точку збору інформації. Передбачається, що в приймальному пристрої сигнали від передавальних вузлів когерентно складаються, таким чином, виникає можливість значного збільшення дальності передачі інформації всередині мережі, що може бути використано для встановлення або відновлення зв'язку з ізольованими групами вузлів і має сприяти підвищенню зв'язності і збільшенню зони покриття мережі в цілому. Для здійснення когерентного складання потужностей насамперед необхідно забезпечити синхронізацію випромінювання мобільних (безпроводових) вузлів (МВ). Рішення завдання синхронізації генераторів в МВ може бути досягнуто на основі стандартного підходу, який передбачає використання систем фазового автопідстроювання. Однак реалізація подібних схем синхронізації значно ускладнює пристрій МВ і істотно підвищує їх вартість. Можливо інше рішення –використання в пристроях вузлів пасивних розсіювачів, які перевипромінюють загальне для всіх електромагнітне поле (поле підсвічування), створюване деяким стороннім джерелом. Таким чином, забезпечується когерентність полів випромінювання мобільних вузлів, при цьому внутрішній устрій самих вузлів може бути вкрай простим.

Висновки. В роботі був запропонований новий спосіб підвищення структурно-інформаційної зв’язності мобільних вузлів радіомереж тактичної ланки управління, заснований на когерентному складанні полів, випромінюваних близько розташованими вузлами. Також було продемонстровано, що застосування методу колективної передачі інформації дозволяє значно продовжити час життя радіомережі, а також збільшити да-

льність передачі інформації. Даний метод може бути використаний для підвищення зони покриття і вирішення проблеми низької зв'язності мережі у випадку неоднорідного розміщення мобільних вузлів.

Гаврилов А. Б., Бойко В. М., Рарог Р. Н., Світенко М. І.

РЕЗУЛЬТАТИ ДОСЛІДНОЇ ЕКСПЛУАТАЦІЇ ПІДСИСТЕМИ ЗАБЕЗПЕЧЕННЯ ЄДИНИМ ЧАСОМ ВІЙСЬКОВИХ СПОЖИВАЧІВ НА БАЗІ СЕРВЕРІВ ТОЧНОГО ЧАСУ MICROSEMI TIME PROVIDER 4100

Метою дослідної експлуатації апаратно-програмних засобів синхронізації є:

- визначення метрологічних характеристик і параметрів засобів синхронізації в штатному та періодичному режимах роботи провідного сервера PTP, а також та при впливі дестабілізуючих факторів (вплив асиметрії лінії зв'язку, навантаження в мережі, вразливість GNSS);
- підтвердження відповідності метрологічних характеристик апаратно-програмних засобів синхронізації вимогам, що висувалися згідно тактико-технічного завдання на науково-дослідну роботу шифр «Пролісок»;
- розробка пропозицій щодо розбудови, впровадження, підвищення надійності та точності системи забезпечення єдиним часом військових споживачів;
- визначення складу та метрологічних характеристик засобів системи метрологічного контролю та управління еталонними сигналами, способів їх застосування для обґрунтування пропозицій складу апаратурного оснащення технічної складової цієї системи.

Для дослідження впливу навантаження в мережі на похибку часу веденого сервера PTP були проведені цілодобові вимірювання похибки часу (TE) його вхідного PTP сигналу та вихідного сигналу 1PPS.

В доповіді наведені результати вимірювань Проведені оцінки функціонування сервісу надання точного часу дозволили сформувати вимоги до провайдера, щодо оптимізації маршрутизації лінії з метою зменшення значення асиметрії.

Дані дослідження є фундаментальною основою для подальшої розбудови незалежної від GNSS системи синхронізації часу в військовому секторі Служби єдиного часу і еталонних частот для визначення вимог до технічних характеристик та функціональних можливостей обладнання системи, режимів її роботи з метою забезпечення необхідної точності часу і надійності цієї системи. Результати досліджень доцільно використати при розробці та впровадженні аналогічних систем в інших критичних до точності часу галузях.

УДК 621.81:621.

Климченко С. В., Удніков О. М., Шеховцова І. О.

АВТОМАТИЗОВАНО-ВИМІРЮВАЛЬНА СИСТЕМА ПЕРЕДАВАННЯ ОДИНИЦІ ПОТУЖНОСТІ ЕЛЕКТРОМАГНІТНИХ КОЛИВАНЬ

Основною операцією при проведенні калібрування еталонних перетворювачів потужності електромагнітних коливань в коаксіальних трактах є визначення їх коефіцієнтів передавання. Однак проведення вимірювань з метою визначення коефіцієнту передавання характеризується значною трудомісткістю, яка обумовлена ручним режимом роботи апаратури, нестабільністю рівня потужності вихідного сигналу генератору, дрейфом еталонних ватметрів та іншими випадковими факторами. При цьому визначення коефіцієнту передавання проводиться на кожній контрольній частоті. Зменшення впли-

ву випадкових факторів можливо здійснити за рахунок проведення багаторазових вимірювань, тому для зменшення трудомісткості вимірювань пропонується розробити автоматизовану систему отримання та обробки вимірювальної інформації.

За допомогою апаратури, що має можливість автоматизованого дистанційного керування, побудувано автоматизовану-вимірювальну систему передавання розміру одиниці потужності електромагнітних коливань в коаксіальних трактах. До складу інформаційно-вимірювальної системи входять перетворювач потужності типу Keysight U8481A–100 в якості еталонного вимірювача потужності, генератор Rohde&Schwarz типу SMB100A та генератори сигналу високочастотні РГ4-04..РГ4-08 в якості джерела потужності високої та надвисокої частоти, мультиметр Picotest M3500A в якості вимірювального блоку ватметра, що калібрується.

Основу автоматизованої-вимірювальної системи складає прикладне програмне забезпечення, основними задачами якого є:

- автоматизувати процеси обробки та реєстрації результатів вимірювань при калібрування засобів вимірювання потужності надвисокої частоти в коаксіальних трактах.
- дистанційно керувати вимірювальними приладами: цифровим мультиметром типу PICOTEST M3500A та генераторами сигналів високочастотними типів SMB100A, РГ4-03 – РГ4-08 за допомогою дистанційного паралельного інтерфейсу GPIB (IEEE-488.2), а також перетворювачем потужності типу Keysight U8481A за допомогою USB інтерфейсу.
- зберігати у базі даних програми інформацію про всі типи вимірювачів, що проходили калібрування, з усіма відповідними частотами калібрування.
- зберігати у базі даних програми інформацію про характеристики всіх еталонних ватметрів, що приймали участь у вимірюваннях.
- обробляти результати вимірювань в ході проведення калібрування вимірювачів та зберігати їх у базі даних програми з можливістю продовження перерваних вимірювань та для подальшого аналізу.
- автоматично створювати протоколи калібрування і зберігати їх у вигляді файлів у форматі Excel.

Створення автоматизованої-вимірювальної системи дозволило зменшити час проведення калібрувальних (повірочних) робіт, підвищити точність вимірювань за рахунок проведення багатократних вимірювань та зменшення невизначеність вимірювань, усунути вплив “людського” фактору на результат вимірювань.

Ковальов М. М.

ОБРОБКА РЕЗУЛЬТАТІВ ВИМІРЮВАННЯ ПРИ ПРОВЕДЕНІ ЗВІРЕНЬ В СКЛАДІ ГРУПОВОЇ МІРИ

В процесі визначення метрологічних характеристик вантажнопоршневих манометрів необхідно зробити обробку отриманих значень. Якщо хоча б в одного з манометрів свідоцтво про калібрування робочого еталону не прострочено, це дозволяє оцінити відповідність їхніх похибок припустимим значенням. Обробка цих значень здійснюється в наступній послідовності.

Після визначення різниці відхилень показань манометрів (ΔР) і середньоквадратичній похибці відхилень (S) при позитивних результатах калібрування, свідоцтво про калібрування робочого еталону продовжують на 6 місяців. Загальний термін свідоцтва не повинен перевищувати 3 роки.

При негативних результатах проводиться виявлення можливих причин, що їх викликають, а також здійснити продування з’єднувальних ліній.

Потім проводиться визначення різниці площ (f1-f2) і його відповідності значенню, що вказане на свідоцтві про калібрування робочого еталону.

Якщо отримані значення різниці площ більше ніж на 0,001 мм попереднього значення, то необхідно перерахувати значення (f1-f2).

Згідно ГОСТ 8.479-82 п. 3.3.6 проводиться перевірка відповідності дійсних значень маси вантажів розрахунковим значенням, що зазначені у свідоцтві про калібрування робочого еталону.

Якщо вантажі не були підігнані під місце прискорення сили земного тяжіння та під розрахункові значення маси вантажів, то здійснюється тільки атестація вантажів.

У відповідності від отриманих результатів здійснюється повторне калібрування або приймається рішення про непридатність манометру.

Котова М. А., Шеховцова І. О., Каревік О. О.

СПОСІБ АВТОМАТИЗОВАНОЇ ПОВІРКИ ОДНОЗНАЧНИХ МІР ЕЛЕКТРИЧНОГО ОПОРУ

На даний час у Збройних Силах України та інших військових формуваннях експлуатується великий парк засобів вимірювальної техніки (ЗВТ) електричного опору – аналогові та цифрові омметри, вимірювачі опору заземлення, мегомметри, комбіновані електровимірювальні прилади, універсальні цифрові та електронні вольтметри, які використовуються для контролю параметрів зразків озброєння та військової техніки і умов техніки безпеки при експлуатації військових об’єктів та електроустановок. Для повірки (калібрування) даних ЗВТ застосовують магазини електричного опору різноманітних типів, метрологічне обслуговування яких, в свою чергу, виконується за допомогою однозначних мір електричного опору (ОМЕО) 2-го розряду. Отже, від рівня метрологічного забезпечення ОМЕО 2-го розряду безпосередньо залежить надійне функціонування багатьох технічних систем у Збройних Силах України та інших військових формуваннях.

На даний час повірка ОМЕО 2-го розряду, які експлуатуються у регіональних військових метрологічних частинах (РМВЧ), здійснюється за допомогою вихідного еталону Збройних Сил України одиниці електричного опору постійному струму (ВЕЗСУ). Існуюча проблема їх метрологічного забезпечення полягає в тому, що у діапазоні номінальних значень від 0,001 Ом до 100000 Ом вимірювання електричного опору ОМЕО здійснюється за допомогою технічно застарілої установки типу УМИС-2, яка знаходиться в експлуатації понад 50 років та має значний ступінь фізичного зносу. Установка забезпечує порівняння електричного опору ОМЕО 2-го розряду та ОМЕО ВЕЗСУ методом заміщення за допомогою одинарно-подвійного моста. Даний спосіб повірки характеризується високою трудомісткістю, зумовленою складною процедурою урівноваження моста та неможливістю автоматизації процесу вимірювань внаслідок технічно застарілої конструкції установки.

В доповіді пропонується вирішення зазначеної проблеми шляхом впровадження способу повірки, заснованого на порівнянні падіння напруг на еталонній ОМЕО ВЕЗСУ та ОМЕО 2-го розряду, що здійснюється за допомогою сучасного 8½ розрядного цифрового компаратора типу КМ300Р при протіканні через них постійного струму високої стабільності, який створює калібратор типу КМ300С-1. Вимірювання проводяться методом заміщення з використанням тарної (баластної) ОМЕО, що дозволяє виключити систематичну похибку компаратора з результатів вимірювань та забезпечити необхідну точність передавання розміру одиниці електричного опору. Компаратор напруг КМ300Р та калібратор струму КМ300С-1 обладнані сучасним дистанційним інтерфейсом, якій дозволяє здійснити керування процесом вимірювань, реєстрацію та обробку результатів вимірювань за встановленим алгоритмом з використанням персонального комп’ютера (ПК) та спеціально розробленого програмного забезпечення. Впровадження запропонованого способу автоматизованої повірки дозволить підвищити рівень

метрологічного обслуговування еталонних ОМЕО 2-го розряду шляхом зменшення трудомісткості та забезпечення високої надійності і оперативності процесу передавання розміру одиниці електричного опору.

Красинський С. В., Ніколенко В. В.

ПРАКТИКА ТА ЗАВДАННЯ СТАНДАРТИЗАЦІЇ ПРОДУКЦІЇ ОБОРОННОГО ПРИЗНАЧЕННЯ

Військова частина А0785 є колективним членом Технічного комітету стандартизації "Стандартизація продукції оборонного призначення" (ТК-176).

Робота ТК-176 спрямована на реалізацію завдань, передбачених: Стратегічним оборонним бюлетенем України; Державною цільовою оборонною програмою розвитку озброєння та військової техніки на період до 2022 року; Державною цільовою програмою реформування та розвитку оборонно-промислового комплексу України на період до 2021 року; Річними національними програмами співробітництва Україна – НАТО/

Військова частина А0785, як колективний член ТК-176, виконує роботи з розроблення, розгляду, перегляду, скасуванню та відновленню дії національних стандартів на озброєння та військову техніку.

У 2019 році військовою частиною А0785:

- розглянуто та надано коментарі до 24 проєктів ДСТУ В, що розробляються ТК 176 та 2 національних стандартів від споріднених ТК;
- проведено аналіз доцільності подальшого застосування стандартів колишнього СРСР на ОВТ (1086 стандартів виду ГОСТ В) та надано пропозиції щодо подовження їх чинності;
- прийнято участь в розгляді та погоджені проекту Пропозицій ТК-176 до Програми робіт з національної стандартизації на 2020 рік;
- прийнято участь в 11 засіданнях ТК-176, на яких розглядались питання погодження та прийняття остаточних редакцій 15 проєктів національних стандартів;
- розглянуто та надано рекомендації щодо впровадження 10 матеріальних стандартів НАТО в якості національних нормативних документів;
- прийнято участь у розробці ВСТ 03.210.030-2019 (01) "Метрологічне забезпечення. Вимоги підтвердження результатів калібрування випробувального та вимірювального обладнання (STANAG 4704, MOD)".

Військовою частиною А0785 в межах здійснення наукової та науково-технічної діяльності протягом 2020 року передбачається прийняти участь у:

- розробці моделей системи національних стандартів та нормативних документів державного замовника виду загальних технічних вимог до ОВТ (на заміну комплексу ГОСТ В 20.39) та системи стандартів якості (на заміну комплексу ГОСТ В 20.57);
- роботі щодо перегляду стандартів колишнього СРСР (відповідно до Указу Президента України від 02.08.2016 № 323/2016), подовження дії міждержавних стандартів на ОВТ (ГОСТ В), які не будуть переглянуті до 2022 року.

В 2-му кварталі 2020 року планується розробити проект ДСТУ В "Система розробки та постановки на виробництво ОВТ. Метрологічне забезпечення Основні положення".

Для врахування міжнародного досвіду стандартизації військова частина А0785 систематично приймає участь в консультаціях та семінарах щодо впровадження стандартів НАТО. На протязі 2019 року фахівці військової частини прийняли участь у навчальному семінарі з військової стандартизації для фахівців МО України, ЗС України та інших складових сектору безпеки і оборони України та семінарі під егідою НАТО "Питання життєвого циклу озброєнь" – Представництво НАТО в Україні.

У 2020 році передбачається продовжити практику участі у семінарах та науково-практичних конференціях з питань стандартизації ОВТ та впроваджувати нові методичні підходи у процеси національної та військової стандартизації.

Демідов Б. О., Кучеренко Ю. Ф., Матющенко О. Г.

ЗРОСТАННЯ РОЛІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ВІЙСЬКОВИХ ЧАСТИН НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ В УМОВАХ ВЕДЕННЯ "ГИБРИДНОЇ" ВІЙНИ

На сучасному етапі розбудови силових структур держави, в тому числі і Національної Гвардії України (НГ України), що характеризується впливом низки негативних факторів, до яких відносяться: загострення міждержавних економічних, політичних, ідеологічних суперечностей; зростання кількості внутрішніх конфліктів етнічного і релігійного характеру на території країни (боротьба концесій Московського та Київського патріархату); зріст злочинності та корупції в державі; неконтрольоване розповсюдження зброї; ведення проти нашої країни "гібридної" війни з боку Російська Федерація (РФ), велике значення повинно приділятись питанню вдосконалення інформаційно-аналітичного забезпечення (ІАЗ) діяльності військових частин (підрозділів) НГ України з метою успішного реагування на визначені виклики та загрози сьогодення при здійсненні оперативного (бойового) застосування військ НГ України. Зараз РФ застосовує методи "гібридної" війни до нашої країни залучаючи до участі у бутімто внутрішніх конфліктах держави недержавні суб'єкти іншої держави, а саме засоби масової інформації, неконституційні військові формування, здійснює: придушення свого опонента використовуючи скриті операції підривного характеру, влаштовуючи різні диверсії; захоплення інформаційного простору нашої держави, здійснюючи кібератаки на державні та військові системи і електронні ресурси; забезпечує всіляку військову та економічну підтримку незаконно проголошеним республікам.

За таких умов, в подальшому слід очікувати, що роль ІАЗ діяльності військових частин (підрозділів) НГ України буде значно збільшуватись і стане надзвичайно важливим фактором успішного реагування військ НГ України на ці виклики та загрози при виконанні ними своїх завдань за призначенням у повсякденній діяльності, в особливому періоді та під час бойових дій.

Основними цілями в рамках виконання процесу ІАЗ НГ України можливо виділити наступні: забезпечення безперервного наповнення інформаційних ресурсів штабів підрозділів (частин, з'єднань, угруповань) НГ України достовірною та своєчасною інформацією, необхідною для її використання в процесі підготовки до оперативного (бойового) застосування різних її формувань; забезпечення аналітичної (інтелектуальної) обробки отриманої інформації та її сортування за відповідними ознаками для оцінки обстановки та прийняття відповідних обґрунтованих управлінських рішень керівництвом (органами управління (ОУ)) щодо застосування відповідних (в тому числі і спеціальних) підрозділів (військ) НГ України; забезпечення процесу автоматизації виконання функцій керівництва (ОУ) для скорочення загального терміну циклів управління військами (засобами) різних формувань (підрозділів) НГ України при їх застосуванні, в тому числі і тих, хто приймає участь у проведенні операції на Сході України; забезпечення розмежування доступу до інформаційних ресурсів штабів підрозділів (частин, з'єднань, угруповань) НГ України з боку усіх учасників процесу ІАЗ діяльності НГ України у відповідності до їх повноважень.

Все це надасть можливість поліпшити оперативність в прийнятті обґрунтованих рішень керівництвом (командирами) різних рівнів управління НГ України щодо застосування підпорядкованих військ в різних умовах обстановки, що визвано певними викликами та загрозами, а також в умовах ведення "гібридної" війни.

Останіна В. Д.

ЗАГРОЗИ ПУБЛІЧНОГО WI-FI ТА ШЛЯХИ ЇХ УНИКНЕННЯ

У наш час майже всі люди, що мають сучасні гаджети з підключенням до мережі Інтернет, охоче використовують публічний Wi-Fi, який зустрічається майже всюди. Проте, зазвичай вони не знають наскільки високою може виявитися ціна за використання безкоштовної публічної мережі у кав'ярні, аеропорту, метро або інших громадських місцях. Платою є власні персональні дані і, як наслідок, великі матеріальні збитки.

У 2018 році фахівцями з AVAST Software (компанія-розробник антивірусих програм) був проведений анонімний експеримент із залученням учасників Mobile World Congress. У рамках експерименту було створено три відкриті Wi-Fi точки біля стенду для реєстрації відвідувачів виставки в аеропорту. Назвали їх стандартними іменами «Starbucks», «MWC Free WiFi» і «Airport_Free_Wifi_AENA».

За 4 години до них підключилося 2000 осіб. За підсумками експерименту була зроблена доповідь. Фахівці змогли проаналізувати трафік усіх цих людей і дізнатися, які сайти вони відвідували. Також дослідження дозволило отримати особисту інформацію 63% учасників: логіни, паролі, адреси електронної пошти тощо. Жертви ніколи б не дізналися про те, що їх дані потрапили до чиїхось рук, якби експерти з Avast не розкрили свій секрет. Більшість людей, які підключилися, були технічно підкованими. Адже вони приїхали на міжнародну IT-виставку. Але чомусь вони не вживали жодних заходів з самозахисту під час використання публічного Wi-Fi.

У своєму інтерв'ю виданню «Радіо Свобода» Олександр Гринчак, перший заступник начальника департаменту кіберполіції України, зазначив, що сьогодні кіберзлочини пов'язані з використання публічного Wi-Fi мають місце в Україні.

У даній роботі наведені порівняння найчастіших загроз, з якими можливо зустрітися під час використання відкритих Wi-Fi мереж, та шляхи їх уникнення. Порівняння проводилися на основі показників, а саме вартість, ефективність, складність та час. Дані показників оцінюються шкалою від 1 до 5. Для кожного показника 1 означає мінімум оцінюваного критерію, 5 – максимум. Так для вартості критерієм є затрачені кошти на реалізацію метода, для ефективності – кількість успішних зламів зі 100 спроб. Для порівняння складності потрібні спеціальні засоби та обладнання, де 1 – нічого не потрібно, 5 – необхідно більше п'яти елементів програмного або спеціального апаратного забезпечення. Для оцінки часу – 1 є менше одного дня, щоб підготувати атаку, 5 – більше трьох тижнів.

Усього у роботі було досліджено 4 найпоширеніші загрози, а саме користування сайтами, які використовують протокол http, фальшиві сторінки реальних сайтів, копії реальних точок доступу, перехоплення управління публічною мережою Wi-Fi.

Аналізуючи введення персональних даних на сайтах, які використовують протокол http можна дати такі варіанти оцінки: вартість – 1, ефективність – 5, складність – 1, час – 1.

Власник Wi-Fi точки або людина, яка отримала доступ до неї, може переглядати весь трафік, який проходить. І за допомогою аналізатора пакетів даних (наприклад, Wireshark або CommView) дізнаватися, на які сторінки люди заходили з підключених пристроїв і що вводили у форми. Це можуть бути дані для входу, тексти листів, повідомлення на форумах, дані банківських карток.

Більшість сучасних сайтів використовують https, за яким логіни і паролі передаються у зашифрованому вигляді. Сучасні браузери вміють розпізнавати небезпечні ситуації і попереджати про це користувача.

Загроза потрапити на фальшиві сайти, які копіюють реально існуючі, має наступні оцінки: вартість – 3, ефективність – 3, складність – 3, час – 2. Людина, у якої є доступ до роутера може налаштувати, наприклад, перенаправлення з online.oschadbank.ua/wb/

на сайт online.oschadBank.ua/wb/, на якому буде розміщена копія головної сторінки, створена для крадіжки паролів.

Для того, що розкрити обман несправжніх сторінок, завжди перевіряйте url-адресу сайту, на якому потрібно вказати логін та пароль. Варто використовувати менеджери паролів, а також, де можливо, підключати підтвердження пароля по SMS або інші методи двотапної авторизації.

Фальшиві точки доступу мають такі оцінки: вартість – 4, ефективність – 4, складність – 4, час – 1. За допомогою вільно доступних в Інтернет програм (наприклад, утиліти airbase-ng) можна створити копію будь-якої точки доступу. І якщо сигнал «фейк» буде сильніше оригіналу, то всі пристрої, у яких налагоджено автоматичне підключення до первісної точки доступу, будуть приєднуватися до «копії». І над ними можна буде проводити всі дії, приведені вище.

Щоб запобігти ризику варто відключити на всіх своїх пристроях автоматичне підключення до Wi-Fi мереж. Потрібно власноруч вибирати мережу, до якої треба підключитися.

Публічний Wi-Fi може бути загрозою як для користувачів, так і для її власника. Наприклад, за допомогою інструменту Wifiphisher, коли жертва підключається до фальшивої точки доступу, вона перенаправляється на фальшиву «сторінку адміністратора», на якій їй пропонується ввести пароль від роутера з метою завантаження оновлення системи. Якщо власник введе пароль, то у зловмисника відпадає необхідність підбирати цей пароль самостійно повністю. Даний спосіб має оцінки: вартість – 1, ефективність – 2, складність – 1, час – 1.

Щоб уберегтися, варто ігнорувати повідомлення, які потребують вводу даних роутерів публічних точок доступу.

Значно знизити більшість ризиків дозволяє використання VPN. Так, він не тільки замаскує маршрут трафіку, але також зможе зашифрувати дані і приховати комп'ютер або мобільний телефон від шахраїв.

У даній роботі були визначені розповсюджені загрози пов’язані з використанням публічних мереж, була проведена їх оцінка, а також шляхи уникнення. Отримавши оцінки можливо реально оцінити вірогідність загрози та можливість натрапити на неї.

Список використаних джерел

1. Що варто знати про кіберзлочинців в Україні? [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.radiosvoboda.org/a/details/29031166.html.

2. Сиделев П. Чи є небезпечні безкоштовні мережі Wi-Fi? [Електронний ресурс] / Павло Сиделев. – 2015. – Режим доступу до ресурсу: https://ain.ua/2015/02/25/chem-opasny-besplatnye-wi-fi-seti/.

Безкоровайний В. В., Іванюк О. А.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ РОЗПОДІЛЕНИХ БАЗ ДАНИХ

Процеси проектування розподілених баз даних (РБД) передбачають розв’язання множини взаємопов'язаних задач, що умовно об'єднуються в етапи концептуального, логічного та фізичного проектування [1]. На кожному з етапів проводиться синтез і аналіз варіантів проектних рішень за множиною функціональних і вартісних показників. При цьому ефективність функціонування та витрати на створення чи реінжиніринг РБД багато в чому визначаються їх фізичною структурою. Це вимагає спільно з традиційними задачами проектування баз даних вирішувати комплекси задач їх топологічної оптимізації.

Формально структура РБД, як територіально розподіленого об'єкта, і її властивості можуть бути подані у вигляді: $s=<E,R,G>$, $\varphi:(E,R,G)\to P(s)$, де E,R,G – відпо-

відно, множини елементів структури, зв'язків між елементами та топологія (територіальне розміщення) елементів і зв'язків РБД, що визначає фізичну реалізацію РБД на комп'ютерній мережі (сукупність топологій вузлів мережі й інформаційних ресурсів (ІР) бази (G_E), каналів G_R і маршрутів передачі інформації G_A в РБД, $G =< G_E, G_R, G_A >$); $P(s)$ – множина функціональних і вартісних характеристик РБД зі структурою s.

Розглядається загальна задача оцінки часу доступу до інформаційних ресурсів РБД $t(s) \in P(s)$ у такій постановці [2]. Задані: кількість користувачів РБД n, що розміщуються у вузлах комп'ютерної мережі заданої топології; кількість m і місця розміщення у вузлах мережі ІР локальних баз даних; розподіл ресурсів по вузлах мережі $x = [x_{ij}]$ (x_{ij} – булева змінна: $x_{ij} = 1$, якщо j-й ресурс зберігається в i-му вузлі мережі; $x_{ij} = 0$, в іншому випадку); інтенсивності надходження запитів від користувачів λ_{ij}, $i = \overline{1,n}$, $i = \overline{1,m}$; час обробки запитів $t_{ij}^{qp}(x)$; пропускні спроможності каналів мережі $h = [h_{ij}]$, $i, j = \overline{1,n}$; обсяги запитів a_{ij}, $i = \overline{1,n}$, $i = \overline{1,m}$ і відповідей на запити b_{ij}, $i = \overline{1,n}$, $i = \overline{1,m}$). Необхідно визначити оцінку часу доступу до інформаційних ресурсів РБД $t(s) \in P(s)$.

Процес функціонування РБД може бути подано у вигляді класичної системи масового обслуговування (Q-схеми): $Q =< W, U, H, Z, R, A >$, де W – вхідний потік запитів; U – потік обслуговувань; H – множина внутрішніх параметрів системи; Z – множина станів системи; R – схема зв'язків елементів системи; A – алгоритм функціонування системи.

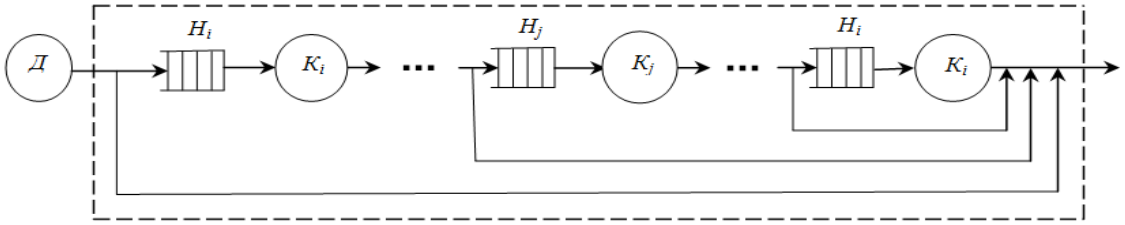


Рисунок 1 – Фрагмент багатофазної СМО для моделювання РБД:
Д – джерело запитів; *Hi, Hj* – накопичувачі для черг запитів і відповідей у вузлах комп'ютерної мережі; *Ki, Kj* – канали обслуговування вузлів видачі запиту та розташування ІР

На ранніх етапах проектування для отримання оцінок використовуються аналітичні співвідношення. Час доступу з i-го вузла мережі до ІР, розташованого в j-му вузлі:

$$t_{ij}(x) = \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} [t_{ij}^{tr}(x) + t_{ij}^{pr}(x) + t_{ij}^{qp}(x) + t_{ij}^{rp}(x)] \cdot x_{ij}}{n \cdot m},$$

де $t_{ij}^{tr}(x)$ – час передачі запиту з i-го вузла мережі до j-го ІР; $t_{ij}^{pr}(x)$ – час очікування запиту з i-го вузла по j-му ІР; $t_{ij}^{qp}(x)$ – час обробки запиту з i-го вузла по j-му ІР; $t_{ij}^{rp}(x)$ – час передачі відповіді на запит з i-го вузла по j-му ІР.

Час передачі запиту t_{ij}^{tr} по комп'ютерній мережі: $t_{ij}^{tr} = \sum_{k,l \in N_{ij}} \frac{a_{ij}}{h_{kl}}$, де a_{ij} – розмір запиту по j-му ІР з i-го вузла мережі; h_{kl} – пропускна здатність каналу зв'язку між k-м і l-м вузлами мережі; N_{ij} – множина вузлів на шляху між i-м і j-й вузлами мережі сети.

Загальний час очікування запитів в чергах вузлів мережі t_{ij}^{pr} визначається як сума очікувань на кожній фазі передачі запиту t_{kl}^{pr} і відповіді t_{lk}^{pr}:

$$t_{ij}^{pr} = \sum_{k,l \in N_{ij}} (t_{kl}^{pr} + t_{lk}^{pr}).$$

Час очікування запитів t_{kl}^{pr} і відповідей t_{lk}^{pr} (для пуассонівських потоків) визначається за співвідношенням: $t_{kl}^{pr} = l_{kl} / \lambda_{kl}$, $t_{lk}^{pr} = l_{lk} / \lambda_{lk}$, $l,k \in N_{ij}$, де $l_{lk} = \rho_k^2 / (1-\rho_k)$, $l_{kl} = \rho_l^2 / (1-\rho_l)$ – середні кількості запитів і відповідей в чергах між *l*-м і *k*-м, а також *k*-м і *l*-м вузлами мережі; $\rho_k = \lambda_{kl} / \mu_k$, $\rho_l = \dfrac{\lambda_{kl}}{\mu_l}$ – коефіцієнти завантаження *k*-го і *l*-го вузлів; λ_{kl}, λ_{lk} – інтенсивності потоків між вузлами *k* і *l*, а також *l* і *k*; μ_k, μ_l – інтенсивності обробки запитів і відповідей у вузлах *k* і *l* відповідно.

Час передачі відповіді на запит з *i*-го вузла мережі по *j*-му IP:

$$t_{ij}^{rp} = \sum_{l,k \in N_{ji}} b_{ij} / h_{lk},$$

де b_{ij} – обсяг відповіді на запит по *j*-му IP з *i*-го вузла; h_{lk} – пропускна спроможність каналу між *l*-м і *k*-м вузлами мережі; N_{ji} – множина вузлів на шляху передачі з *j*-го в і-й вузол мережі.

Як оцінки часу доступу використовуються значення середнього, максимального або середньозваженого значення. Визначення найкоротших шляхів для пересилання запитів і відповідей у комп'ютерній мережі, а також множин транзитних вузлів N_{ij} і N_{ji}, $i,j = \overline{1,n}$, трафіку між вузлами λ_{kl}, λ_{lk}, $k,l = \overline{1,n}$ здійснюється за алгоритмом Флойда-Уоршелла.

На завершальних етапах синтезу фізичної структури РБД, коли виникає необхідність визначення більш точних і достовірних оцінок пропонується використовувати імітаційну статистичну модель. Точність результатів визначається точністю завдання вхідних даних і кількістю реалізацій моделювального алгоритму.

Список використаних джерел

1. Арсеньев В. П. Интегрированные распределенные базы данных / В. П. Арсеньев. – СПб. : Изд.-полигр. центр СПбГЭТУ (ЛЭТИ), 2004. – 498 с.

2. Бескоровайный В. В. Оценка времени доступа к информационным ресурсам распределенных баз данных при решении задач синтеза их физических структур [Текст] / В. В. Бескоровайный, О. С. Ульянова // Системи управління, навігації та зв'язку. – 2010. – № 3(15). – С. 210 – 214.

Ругалёва И. Е., Ганак А. Д., Косовец А. А.

ПЕРСПЕКТИВЫ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ

В современном мире абсолютно все системы и электронные сети подпадают под общее определение «системы промышленной автоматизации и управления» (IACS). Понятие безопасность IACS относится к устранению противозаконного или нежелательного вторжения, преднамеренного или непреднамеренного вмешательства в рутинную работу или ненадлежащего доступа к засекреченной информации. *Кибербезопасность* – это осуществление мер по защите систем, сетей и программного обеспечения

от цифровых атак. Такие атаки обычно направлены на получение доступа к секретной информации, ее изменение и уничтожение, получение денег от пользователей или нарушение нормального функционирования компаний. Кибербезопасность применяется к персональным компьютерам, мобильным устройствам, сетям, операционным системам, приложениям и другим настраиваемым компонентам IACS.

Концепция кибербезопасности была разработана и введена в 1991 году в связи с широкой популяризацией технологий цифровых сетей. Кибератаки планируются и инициируются киберпреступниками с целью получения несанкционированного доступа к защищенной информации с целью копирования, изменения, уничтожения. Кибератаки также проводятся с целью получения денег от пользователей информационных систем.

Выполнение основных требований информационной безопасности позволяет сохранить цифровые данные в целости, защищенности от разглашения, использования (включая модификации), проверки или полного уничтожения, то есть полностью от несанкционированного доступа к ним.

Информационная безопасность является показателем гарантированной защиты как отдельных лиц, так и каждой организации (государства) и их различных интересов от любых разрушительных угроз или влияния в информационном пространстве. Информационная безопасность состоит из следующих основных компонентов информации:

1) *конфиденциальность* – это состояние информации, когда она предоставляется пользователям или объектам при наличии предоставленных ей прав;

2) *целостность* – термин в теории телекоммуникаций, который означает, что данные полны, условие того, что данные не были изменены при выполнении любой операции над ними, будь то передача, хранение или представление;

3) *доступность* - это открытость информации для пользователей или объектов в соответствии с предоставленными им правами доступа.

Информационная безопасность в этом случае отличается от кибербезопасности тем, что информационная безопасность используется для комплексной защиты защищенных информационных ресурсов и данных в любой форме, а кибербезопасность используется исключительно для защиты обработанных цифровых данных. Следовательно, для защиты как компаний, так и государств необходимо сделать интегрированную систему защиты объектов, а ее основой является информационная безопасность.

На данном этапе, в мире, где организации коммерческого, финансового, медицинского, перерабатывающего и энергетического секторов, включая все государственные органы, организуют сбор, хранение и обработку всей информации, нужной для работы, а также персональных данных сотрудников и пользователей. Фактически, абсолютно вся эта информация должна быть защищена, потому что она является конфиденциальной, и ее возможная утечка, потеря или кража могут иметь непредвиденные (негативные) последствия для отдельных лиц и организаций (государств). Организации или структуры, которые непосредственно предоставляют информационную структуру для городов, стран и мирового сообщества в целом, чаще подвергаются кибератакам, называются критической инфраструктурой. Критическая инфраструктура включает в себя: электроснабжение и теплоснабжение, водоснабжение и электроснабжение, системы обработки отходов и различные транспортные средства.

Индустрия информационной безопасности постоянно изменяется. Киберпреступность набирает обороты. По данным Forbes, в 2017 году 100% предприятий (850 компаний-участников исследования) попались под атаки через вредоносное ПО для мобильных устройств, 89% компаний стали жертвами man-in-the-middle через Wi-Fi.

На сегодняшний день в мире многие компании недооценивают программы по защите данных. В ходе исследования Ernst&Young было установлено, что 70-75% компаний заявили о необходимости повышения расходов на кибербезопасность более чем на 50%. И только около 12% опрошенных заявили, что не пользуются программами контроля доступа или обходятся неформальными методами.

Обеспечение защиты данных и информации от несанкционированных изменений и проверки их достоверности является главным моментом кибербезопасности. Когда поток информации увеличивается с такой скоростью, не имеет смысла «охранять периметр»: даже небольшая слабость может стать катастрофической, и сама компания рискует не заметить изменения данных вовремя.

Решение этого – блокчейн (*англ*. blockchain): распределенный реестр исключает несанкционированные изменения и редактирования файлов. Эта же технология может быть использована для ограничения доступа к информации. Не заблуждайтесь, рассматривая блокчейн как "разрушительную" технологию, которая быстро изменит существующие бизнес-модели, предложив менее дорогие и быстрые инструменты. Это фундаментальная технология, полная разработка которой потребует десятилетий, возможно, не одно.

Блокчейн сравнивается со стеком протоколов TCP/IP, которые лежат в основе Интернета. Это очень хорошая аналогия. Сначала архитектура телекоммуникаций базировалась на коммутации схем, потом появилась TCP/IP, но это не изменило подхода к телекоммуникациям. В 1970-х гг. TCP/IP использовались для разработки ARPAnet, в 1980-х и в начале 1990-х использовались для создания частных сетей крупных коммерческих предприятий, и только в середине 1990-х, с появлением всемирной паутины, TCP/IP получил широкое распространение. Скорее всего, формирование блокчейна состоится по аналогичной схеме.

Но это вовсе не означает, что вы еще не можете думать о блокчейн в кибербезопасности. Напротив, блокчейн принципиально изменит наши представления о всех бизнес-процессах и информационных технологиях, поэтому вам нужно изучить его и адаптировать его к вашей отрасли прямо сейчас.

Ругалёва И. Е., Комиссарова Е. И.

ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ КАК СПОСОБА ЗАЩИТЫ ИНФОРМАЦИИ

В связи с широким распространением инновационных технологий в современном мире необходимо создать совокупность условий, гарантирующих защищенность всех составляющих элементов информационных систем от максимального числа угроз и неприемлемых воздействий на физическом, эмоционально-психическом, финансовом, духовно-образовательном, политическом и профессиональном уровнях воздействия или нежелательных негативных последствий в случае возникновения ошибок, при повреждениях, авариях, несчастных случаях, а также иного вреда в киберпространстве.

Кибербезопасность – это воплощение всех мер защиты приложений, сетей и устройств. Данное направление решает проблему безопасности конфиденциальных данных, защищает их целостность, а также сохраняет возможность корректной работы той или иной организации.

Разносторонней комплексной кибератаке с большей вероятностью подвергаются организации, которые обеспечивают инфраструктуры целых городов, стран и мирового сообщества в целом. Такие организации или структуры называются критическими инфраструктурами. Они имеют многоуровневую структуру, включающую: уровень технических компонентов (машины, оборудование и аппаратура); социальный уровень (персонал), организационный уровень (взаимодействие служб компании); уровень государственного управления (нормативные и контролирующие органы, осуществляющие надзор и государственное регулирование в сфере деятельности критических инфраструктур).

Кибербезопасность, как и все виды защиты подлежит совершенствованию с течением времени и требует скоординированных действий всей системы. С каждым днем принципы, технологии и характер кибератак трансформируются в более вредоносный,

в связи с этим устаревший подход к защите главной информации и игнорированию побочной является нецелесообразным. Необходимо не документально на длительное время предупреждать о возможных угрозах, а вести постоянный мониторинг с последующим анализом и незамедлительной разработкой мер обезвреживания атак без ущерба для существующей информации. Превалирующим принципом защиты необходимо считать сохранность личных данных, паролей при аунтефикации, а также электронного документооборота и т.п.

Стратегическая угроза киберопасности – движущая сила разработки средств защиты. Целью является разработка систем защиты всех видов трудовой отрасли в мире.

По прогнозам экспертов, мировой ущерб от кибератак в 2020 году может достигнуть $2 трлн., при этом компании на защиту от хакеров потратят $100 млрд, что значительно повысит востребованность специалистов в области кибербезопасности.

Однако, по мнению Forbes, тотальной ошибкой специалистов данной области является игнорирование 95% оповещений защитного ПО, которое хоть и несовершенно в защите от киберугроз, но является необходимым в борьбе за конфиденциальность данных. В ближайшие 10 лет необходимы будут разработки по усовершенствованию кибербезопасности, которые будут сделаны с молниеносной скоростью, но при этом будут качественно работать, в связи со столь же невероятной скоростью освоения злоумышленниками новых технологий.

Анализируя тенденции можно сделать вывод, что киберриски ассоциируются со сферой IT. Задачей же IT-отделов в реальной финансовой организации скорее является быстрое интуитивное внедрение технологических возможностей защиты, а это не согласуется с обеспечением более безопасного использования информации. Нецелесообразно считать кибербезопасность ответственностью IT-отделов, т.к. при возникновении кибератаки в ее обезвреживании должны принять участие не только IT-специалисты, но и необходима работа со страховыми компаниями и регулирующими органами. Есть острая необходимость к рассмотрению иного подхода к обеспечению изоляции киберрисков, отклонившись от поиска некого единого технологического решения. В связи с этим целесообразно принять меры для разработки методов, устройств и систем защиты от киберрисков, а не фокусироваться на приобретение юридическими корпорациями устройств, которые они смогут подключить к своей системе для обеспечения защиты.

Прогнозирование по решению проблемы киберугроз на глобальном и локальном уровнях все чаще ассоциируют с внедрением в разработки искусственного интеллекта, которым сможет быть адаптирован к технологам в инфраструктурах заказчиков. Однако, будет наблюдаться существенная нехватка кадровых единиц, в связи с увеличившимся в несколько раз интересу к кибербезопасности, поэтому целесообразно готовить и обучать специалистов внутри компании, а также прибегать к найму молодых специалистов.

Также желание себя заблаговременно обезопасить заставляет руководителей прибегать к использованию экспертной технической поддержки, которая контролирует бесперебойную работу всех систем компании и решение возникающих проблем. Безопасности всей критической информационной структуры также уделено немалое внимание, так как она включает помощь в определении критических участков работы системы, планирование действий для обеспечения соответствия киберструктур требованиям законодательства, включая обучение специалистов в учебном центре.Для проверки защиты данных проводится тест на проникновение (pentest). Данный тест позволяет выявить уровень защищенности клиента и его сотрудников.

В связи с необходимостью конкурентоспособности на рынке бизнеса на данный момент все компании производят цифровую трансформацию. Она представляет собой процесс интеграции цифровых технологий во все аспекты бизнеса. Актуальной разработкой для обеспечения безопасности таких процессов в сфере бизнеса является пакет Softline, включающий в себя аутсорсинг, позволяющий передачу информационных систем заказчика на обслуживание и контроль специализированным организациям, техническую поддержку

IT-систем и комплексов. Незаменимым также в пакете является аутсорсинг печати, подразумевающий как саму печать, так и предоставление средств печати в регионы. В пакет входит и безопасность критической информационной инфраструктуры, и тестирование на проникновение. Составляющей также является услуга SOC, позволяющая максимально быстро распознавать и устранять разного рода атаки, будь то вирусы, подозрительные рассылки или попытки проникновения в сеть. Цель данной услуги уменьшение риска потери данных и снижение ущерба возникающих инцидентов.

Неотъемлемой частью является защита бренда. Прежде всего это защита наработок и интеллектуальной собственности клиента. Она распространяется на несколько типов угроз: репутационные риски, санкционные и налоговые риски, невыполнение договорных обязательств, работа сотрудников против интересов компании и корпоративный шпионаж, ущерб из-за утечек информации, нелегитимного доступа к данным, использования вредоносного ПО, фишинга, а также мониторинг теневого интернета или «Даркнета». По выявлении угрозы или возможности несанкционированного пользования система безопасности клиента мгновенно уведомляет его об этом.Проверка подлинности данных и защита их от несанкционированного изменения (блокчейн) – аспект кибербезопасности, который не подлежит игнорированию.

Количество информации растет с невероятной скоростью и только безостановочная работа по поддержке кибербезопасности дает возможность сохранения желаемой конфиденциальности данных, ведь непоправимые изменения в данных организация может слишком поздно, что фактически остановит жизненный цикл бизнеса.

Корольов В. М., Климович О. К., Заєць Я. Г.

ЩОДО УПРАВЛІННЯ ВЗАЄМОДІЄЮ ПІДРОЗДІЛІВ СУХОПУТНИХ ВІЙСЬК НА ОСНОВІ ЗАСТОСУВАННЯ НАВІГАЦІЙНОЇ ІНФОРМАЦІЇ

З урахуванням досвіду застосування військових підрозділів сухопутних військ у збройних конфліктах та війнах сучасності, інтенсивність переміщень в ході виконання ними завдань за призначенням, як на етапах підготовки, так і ведення бойових дій зростає.

Пересування, бойові зіткнення, спеціальні операції відбуваються переважно вночі або в умовах обмеженої видимості, як правило, на не знайомій місцевості. У зв’язку з цим значно зростає роль та значення управління підрозділами з метою забезпечення контролю їх дій та своєчасного і точного виходу в пункти призначення. Під час виконання завдань за призначенням в складі підрозділів, командири повинні володіти повною інформацією про розташування як своїх сил і засобів, так і противника у будь-який момент часу.

Таким чином, стійке та безперервне забезпечення навігаційною інформацією (навігаційне забезпечення) стає одним із вирішальних чинників в організації системи управління взаємодією підрозділів сухопутних військ. Це дає можливість у будь-який момент часу знати місцезнаходження підрозділів на марші, їх бойовий порядок при штатному застосуванні, здійснювати пересування автомобільних та змішаних колон в умовах обмеженої видимості, на місцевості що зазнала значних змін внаслідок масованих ракетно-артилерійських ударів, або на місцевості де мало орієнтирів, а також дотримуватись заданого напряму руху при подоланні водних перешкод на плаву та під водою.

Військові фахівці, провідних у військовому відношенні країн світу, розглядають навігаційне забезпечення як важливий вид бойового забезпечення, а навігаційну апаратуру – як одну із складових системи управління взаємодію підрозділів під час їх бойового застосування.

Але, на сучасному етапі, системи управління взаємодією не дозволяють повною мірою використовувати навігаційну інформацію для цілевказування, управління підрозділом з урахуванням оцінки вигідного положення кожної бойової машини, незалежно від наявнос-

ті прямої видимості між машинами командира та підлеглого, графічного відображення місць розташування машин підрозділу, їх змін за часом, на фоні топографічної основи електронної карти автоматизованого робочого місця командира підрозділу.

В умовах сьогодення існує необхідність значного скорочення часу на підготовку даних для роботи навігаційної апаратури, максимальної автоматизації опрацювання навігаційної інформації що поступає до командира підрозділу від бойових машин, вирішення завдання отримання цілевказування від вищого командира (начальника) та прийняття рішень щодо залучення будь-якої машини підрозділу, яка знаходиться у найбільш вигідному положенні для ураження противника, передачі цілевказування на підлеглі машини та здійснення контролю за їх діями під час маршу та в ході бойового застосування.

Таким чином, з метою розширення кола завдань, які вирішуються підрозділами сухопутних військ, та значного скорочення часу на їх виконання, існує необхідність вдосконалення систем управління взаємодією на основі широкого застосування навігаційної інформації.

Корольов В. М., Климович О. К., Заєць Я. Г.

ЗАСТОСУВАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ МОДЕЛЮВАННЯ БОЙОВИХ ДІЙ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Розвитку автоматизованих систем моделювання бойових дій, в планах командування збройних сил провідних країн світу, на сьогодні, відводиться важлива роль.

У сучасну епоху потужних засобів розвідки, комплексної вогневої, електронної, інформаційної і інтелектуальної протидії, командиру необхідно приймати рішення, спираючись на результати моделювання бою. Для цього необхідні новітні комп'ютерні і ситуаційні центри, розробка нових систем і засобів моделювання і автоматизації управління боєм.

На основі досвіду розвитку систем та засобів моделювання бойових дій (операцій) в арміях провідних держав світу, пропонується сформулювати вимоги щодо обліку перспективної вітчизняної автоматизованої системи моделювання бойових дій у Збройних силах України на основі єдиних науково-методологічних і технічних підходів при її створенні. Вона має відповідати низці чинників, основними з яких є:

мати ієрархічну інтегровану модульну структуру, побудовану на платформі сучасних ЕОМ та операційних систем, з програмним забезпеченням на основі єдиного інформаційного середовища;

в залежності від ієрархічного рівня складатися з оперативної, оперативно-тактичної та тактичної підмоделей бойових дій (операцій). Останні, в свою чергу, мають поєднувати комбінацію тактичних імітаторів бойової обстановки в межах інтегрованої мережі і тренажерів (симуляторів) військової техніки;

бути гнучкою з можливістю нарощування і удосконалення під різні варіанти і умови ведення бойових дій, розширення переліку вирішуваних завдань та визначення оптимального складу сил і засобів необхідних для виконання конкретного завдання;

враховувати реальні характеристики і стан озброєння і військової техніки протиборчих сторін, кількість військ, систему прийняття і підтримки рішень;

допомагати командирам різного рівня у прийнятті рішення на бій (операцію), співставляючи обрані способи дій своїх військ і противника та, прорахувавши декілька варіантів ведення бою, надавати пропозиції для вибору оптимального;

в обов’язковому порядку має бути створена на основі стандартів єдиної так званої «HLA-архітектури», яка передбачає структуру системи на рівні взаємозв'язків окремих компонентів, а також стандартів, правил і специфікацій інтерфейсів, що визначають взаємодію моделей при розробці, модифікації і функціонуванні, сумісність програмного забезпечення для всіх моделей і широку промислову базу для виробництва комплектуючих, доступність для технічної реалізації програм потенційними розробниками.

Застосування автоматизованої системи моделювання бойових дій, у поєднанні із заходами які проводяться на місцевості з реальною участю військ, буде сприяти підвищенню реалістичності оперативної і бойової підготовки, дозволить покращити якість підготовки командирів, які уміли б швидко і з залученням оптимального комплекту сил та засобів ухвалювати правильні рішення, підняти рівень повсякденної бойової готовності і підвищити можливості перевірки та оцінки на практиці нових концепцій і способів бойового застосування військ (сил).

Таким чином, одним із основних факторів забезпечення ефективності розбудови і застосування Збройних Сил, в перелік пріоритетних технологій при формуванні воєнно-технічної політики держави, мають бути включені питання щодо створення і розвитку систем та засобів моделювання і імітації бойових дій.

Пащук Ю. М., Заєць Я. Г.

ЩОДО НАПРЯМІВ РОЗВИТКУ ПЕРСПЕКТИВНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В ІНТЕРЕСАХ ЗБРОЙНИХ СИЛ

Особливе місце в планах розвитку засобів повітряного нападу іноземних держав відводиться створенню і прийняттю на озброєння безпілотних літальних апаратів (БПЛА). За оцінками зарубіжних експертів, одним із пріоритетних напрямків підвищення ефективності застосування військ (сил) вважається оснащення збройних сил БПЛА різного призначення.

Бойове застосування БПЛА у військових діях розглядається в рамках декількох напрямів.

Перший напрям передбачає задіяння БПЛА в розвідувальних цілях, для розвідки об'єктів і їх позначення, а також організацію передачі з борту розвідувальних БПЛА інформації про цілі на пункти управління (ПУ) військами, в кабіни екіпажів бойових літаків. Ввважається необхідним покласти на БПЛА завдання безпосереднього цілевказування високоточним системам озброєння і контролю результатів ударів.

Другий напрям передбачає застосування БПЛА в ударному варіанті. Відповідно до нього на ударні БПЛА можуть бути покладені такі завдання: придушення системи протиповітряної оборони противника; вибіркове ураження ключових військово-економічних об'єктів в залежності від ступеня їх важливості; боротьба з малорозмірними, в тому числі мобільними, цілями.

При розробці основ бойового застосування ударних БПЛА військові фахівці передбачають наступну послідовність їхніх дій: політ в заданий район, пошук об'єктів, передача на відповідний КП (ПУ) зображень для ідентифікації цілей, їх ураження за командою з землі і подальше повернення до місця базування. Після нанесення ударів БПЛА можуть продовжувати політ для збору інформації або чекати команди для нанесення ударів по інших об'єктах.

Відповідно до третього напряму БПЛА ведуть радіоелектронну боротьбу. Ця ідея узгоджується з концепціями інформаційно-психологічних війн, також орієнтованими не на масштбні бойові дії і знищення живої сили і техніки противника, а на виведення з ладу систем управління військами та зброєю і морально-психологічний вплив на протиборчу сторону.

На думку авторів цього варіанту, в ході інформаційного протиборства БПЛА повинні брати активну участь в радіоелектронному придушенні об'єктів противника і тим самим створювати для нього невизначеність обстановки. БПЛА можуть застосовуватися також для постановки перешкод радіо- і телевізійним центрам.

Четвертий напрям пов'язаний із застосуванням БПЛА для боротьби з системою протиповітряної оборони противника. За своєю суттю таке завданя є неодмінною складо-

вою усіх попередніх напрямів і розробляється стосовно перспективних ешелонованих систем протиповітряної оборони противника.

Таким чином, на думку військових фахівців, перспективні БПЛА сприятимуть зростанню бойової могутності збройних сил і їх основна роль буде полягати головним чином в тому, щоб забезпечувати бойові дії авіації і наносити удари по розвіданим об'єктам противника за відносно нескладної обстановки.

У перспективі створення нових високоефективних безпілотних авіаційних комплексів і розширення спектра завдань, що раніше виконувались екіпажами пілотованих літаків, приведуть до формування спеціального роду авіації - безпілотної.

УДК 681.518:339.13

Железко Б. А.

МУЛЬТИАГЕНТНЫЕ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ПРОЕКТАХ ПО МАРКЕТИНГОВОМУ ИНЖИНИРИНГУ БИЗНЕСА[1]

Исследования в сфере мультиагентных систем поддержки принятия решений (МА СППР) и их применения для цифровизации процессов управления проектами по маркетинговому инжинирингу и реинжинирингу бизнеса (МРБП) ведутся достаточно давною [1]. Однако, в связи с исключительно высокой динамикой развития информационных технологий, разработки в области МА СППР требуют постоянной адаптации к уровню достижений научно-технического прогресса и изменениям во внешней бизнес-среде.

Несмотря на имеющиеся разработки в данной области, существующие технологии поддержки принятия решений предполагают адаптацию только отдельных компонент СППР и не обеспечивают адаптацию модели предметной области. Это приводит к использованию неактуальных и недостоверных данных в СППР, что отрицательно сказывается на эффективности принятия решения в условиях быстро меняющейся внешней среды.

МРБП – разновидность реинжиниринга бизнес-процессов (РБП) ориентированная на достижение основных целей маркетинговой деятельности (расширение объема продаж и рынков сбыта; увеличение занимаемой роли на рынке; рост прибыли и обеспечение обоснованности принимаемых руководством фирмы решений в области производственно-сбытовой и научно-технической деятельности). Этим он отличается от, например, стратегического корпоративного РБП, целью которого является поиск стратегического инвестора.

В данной работе проведено обобщение методов построения автоматизированных систем применительно к задачам создания и развития МА СППР, в результате чего разработан подход к совместному описанию согласованных требований Потребителя, Производителя и Проектировщика (концепция трех П), базирующийся на макетировании, моделировании и поэтапной реализации средствами современных информационных технологий компонентов и подсистем МА СППР (ММР-методология) и на этой основе ряд ИА СППР и автоматизированных рабочих мест (АРМ), обеспечивающие (за счет улучшения их возможностей к адаптации модели предметной области) повышение эффективности и качества принимаемых решений [2].

Список использованных источников

1. Железко Б. А. Системы поддержки принятия решений: вопросы создания и примеры использования / Под ред. А. Н. Морозевича. – Мн.: КИВТ НАН Беларуси, 1998. – 80 с.

[1] Результаты частично получены в рамках выполнения проекта 543853-TEMPUS-1-2013-1-DE-TEMPUS-SMHES «Поддержка треугольника знаний в Беларуси, Украине и Молдове»

2. Navitskaya, K. Information and Analytical Support of Decision-Making Procedures in Strategic Corporate Reengineering / K. Navitskaya, B. Zhalezka // Eastern European Journal of Regional Studies. – 2016. – Volume 2. Issue 2. December 2016. – P. 41 – 49.

УДК 621.372

Аркушенко П. Л., Борщ В. В., Вервейко О. І., Коваленко А. В. Семироз А. О.

ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ ЩОДО НОРМАТИВНОЇ ДОКУМЕНТАЦІЇ З МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ ВИПРОБУВАНЬ ОЗБРОЄННЯ І ВІЙСЬКОВОЇ ТЕХНІКИ

В даний час Україна інтенсивно проводить заходи щодо побудови сектору безпеки і оборони країни, який відповідає найкращим зразкам провідних європейських держав та держав-членів НАТО, що потребує, зокрема, створення нових та модернізацію існуючих систем, комплексів і зразків озброєння та військової техніки (ОВТ).

Рішення про прийняття на озброєння (постачання) нових та модернізованих ОВТ або щодо можливості їх допуску до експлуатації та/або постачання в особливий період приймають на підставі позитивних результатів випробувань (попередніх, міжвідомчих, державних, визначальних відомчих).

Основним документом, що визначає порядок підготовки і проведення випробувань ОВТ, є ГОСТ В 15.210-78 «Испытания опытных образцов изделий и опытных ремонтных образцов изделий. Основные положения», який введений в дію понад сорок років тому і в Україні не коригується. Однак цей стандарт має ряд недоліків: не враховує перетворення, що відбулися в економіці України; неузгоджений з актами національного законодавства тощо.

Для усунення ряду зазначених недоліків:

- Кабінет Міністрів України і Міністерство Оборони України розробили і ввели в дію ряд нормативних документів;
- Кабінет Міністрів України розробив проекти Закону «Про виробництво військової техніки» та двох редакцій Закону «Про створення та виробництво озброєння, військової і спеціальної техніки», які надійшли до Верховної Ради України відповідно у 2010, 2013 і 2017 роках. Однак за результатами розгляду цих проектів Верховною Радою вони були повернути на доопрацювання ініціатору внесення або відкликані;
- в даний час знаходяться на обговоренні та узгодженні проекти документів:

1) стандарту ДСТУ В-П «Система розроблення і поставлення на виробництво озброєння та військової техніки. Випробування дослідних зразків виробів і дослідних ремонтних зразків виробів. Основні положення», який розроблений Державним науково-дослідним інститутом випробувань і сертифікації озброєння та військової техніки;

2) наказу Міністерство Оборони України про затвердження «Інструкції з організації проведення випробувань дослідних зразків озброєння та військової техніки», який розроблений Центральним науково-дослідним інститутом озброєння та військової техніки Збройних Сил України.

У доповіді:

- показані основні положення чинних нормативних документів з організації та проведення випробувань та метрологічного забезпечення ОВТ, відзначені особливості проектів документів з даної тематики;
- наведені причини збільшення ролі метрологічного забезпечення випробувань на сучасному етапі;
- відзначено, що метрологічне забезпечення випробувань побічно регламентують нормативні документи з організації та проведення випробувань ОВТ.

За результатами досліджень обґрунтовано необхідність розробки нормативного документа з метрологічного забезпечення випробувань ОВТ з формуванням вимог до випробувальної організації та його персоналу, засобів вимірювальної техніки та випробувального обладнання, методик виконання вимірювань, програм і методик випробувань, проведення оцінки метрологічного забезпечення випробувань.

УДК 629.78:528.8

Беспалко І. А., Пекарєв Д. В.

ПІДХІД ДО ОПТИМАЛЬНОГО РОЗПОДІЛУ ФУНКЦІЙ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНО-АЛГОРИТМІЧНОГО ЗАБЕЗПЕЧЕННЯ АНАЛІЗУ СТАНУ ТА ЗМІН КОСМІЧНОЇ ОБСТАНОВКИ В ІНТЕРЕСАХ СКЛАДОВИХ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Сучасний світ характеризується стрімким розвитком інформаційних технологій, розробленням, створенням та застосуванням (використанням) високотехнологічних систем і засобів для забезпечення існування та діяльності людства у різних сферах. Однією з таких сфер є космічна. Разом із позитивними аспектами, що виникають при застосуванні космічних систем і засобів у комерційній, дослідницькій, інформаційній, телекомунікаційній, військовій та інших галузях, виникають, існують та зростають відповідні загрози. Вони, насамперед, стосуються діяльності силових структур держави та впливають на рівень національної безпеки.

Для забезпечення прийняття вірних управлінських рішень та з метою врахування і подальшої нейтралізації або зменшення наслідків від загроз, які пов’язані з космічною сферою, перш за все, штучних дій з космосу, у космосі та через космос, питання оцінювання рівня згаданих загроз доцільно розглядати комплексно. Спочатку це має стосуватися всебічного аналізу стану та змін комічної обстановки, зокрема застосування космічних апаратів (КА).

Наразі практично всі складові сектору безпеки і оборони держави мають розгорнуті ситуаційні центри, а Указом Президента України Про рішення Ради національної безпеки і оборони України від 04 березня 2016 року “Про Концепцію розвитку сектору безпеки і оборони України” визначено створення системи моніторингу, аналізу, прогнозування, моделювання та підтримки прийняття рішень у сфері національної безпеки і оборони за єдиними методиками, що підготовлені з використанням можливостей Головного ситуаційного центру України.

Слід врахувати, що складові сектору безпеки і оборони часто виконують завдання, пов’язані з інформацією, що має обмеження доступу. У свою чергу для забезпечення якісного аналізу стану та змін космічної обстановки необхідно мати постійний доступ до ресурсів мережі Internet, забезпечити автоматичні/автоматизовані пошук та оновлення даних, а також відображення космічної обстановки для різних умов та сценаріїв на відповідних засобах ситуаційних центрів. Реалізація виконання всіх зазначених завдань на одному програмно-апаратному комплексі (враховуючи, що не всі складові сектору безпеки і оборони мають гарантовано захищені засоби та високошвидкісні канали зв’язку) створює передумови витоку інформації, що має обмеження доступу.

Виходячи з викладеного, пропонується розділити функціонал програмно-апаратного комплексу аналізу стану та змін космічної обстановки на відкриту та спеціалізовану частини. Згадане, перш за все, забезпечить безперервність і автоматизацію збору необхідних даних та унеможливить витік конфіденційної, службової чи таємної інформації, що циркулюватиме виключно у спеціалізованому програмно-апаратному комплексі. З іншого боку функціонал відкритої частини програмно-алгоритмічного забезпечення є однаковий для

всіх складових сектору безпеки і оборони та має забезпечувати наявність уніфікованої вхідної інформації для спеціалізованих частин зазначених складових.

У доповіді наведено результати вирішення наукового завдання оптимального розподілу функцій між відкритою та закритою частинами програмно-алгоритмічного забезпечення аналізу стану та змін космічної обстановки. Розглянуто підходи до реалізації зазначеної ідеї на прикладі роботи з даними про КА. Визначено функціонал відкритого програмно-алгоритмічного забезпечення, який складається з п'яти основних блоків:

1. Оцінювання космічної обстановки:
   - пошук нових джерел інформації;
   - аналіз апріорної інформації про КА (до виведення його на робочу орбіту);
   - відслідковування запусків КА;
   - аналіз апостеріорної інформації про КА (під час його оперативного використання);
   - відслідковування маневрів КА;
   - відслідковування фактів здійснення корекцій орбіт КА;
   - проведення перспективного і ретроспективного аналізу руху КА;
   - оцінювання можливостей бортових інформаційних комплексів КА, орбітального угруповання КА тощо;
   - оцінювання достовірності й точності інформації про космічні системи та КА;
2. Формування початкових умов для проведення розрахунків:
   - отримання (добування) даних про орбітальне положення КА;
   - перевірка актуальності початкових умов руху КА;
   - уточнення початкових умов руху КА з бази даних;
   - формування орбітальних угруповань КА для проведення розрахунків;
   - визначення зон (об'єктів) інтересу на земній поверхні;
   - врахування додаткових вхідних даних у визначених зонах (на об'єктах) інтересу;
3. Формування вихідної інформації:
   - проведення розрахунків польоту та можливостей КА;
   - відображення результатів розрахунків;
   - формування вихідних документів у текстовій та графічній формах;
4. Ведення бази даних:
   - уточнення статусу КА (оперативне використання, резерв, випробування, недіючий);
   - класифікація КА (визначення призначення, державної належності, типу орбіти тощо);
   - оновлення початкових умов руху КА в базі даних;
   - архівація початкових умов руху КА для ретроспективного аналізу;
   - архівація результатів проведення розрахунків (за потреби);
5. Доведення вихідної інформації до споживачів:
   - відображення загальної космічної обстановки (поточне, перспективне, ретроспективне);
   - доведення вихідних документів до віддалених споживачів (за потреби).

Функціонал спеціалізованого програмно-алгоритмічного забезпечення, в якому циркулює інформація з обмеженим доступом, є динамічним і залежить від його призначення, цілей та завдань. Проте, за умови наявності декількох кінцевих споживачів закритої інформації побудова архітектури програмно-алгоритмічного забезпечення має базуватися на децентралізованому принципі, що дозволить забезпечити повноту і достовірність вхідних даних та зменшити час на доведення (отримання) вихідної інформації і знизити ризик її витоку.

Представлено особливості реалізації основних сценаріїв, що стосуються оновлення та реплікації бази даних, відображення космічної обстановки, відслідковування маневрів та корекцій орбіт КА.

Перспективами подальших досліджень визначено практична реалізація зазначених досліджень, розроблення основних сценаріїв виконання часткових завдань оператором

відкритого програмно-апаратного комплексу з подальшим пошуком нових організаційних та технічних (програмних) шляхів удосконалення процесу аналізу стану та змін космічної обстановки в інтересах конкретних споживачів.

УДК 004.422.81

Зибіна К. В., Тарасов Р. О.

ІНФОРМАЦІЙНА СИСТЕМА ПІДТРИМКИ ВИБОРУ АЛЬТЕРНАТИВНИХ ДИСЦИПЛІН

Висококласні спеціалісти мають попит в усіх сферах діяльності, а особливо в IT індустрії. На жаль, навчальна програма в її класичному розумінні не може надати всю цілісність знань через те, що студенти обмежені у виборі дисциплін. Саме тому університети впровадили можливість вибору альтернативних дисциплін, які відрізняються за напрямами та переліком компетентностей, яких студент набуде після опанування цих дисциплін.

Процес вибору альтернативних дисциплін є дуже трудомістким. Спочатку студенти повинні записати ті дисципліни, які вони бажають засвоїти у наступних семестрах. Далі адміністратор формує списки студентів до цих дисциплін. З урахуванням того, що необхідно зробити ці дії для усіх навчальних років, а кількість студентів на потоці нараховує декілька сотень, ця робота стає дуже важкою для виконання вручну.

З предметної області можна виділити три ключові етапи, які потребують автоматизації:

- додавання студентів та дисциплін до бази даних;
- обробка вибору студентів;
- формування списків студентів.

В якості додаткового функціоналу користувач зможе переглядати найбільш популярні дисципліни серед студентів, що дасть змогу в наступному навчальному році корегувати навантаження викладачів та максимальну/мінімальну кількість груп для цієї альтернативи.

Інформаційна система реалізована у вигляді веб-додатку.

Спочатку адміністратор додає студентів та дисципліни до бази даних; це можна зробити вручну чи імпортувати таблицю Excel, що значно скорочує час.

Далі студент входить до системи, щоб обрати певну кількість дисциплін на наступний навчальний рік. Студент робить вибір одразу на 2 семестри наступного навчального року. Слід зазначити, що студент не тільки обирає ту кількість дисциплін, що йому потрібна, а й виставляє пріоритети свого вибору. Система фіксує вибір студента та зберігає його у базі даних. Коли час, передбачений адміністратором буде вичерпано, то система закриває можливість вибору.

Наступним кроком йде автоматичне формування списків зі студентами до кожної дисципліни. Для кожної дисципліни є ряд обмежень, що задаються через форму редагування предметів; такими обмеженням є:

- максимальна/мінімальна кількість груп;
- максимальна/мінімальна кількість студентів в групі;
- необхідність проходження співбесіди;
- результат проходження співбесіди (за необхідності);
- середній/мінімальний бал атестату.

Обмеження «необхідність проходження співбесіди» залежить від того, чи хоче лектор цієї дисципліни організувати додаткове інтерв'ю зі студентом. Це зумовлено тим, що деякі альтернативні дисципліни потребують базових знань з математики чи програмування. І при низькому рівні базових знань викладач може відмовити у проходженні цього курсу.

Мінімальний бал атестату є необхідною умовою при виборі альтернативних дисциплін. За умови, якщо на одну альтернативу претендує велика кількість студентів, то від-

бір проводиться на основі середнього балу студента. Викладачі, що читають курс, мають право також зазначати мінімальний бал атестату.

Також система передбачає наступну функцію. Якщо студент не зміг, не захотів чи не встиг заповнити свою анкету із вказанням альтернатив, то система автоматично зараховує його на предмет згідно з обмеженнями по цьому предмету.

В результаті адміністратор отримує таблицю з усіма студентами та має можливість експортувати її в файл Excel. Приклад розподілення студентів по групам можна побачити на рисунку 1.

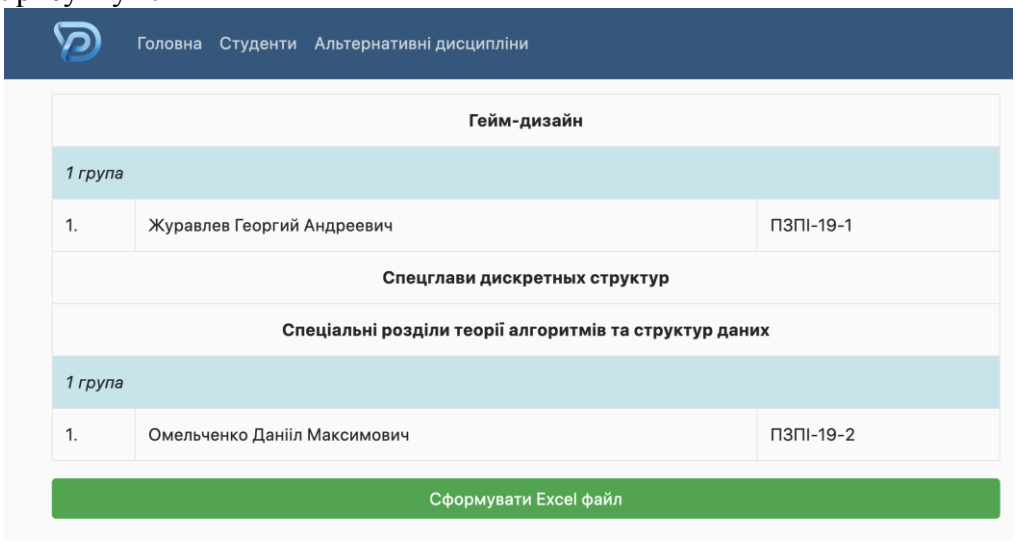


Рисунок 1 – Таблиця з розподіленими студентами за альтернативними дисциплінами

Усі дані інформаційної системи «Підтримка вибору альтернативних дисциплін» зберігаються в об’єктно-реляційній базі даних PostgreSQL. Веб-додаток був розроблений за допомогою фреймворка Django та мови програмування Python.

Таким чином, розроблена інформаційна система значно полегшує роботу по розподіленню студентів по альтернативам. Були виконані наступні задачі автоматизації – додавання студентів з файлу Excel, додавання альтернативних дисциплін з файлу семестрової роботи, розподіл студентів на групи за альтернативними дисциплінами.

Список використаних джерел

1. Теория и практика построения баз данных. 8-е изд. / Д. Кренке. СПб.: Питер, 2003. 800 с.: ил.

УДК 621.37:621.391

Сербин В. В., Рассомахін С. Г.

ЛІНІЙНА АЛГЕРБРАЇЧНА ОБРОБКА СКЛАДНИХ СИГНАЛЬНИХ КОНСТРУКЦІЙ

У сучасних умови, що характеризуються складністю завдань, що вирішуються радіосистемами, і різноманітністю обстановки при постановці противником електромагнітних завад, розробка досить досконалих систем можлива лише на базі сучасних методів оптимізації. Загальну проблему синтезу радіотехнічних систем умовно можна поділити на дві приватні задачі: вибір «найкращих» сигналів для досягнення необхідного результату з урахуванням реальної обстановки і оптимальна обробка сигналів.

Головне завдання прийому сигналів зводиться до найкращого відновленню корисної інформації по сигналу, який викривлений при поширенні, і приймається спільно з перешкодами, які мають природний або навмисний характер. Викривлення сигналу і наявність перешкод зменшують ймовірність правильного прийому переданого інформаційного повідомлення, порушуючи його цілісність і сприяючи реалізації загроз інформаційної безпеки.

Побудова ефективних систем передачі інформації (СПІ) в даний час нерозривно пов'язана з проблемою збільшення використання тимчасового і частотно-енергетичного ресурсу фізичних каналів зв'язку. Одним з найбільш поширених прикладів такого вирішення проблеми є застосування сигналів з фазочастотною модуляцією, що використовують набори гармонійних коливань, кожне з яких модульоване по фазі. Забезпечення ортогональності гармонійних коливань привело до інтенсивного використання одного з найбільш перспективних видів сигналів – OFDM (Orthogonal Frequency Division Multiplexing). Складність структури таких сигналів є причиною істотних труднощів при вирішенні задач демодуляції і радіомоніторингу. Тому вдосконалення методів автоматичного цифрового аналізу багаточастотних багатофазних сигналів є досить актуальним завданням.

У доповіді розглядається математична модель представлення та обробки OFDM структур та запропонований метод алгебраїчної обробки складних сигнальних конструкцій,що дозволяє зробити демодуляцію сигналу шляхом вирішення *систем лінійних алгебраїчних рівнянь* без використання методу швидкого перетворення Фур'є.

УДК 004.03:658.15

Васильцова Н. В., Путятін В. П.

ОБЛІК ТА АНАЛІЗ ДИНАМІКИ ЗМІНЕННЯ КАДРОВИХ СТРАТЕГІЙ В СИСТЕМІ УПРАВЛІННЯ ПЕРСОНАЛОМ ОРГАНІЗАЦІЇ

У теперішній час розвиток країни характеризується серйозними змінами в її політичній, економічній та соціальній сферах. Саме в такі зламні періоди життя організації та підприємства різко змінюють стратегію своєї діяльності, наприклад, приймають рішення про відмову від яких-небудь видів діяльності, розділення організації на декілька частин або злиття її з іншими організаціями тощо. Кожний такий поворот пов’язаний із стратегічними рішеннями в області управління персоналом, а, отже, з обліком, контролем та аналізом динаміки змінення кадрових стратегій [1].

Згідно з постулатами стратегічного кадрового менеджменту цикл стратегічного управління складається з наступних основних етапів: стратегічний аналіз діяльності персоналу організації; формулювання кадрової стратегії; передача стратегії в підрозділ організації; реалізація стратегії; моніторинг діяльності; прийняття та здійснення коригуючих дій.

Процес стратегічного управління персоналом є безперервним та являє собою замкнений цикл [1]. Аналіз процесу стратегічного управління персоналом показав, що для побудови такого циклу найчастіше використовуються вже відомі концепції [1-3]: концепція системи збалансованих показників (Balanced Scorecard – BSC); концепція цілеполагання SMART; концепція ключових показників діяльності (KPI); концепція STEP-аналізу, на основі якої здійснюється вивчення зовнішнього оточення організації; концепція SWOT-аналізу (SWOT – «сила» (strength), «слабкість» (weakness), «можливості» (opportunities), «загрози» (threats)), як інструментарію розробки та оцінювання альтернативних варіантів стратегії.

Ці та інші концепції допомагають створити ефективну стратегію розвитку організації, яка повинна бути заснована на правильно підібраних довгострокових цілях, глибокому розуміння потреб ринку й конкурентного оточення, на реальній оцінці власних ресурсів і можливостей. Однак специфіка людських ресурсів, як об’єкта стратегічного

управління, потребує адаптації даних концепцій з метою використання їх в інформаційних системах управління персоналом організації [4].

В роботі пропонується автоматизована методика обліку та аналізу динаміки змінення кадрових стратегій в системі управління персоналом організації. Розроблена методика заснована на таких концепціях: концепції KPI, яка враховує як виробничі, так й особисті показники діяльності персоналу; концепції BSC; концепції SWOT-аналізу, яка враховує використання профілю середовища й аналізу матриці можливостей та загроз.

На першому кроці використання методики виявляються сильні й слабкі сторони організації в області управління персоналом, а також можливості, які вона має, й загрози, яких треба уникнути. Для автоматизації даного кроку методики попередньо формується база даних існуючих (можливих) показників (ключових показників діяльності (KPI)), яка коригується з урахуванням специфіки конкретної організації.

Формування KPI здійснюється в рамках концепції BSC, яка пропонує формування так званих стратегічних карт, які згруповують цілі й показники діяльності персоналу за чотирма категоріями (перспективами): «фінанси» (фінансові цілі розвитку й результати роботи організації – прибуток, рентабельність тощо); «клієнти та ринки» (цілі присутності на ринку й показники якості обслуговування клієнтів – освоювання ринків і територій продажу, час виконання замовлень, «ідеальне замовлення» тощо); «процеси» (вимоги до ефективності процесів – вартість, час, кількість помилок, ризикованість тощо); «розвиток» (цілі пошуку нових технологій та підвищення кваліфікації персоналу).

Далі з бази даних вибираються показники, що характеризують сильні й слабкі сторони організації, можливості та загрози, й формуються відповідно чотири множини показників, які надалі будуть аналізуватись з використанням конкурентного профілю організації. Оцінка показників проводиться методом порівняльного аналізу, а функцій управління – методом експертного оцінювання. Результат оцінювання показників і динаміка їх змінення може бути представлена у вигляді графіків і гістограм.

Формалізація кроку методики, який враховує пріоритетність напрямів стратегії управління персоналом, пов’язана з формуванням бінарного відношення, яке надається у вигляді матриці. Перша координата кортежу, який є елементом відношення, представлена показником сильних або слабких сторін організації, друга координата – показником можливостей або загроз. Кортежі, які складають відношення, розташовуються з урахуванням пріоритетності спрямувань. Для обліку обмежень в матрицю відношень на перехрещенні рядків і стовпчиків пропонується ввести кількісний показник, який характеризує заданий критерій вибору стратегії (об’єми відокремлених ресурсів, часові обмеження, наявність достатнього професійно-кваліфікаційного рівня персоналу тощо).

Методика, що запропонована у роботі, дозволяє враховувати динаміку змінення стратегії управління персоналом організації, здійснювати вибір стратегії управління персоналом на основі систематичного аналізу факторів зовнішнього та внутрішнього середовища (зокрема виробничих та особистих KPI), в результаті чого може бути представлена концепція розвитку персоналу організації в цілому.

Список використаних джерел

1. Дериховська В. І. Взаємозв’язок розвитку персоналу та стратегії управління персоналом / В. І. Дериховська // Бізнес Інформ. – 2013. – № 7(426). – С. 341–347.

2. Антощишина Н. І. Сучасний погляд на систему управління персоналом в аспекті забезпечення конкурентоспроможності [Електронний ресурс] / Н. І. Антощишина, Д. О. Малюкіна // Електронне наукове фахове видання. Ефективна економіка. – 2014. – №9. – Режим доступу: http://www.economy.nayka.com.ua. – Загол. з екрана.

3. Кизим М. О. Збалансована система показників: монографія / М. О. Кизим, А. А. Пилипенко, В. А. Зінченко. – Харків: ВД "Інжек", 2007. – 192 с.

4. Василів Б. В. Інформаційні системи в менеджменті / Б. В. Василів. – Рівне, 2008. – 167 с.

УДК 351.741:[621.397.4+004]

Мордвинцев М. В., Хлєстков О. В., Ницюк С. П.

ЗАРУБІЖНИЙ ДОСВІД ВИКОРИСТАННЯ ТЕХНІЧНИХ ПРИЛАДІВ І ТЕХНІЧНИХ ЗАСОБІВ ФОТО- І КІНОЗЙОМКИ, ВІДЕОЗАПИСУ

Для забезпечення громадської безпеки в розвинених країнах масово використовують системи фото- і кінозйомки, відеозапису. На базі цих пристроїв створюються інтелектуальні системи, що дозволяють не тільки аналізувати обстановку, але і прогнозувати розвиток подій і в найкоротші терміни генерувати рекомендації для управління силами і засобами, які забезпечують громадську безпеку. Все частіше в США, Західній Європі, Китаї Росії з метою забезпечення громадської безпеки використовуються системи зі штучним інтелектом (далі – ШІ) які поєднуються з системами відео спостереження [1].

Досвід Китаю. Правоохоронні органи Китаю користуються допомогою багатьох високотехнологічних ШІ-компаній (розробки в сфері штучного інтелекту). До кінця 2020 року на китайський ринок надійдуть 450 млн нових камер. Понад 400 банків Китаю вже впровадили технологію розпізнавання облич мережах банкоматів.

Китайські вчені вже розробили систему розпізнавання облич, яка здатна виявити в натовпі потрібну людину з точністю до 99,8 % з 91 ракурсу. Програма може знаходити відмінності між ідентичними близнюками, розпізнавати дуже загримованих осіб, а також ідентифікувати людину, щільно укутану в одяг.

Китайська поліція тестує технологію розпізнавання людей за ходою. Програмне забезпечення може ідентифікувати людину на відстані 50 м від точки зйомки, навіть якщо в неї приховано обличчя або віна стоїть до відеокамери спиною.

Необхідно відзначити, що для боротьби з поширенням коронавірусу в цій країні широко застосовуються звичайні та інфрачервоні камери з використанням систем ШІ для вимірювання температури тіла людини і фіксації лиця з метою подальшого його визначення в натовпі [2]. Вони широко застосовуються в місцях з високою щільністю пасажиропотоку, таких як метрополітен, автобусні станції, залізничні станції та аеропорти і дозволяють швидко ідентифікувати людей, які можуть мати підвищену температуру тіла, а також виключити з ними фізичний контакт.

Досвід Сполучених Штатів Америки. Крім системи розпізнавання облич, в США застосовується система ShotSpotter. Це система пов’язаних між собою акустичних датчиків, здатних забезпечити покриття міста. Система, оснащена кількома звуковими датчиками, може підбирати тип вогнепальної зброї згідно із зафіксованими звуками, а алгоритм машинного навчання, використовуючи тріангуляційні алгоритми, визначати координати місця події [3].

Досвід Ізраїлю (віброкамери). Ізраїльська компанія «Cortica», яка працює в сфері безпеки і досліджень ШІ, проводить аналіз терабайтів даних, переданих з камер відеоспостереження у громадських місцях [4]. Її метою є підвищення безпеки у громадських місцях. Використання ШІ у системах відеоспостереження спрямоване насамперед на попередження злочинів. Дослідження та виробництво систем «Cortica» направлені на пошук поведінкових аномалій у рухах людини, які сигналізують про те, що вона збирається вчинити злочин [4].

Досвід Росії (віброкамери). В Росії інтенсивна розробляються системи віброкамер. Віброкамера реєструє мікрорухи, на основі аналізу яких можна отримати будь-яку інформацію про людину. Кожна частина тіла людини здійснює власні рухи, по-своєму вібрує. Око може цього не помітити. Віброкамера фіксує всі незначні (десятки мікрон) мікрорухи людини, потім за частотою вібрацій система аналізує її психологічний стан [5].

Віброкамери встановлені в аеропортах, на стадіонах, у метрополітені й у великих супермаркетах, де вони стежать за безпекою людей та виявляють потенційних правопорушників.

В Україні прийнято ряд нормативних документів, що регламентують впровадження си-

стеми фото- і кінозйомки, відеозапису в Національній поліції. Створено Управління організації діяльності підрозділів поліції на воді та повітряної підтримки, ефективно працює Єдиний аналітично-сервісний центр (UASC) в Донецькій області, патрульна поліція використовує персональні відеореєстратори, їх автомобілі обладнані системами відеозапису.

Список використаних джерел

1. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду : методичні матеріали для працівників підрозділів поліції / [уклад. В. А. Коршенко, М. В. Мордвинцев, Ю. В. Гнусов, В. В. Чумак, В. А. Світличний] ; МВС України, Харків. нац. ун-т внутр. справ. – Харків, 2020. – 44 с.

2. China uses AI to combat the novel coronavirus outbreak // Tsinghua University/Megvii сайт 18.02.2020 URL: https://healthcare-in-europe.com/en/news/china-uses-ai-to-combat-the-novel-coronavirus-outbreak.html

3. Коротенко Г. М., Коротенко Л. М., Косиченко О. О. Застосування технологій штучного інтелекту для підвищення швидкості розкриття злочинів // Використання сучасних інформаційних технологій в діяльності Національної поліції України : матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 23 листоп. 2018 р.) / МВС України, Дніпропетровськ. держ. ун-т внутр. справ. Дніпро, 2018. С. 32-34.

4. John R. Quain. Crime-predicting A.I. isn’t science fiction. It’s about to roll out in India / Digital Trends, Nov., сайт. 11.04.2018 URL: https://www.digitaltrends.com/cool-tech/could-ai-based-surveillance-predict-crime-before-it-happens

5. Минкин В. А. Технология виброизображения, 20 лет спустя // Современная психофизиология. Технология виброизображения : тр. 1-й Междунар. науч.-тех. конф. (Санкт-Петербург, Россия, 28–29 июня 2018 г.) / под ред. В. А. Минкина. СПб. : Элсис, 2018. С. 7-14.

УДК 338.46

Громова В. С.

ПРИНЦИП ЭЛЕКТРОННОГО «ОДНОГО ОКНА» КАК СРЕДСТВО ДЛЯ ЭФФЕКТИВНОГО ПРИНЯТИЯ РЕШЕНИЙ

Современные тенденции развития информационных технологий вносят свой вклад и преобразовывают множество сфер деятельности. С переходом большинства отраслей на «электронные» виды деятельности, например электронный документооборот, преобразовались и некоторые понятия. Так, на смену принципу «одно окно» в 21-м веке, пришло понятие «электронное «одно окно».

Принцип электронного «одного окна» – технология предоставления услуг для граждан и бизнеса посредством информационного-коммуникационных технологий (ИКТ). Данный принцип проник во многие сферы деятельности. Например, в России принцип электронного «одного окна» реализуется в системе межведомственного электронного взаимодействия, благодаря которой граждане и организации могут получать государственные услуги в многофункциональных центрах и на портале государственных услуг. В Китае разработана и используется система электронного учреждения предприятий [1].

В Республике Беларусь данный принцип активно внедряется в таможенную сферу. Реализуется электронное декларирование, сформирована основа для расширения информационного взаимодействия между министерствами и организациями, выдающими разрешения на перемещение товаров через таможенную границу, ведется работа по повышению эффективности обмена информацией между участниками международной

торговли и правительственными учреждениями – реализации принципа «одно окно» при таможенном декларировании и др.

ИКТ позволяют организовать относительно недорогой информационный обмен в рамках оказания государственных услуг и удешевить технологию «одно окно». При этом появляется возможность разделять территориально офисы по взаимодействию с заявителями («фронт-офисы») и офисы, где происходит обработка информации и принятие решений органами власти («бэк-офисы»). Повышается оперативность процедур информационного обмена и, следовательно, оперативность предоставления коммерческих или государственных услуг [2].

Помимо физических точек доступа к службам «одного окна», посредством применения современных ИКТ, можно реализовать возможность обращения не выходя из дома через Интернет-порталы. Так перспективным направлением реализации принципа электронного «одного окна» в Республике Беларусь будет осуществление с его помощью подачи пакета документов для регистрации в качестве резидента свободной экономической зоны, что создаст привлекательные условия для привлечения инвесторов, преимущественно зарубежных. Применение ИКТ способствует эффективному принятию важных решений.

Список использованных источников

1. Громова В. С., Полоник И. С. Модель инновационного развития Республики Беларусь на основе опыта Китайско-Сингапурского индустриального парка «Сучжоу» // Новая экономика. – 2018. – №2. – С. 43-52.

2. Одно окно [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Одно_окно. – Дата доступа: 05.03.2020.

Прасол И. В., Ерошенко О. А.

ЭЛЕКТРОМИОГРАФИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПРИ ВЫПОЛНЕНИИ ПРИЦЕЛЬНЫХ ДВИЖЕНИЙ

Исследование механизмов регуляции движений, обеспечивающих достижение успешного результата, является одной из центральных проблем физиологии.

При изучении этой проблемы используется разнообразный спектр методических подходов, причем особенный размах приобрели тонкие нейрофизиологические исследования, благодаря которым получены точные сведения о функционировании нервных и мышечных структур, входящих в систему управления движениями. Но такие исследования не могут заменить изучение целостных двигательных действий, их функциональной структуры, принципов, на которых они строятся и закономерностей достижения необходимого результата.

Среди основных факторов, влияющих на качество стрельбы, важная роль принадлежит процессам прицеливания, выстрела и сохранения устойчивого положения стрелка.

Интегрированная электрическая активность складывается из значений амплитуды и частоты биопотенциалов. Причем повышение интегрированной электроактивности может происходить преимущественно как за счет увеличения амплитуды потенциалов действия, так и возрастания их частоты.

Для выполнения точного выстрела из пистолета необходим оптимальный баланс проявлений мышечных усилий целого ряда скелетных мышц. Исходя из этого, при выполнении выстрела в тренировочные занятия целесообразно включать методы биоуправления мышечной активностью на основе электромиографии (ЭМГ). Такие методы позволят оперативно корректировать структуру ЭМГ паттернов определенных мышц в конкретной фазе выстрела и потенциально способствовать повышению результативности стрельбы.

Основным методом исследования записи электрической активности мышц была поверхностная электромиография. Отведение и регистрация биопотенциалов скелетных

мышц осуществлялись по общепринятой методике. Во время выполнения выстрела на выявленных мышцах закреплялись электроды [1].

При исследовании стрелков были определены следующие скелетные мышцы, которые предположительно обеспечивают реализацию выстрелов из пневматического пистолета: мышцы правой руки (лучевой сгибатель кисти, локтевой разгибатель кисти, двуглавая плеча, трехглавая плеча, дельтовидная), билатеральные мышцы груди и спины (большие грудные, трапециевидная, выпрямляющие позвоночник), билатеральные мышцы нижних конечностей (двуглавая бедра, прямая бедра, икроножная, передняя большеберцовая) [2-3].

Ведение огня из пистолета выполнялось из положения стоя с одной руки (рис. 1). Ступни ног расставлены на ширину плеч и развернуты под углом 40-60° по отношению друг к другу. С учетом индивидуальных особенностей строения тела в стойку могут быть незначительные отклонения в ту или иную сторону. Вес тела стреляющего должен равномерно распределяться на обе ноги. Никакого скручивания корпуса допускать нельзя, возможно незначительное отклонение назад с прогибом в пояснице. Обучаемый смотрит в сторону мишени. Сильно поворачивать голову, наклонять ее вперед или откидывать назад не рекомендуется, так как быстро устают шейные мышцы, и теряется контроль за горизонтальным положением целика. Руку, свободную от оружия, нужно расположить на поясе, убрать в карман, за спину или просто положить на кобуру.

Рисунок 1 – Ведение огня из пистолета

При выполнении выстрела из пистолета наиболее задействованы были следующие мышцы: лучевой сгибатель кисти прав. руки; локтевой разгибатель кисти прав. руки; средняя часть прав. дельтовидной; верхние пучки прав. Трапециевидной; выпрямляющая позвоночник лев.; выпрямляющая позвоночник прав.; передняя большеберцовая лев.; передняя большеберцовая прав.

При анализе амплитуды ЭМГ у спортсменов стрелков были выявлены индивидуальные особенности мышечной активности при стрельбе. Применение в тренировочном процессе исследования электрической активности мышц способствует выявлению индивидуальных ошибок и их дальнейшему устранению. Это способствует повышению чувства межмышечной координации стреляющего, а также формированию более устойчивой модели успешного выстрела, характеризующейся оптимальными величинами электроактивности ведущих мышц и потенциально приводит к повышению результативности стрельбы.

Список использованных источников

1. Дацок О. М. Побудова біотехнічної системи м’язової електростимуляції / О. М. Дацок, І. В. Прасол, О. А. Єрошенко // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2019. – № 13 (1338). – С. 165-175.

2. Пухов А.М. Электромиографические критерии результативности стрельбы из пистолета / А.М. Пухов, Р.М. Городничев // Теория и практика физической культуры. – 2012. – №11. – С. 79.

3. Пухов А. М. Закономерности управления движениями у высококвалифицированных стрелков из лука / А.М. Пухов и др. // Теория и практика физической культуры. – 2015. – № 6. – С. 20-22.

Трубицын А. А., Ерошенко О. А.

ОРГАНИЗАЦИЯ БЕСПРОВОДНОЙ СИСТЕМЫ СБОРА МЕДИКО-БИОЛОГИЧЕСКИХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕМЕНТОВ "УМНОЙ ОДЕЖДЫ"

На протяжении многих лет крапивница является распространенным, но в то же время наименее изученных заболеваний. Симптомы крапивницы, особенно зуд, сильно влияют

на качество жизни военнослужащих, имеющих данное заболевание, приводят к нарушению сна и дневной активности, тревожности, депрессии. Холинергическая крапивница (ХК) – тип крапивницы, характеризующийся появлением мелких волдырей в результате стимуляции потоотделения из-за увеличения температуры тела (например, при физической нагрузке) или эмоционального стресса. У пациентов с ХК часто присутствуют сопутствующие атопические заболевания (атопический дерматит, анафилаксия и др.) [1].

Для анализа анамнеза жизни военнослужащего с ХК возможно применение элементов, так называемой, "умной одежды", содержащей ткани электронного текстиля, что может дать врачу важную диагностическую информацию для наблюдения в динамике и выработки рекомендаций для дальнейшего лечения. Измерение уровня влажности (потоотделения) пациента возможно с использованием резистивных и емкостных датчиков на основе электронного текстиля с PEDOT-PSS/PAN нановолоконами, PEDOT-PSS/полиамидами, PEDOT-PSS/лайкрой, тканей, содержащих полисульфон (PES), polysulfone (PSF) [2]. Также устройства, использующие такие волокна, могут быть изготовлены в виде браслета для измерения пульса, уровня кислорода в крови, либо быть интегрированы в повязку для постоянного контроля процесса заживления.

Для уменьшения негативного влияния тепла и влаги на встроенные в ткань электронные компоненты должно быть реализовано свойство «дышащей ткани», что возможно реализацией использованием многослойной комбинации тканей на основе влагоотводящего двухслойного гидрофильного мембранного нановолокна и гидрофобной мембранной хлопковой ткани [3]. Каждый слой ткани обладает определенными свойствами: первый слой из волокна гидрофильного полиакрилонитрила (PAN) непосредственно соприкасается с кожей и впитывает влагу; промежуточный слой из гидрофильного PA6 нановолокна поглощает пот из PAN слоя и распределяет его по своей поверхности; слой гидрофобной "дышащей хлопчатобумажной ткани" предотвращает попадание влаги на электроды.

Для коммутации «умной одежды» с устройством вывода информации в медицинских учреждениях предлагается использовать систему передачи медико-биологической информации, состоящей из сети датчиков, реализованных с использованием «умных тканей». Она может быть построена на основе комбинации протоколов ZigBee и Wi-Fi, что дает возможность объединить преимущества малого энергопотребления, надежности передаваемой информации.

В качестве встраиваемых модулей для организации ZigBee сети можно использовать XBee – устройства компании Digi. Управление данными модулями осуществляется с помощью AT-команд или API-фреймов по USB-интерфейсу. Модули могут работать как автономные узлы без применения внешнего микроконтроллера. Конфигурация узлов для работы в автономном режиме может включать установление интервалов передачи данных от долей секунд до нескольких дней и недель.

Разработка изделий на основе электронного текстиля, связана с проведением исследований нетоксичности используемых материалов, сохранения рабочих характеристик при санитарной обработке, износостойкости, устойчивости к растяжениям, компоновки электронных узлов и увеличения сроков службы. Также необходимо развитие технологий доказательного контроля состояния пациента в динамике на основе анализа изображений [4-6]. Дальнейшее совершенствование технологий применения электронного текстиля в системах передачи медико-биологической информации способно привести значительным достижениям при мониторинге состояния здоровья военнослужащих с хроническими заболеваниями кожи.

Список использованных источников

1. Колхир П. В. Эффективность дапсона в лечении тяжелой хронической холинергической крапивницы / П. В. Колхир, О. Ю. Олисова, Н. Г. Кочергин // Эффективная фармакотерапия. – 2013. – Т.8.

2. Gonçalves C. Wearable E-Textile Technologies: A Review on Sensors, Actuators and Control Elements / Gonçalves C., Ferreira da Silva A., Gomes J., Simoes R. // Inventions. – Том 3. – 2018.

3. Yang W. All-fiber tribo-ferroelectric synergistic electronics with high thermal-moisture stability and comfortability / Weifeng Yang, Wei Gong, Chengyi Hou, Yun Su // Nature communications. – 2019. – Том. 10.

4. Книгавко Ю. В. Алгоритмы программного рендеринга трехмерной графики для задач медицинской визуализации/ Ю. В. Книгавко, О. Г. Аврунин // Журн. Технічна електродинаміка – 2010. – С. 258-261.

5. Yeroshenko O. Organization of a Wireless System for Individual Biomedical Data Collection / O. Yeroshenko, I. Prasol, O. Trubitsyn, L. Rebezyuk // International Journal of Innovative Technology and Exploring Engineering. – Vol. 9. – No. 4. – 2020. – Pp. 2418-2421.

6. Трубицын А. А. Инструментальные методы оценки состояния кожи при атопическом дерматите / А. А. Трубицын, О. А. Исаева, В. А. Клименко, О. Г. Аврунин // Наука та виробництво: міжвуз.темат. зб. наук. пр. / ДВНЗ «ПДТУ». Вип. 20. – Маріуполь, ПДТУ, 2019. – С. 182-188.

УДК 623.55.02

Іохов О. Ю., Малюк В. Г., Ткаченко К. М.

АЛГОРИТМ ВИЗНАЧЕННЯ МЕЖ ЗОНИ ЗАВАДОСТІЙКОГО РАДІООБМІНУ РАДІОПРИЙМАЧА UHF / VHF ДІАПАЗОНУ

На тлі бурхливого розвитку сучасних засобів радіоелектронної боротьби виникла сукупність актуальних проблем в галузі забезпечення необхідних показників стійкості систем зв'язку, зокрема завадостійкості і електромагнітної сумісності радіоелектронних засобів. У цивільній сфері аналогічними є завдання захисту засобів мобільного радіозв'язку UHF / VHF діапазону, офісних і промислових мереж від індустріальних радіоперешкод, перешкод від повітряних ліній електропередачі, високовольтного устаткування тощо. Таким чином, при плануванні військових операцій, будівництві офісних і промислових мереж бажано мати спосіб визначення меж зони перешкодостійкого радіообміну, де забезпечується якісний рівень радіозв'язку.

Запропоновано алгоритм визначення меж максимальної за розміром зони стійкого радіоприйому в діапазоні UHF / VHF для мобільних засобів радіозв'язку в умовах дії системи радіоперешкод. Передбачається використання радіоприймачем спрямованої антени або екрану. Збільшення розмірів зони стійкого радіоприйому забезпечується за рахунок оптимальної орієнтації в кожній її точці антенного пристрою по азимуту і куту місця з використанням моделі каналу радіозв'язку, який дозволяє обчислити відношення сигнал/перешкода з урахуванням просторового розташування джерел радіоперешкод і характеристик цифрованої 3D-діаграми спрямованості антени приймача.

Приклади практичного використання пропонованого чисельного алгоритму дозволяють зробити висновок про несуперечність результатів з даними, отриманими у відомих роботах аналітичним алгоритмом для окремого випадку. У той же час використовуваний чисельний підхід суттєво розширює можливості розрахунків шляхом урахування розташування множинних джерел радіозавад на різних висотах, а також оптимальної орієнтації цифрованої 3D-діаграми спрямованості антенного пристрою приймача сигналу.

Ефективність запропонованого алгоритму підтверджується збільшенням площі зони перешкодостійкого радіообміну у 2,8 раз по відношенню до варіанту використання мобільного радіоприймача зі штирьовою антеною. Для випадку оптимальної орієнтації

спрямованої антени приймача по куту азимута додаткова оптимізація по куту місця дає виграш у 1,5 рази.

УДК 681.518.3

Горєлишев С. А., Байда М. С., Баулін Д. С.

АВТОМАТИЗОВАНЕ РОБОЧЕ МІСЦЕ ПСИХОЛОГА ВІЙСЬКОВОЇ ЧАСТИНИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

В даний час перспективним шляхом розвитку автоматизації процесів управленія є концепція розподілених автоматизованих систем управління (АСУ), спрямованих на локальну обробку інформації. Дана концепція може бути застосована і при організації діяльності фахівців системи психологічного забезпечення Національної гвардії України (НГУ). Це дозволить організувати поділ праці управлінського персоналу, здійснити контроль за діяльністю підлеглих і автоматизувати виконання ними своїх функцій.

Для реалізації цієї ідеї необхідно створити для кожного рівня управління автоматизовані робочі місця (АРМ) на базі персональних комп'ютерів. АРМ фахівця системи психологічного забезпечення – сукупність інформаційно-програмно-апаратних ресурсів, що забезпечують обробку даних в реальному масштабі часу і автоматизацію управлінських функцій діяльності психологічної служби НГ України на всіх її рівнях.

Для забезпечення діяльності органів управління системи психологічного забезпечення НГУ АСУ психологічної служби повинна мати трирівневу ієрархічну структуру і включати: а) АРМи Головного управління НГУ (оперативний рівень); б) АРМи психологічної служби оперативно-територіальних об'єднань НГУ (оперативний та оперативно-тактичний рівні); в) АРМи психологічної служби частин і підрозділів НГУ (тактичний рівень). Передбачається наступні типи АРМ фахівця психологічної служби на тактичному рівні (рівень бригада, полк, окремий батальйон НГУ): АРМ заступника командира частини (по роботі з о/с); АРМ начальника відділення психологічного забезпечення; АРМ начальника служби психологічного забезпечення; АРМ старшого офіцера (психолога) відділення психологічного забезпечення; АРМ офіцера (психолога) відділення психологічного забезпечення; АРМ відповідального виконавця (психолога).

Основна функціональна спрямованість АРМ фахівця психологічної служби: супровід СБД і професійно-психологічна підготовка; професійно-психологічний відбір; вивчення соціально-психологічного клімату; психопрофілактична робота і психологічна реабілітація. Відмінною особливістю АРМ ГУ НГУ, АРМ ОТО, АРМ заступника командира частини є наявність в складі їх АРМ програмних засобів для контролю і координації діяльності підлеглих, де вся управлінська діяльність описується як сукупність процесів, кожний з яких має дати початку, кінця і відповідальних виконавців.

Відмінні особливості АРМ психолога НГ України: тестова бібліотека включає понад 60 психодіагностичних тестів, які оцінюють найважливіші психологічні, психофізіологічні та соціальнопсихологічні характеристики; є як готові проблемно-орієнтовані тестові батареї, так і можливість формування довільної кількості призначених для користувача тестових батарей; для абсолютної більшості реалізованих тестів здійснюється формування і висновок на друк тестових матеріалів (буклетів та бланків), необхідних для проведення групового бланкового психодіагностичного обстеження; розмежування рівнів доступу до системи, що забезпечує необхідну конфіденційність персональних даних; розвинені засоби комплексного аналізу масивів психодіагностичних даних (угруповання, розрахунок тестових норм, рейтингів та ін.); on-line контроль за ходом тестування і апостеріорного контроль достовірності результатів за шкалами валідності. Користувачам АРМ надається персональ-

ний допуск до психологічної інформації у межах передбачених їх функціональними обов'язками.

Визначаються наступні рівні допусків: рівень 1 "максимальний" – повний доступ до психологічної інформації, персональних даних суб'єктів, конфіденційної інформації та інформації з обмеженим доступом; рівень 2 "повний" – обсяг доступу у межах психологічної інформації відносно суб'єктів на яких розповсюджується їх компетенція; рівень 3 "частковий" – обсяг доступу у межах психологічної інформації відносно суб'єктів на яких розповсюджується їх компетенція; рівень 4 "респондент" – доступ до інформації відносно себе особисто, до інших об'єктів – у разі письмового їх дозволу.

Базова конфігурація АРМ психолога включає в себе наступні модулі: 1) меню входу для психолога; 2) модуль відомостей про суб'єктів; 3) модуль – план психологічного забезпечення НГУ; 4) модуль – картка психологічного супроводу об'єкта; 5) модуль результатів психологічного вивчення; 6) модуль професійно-психологічної підготовки; 7) модуль обліку результатів вивчення соціально-психологічного клімату, соціометричних досліджень відносно об'єкту, військового колективу підрозділів, військових частин НГУ; 8) модуль результатів психологічного супроводження виконання службово-бойових завдань; 9) модуль психопрофілактичних заходів; 10) модуль додаткової психологічної інформації; 11) модуль обліку заходів із членами сімей; 12) модуль-конструктор форм звітів. Всі форми звітів повинні бути формалізовані з невеликими можливостями налаштування.

Прасол І. В., Дацок О. М., Єрошенко О. А.

МЕТОД ОЦІНЮВАННЯ СТАНУ НЕРВОВО-М'ЯЗОВОЇ СИСТЕМИ СПОРТСМЕНА

В теперішній час спостерігається зниження рухової активності, а внаслідок – погіршення рівня фізичного розвитку людини. Під час фізичного навантаження можуть розвиватися м'язові спазми, викликані перевтомою м'язових волокон і спазми на тлі дефіциту електролітних іонів. І, якщо спазми втомлених м'язів успішно ліквідуються за допомогою розтягування, масажу і т.д., то електролітні спазми вимагають зовсім інших рішень. Аналогічна ситуація стосується профілактики м'язових судом – для обох різновидів м'язових судом необхідно формувати різні типи фізичного навантаження.

Досвід показує, що одним із ефективних заходів профілактики різних захворювань, особливо серед молоді, є заняття фізичною культурою і спортом з індивідуалізацією виконання фізичних навантажень. Але в той же час, навантаження, що характерні для сучасного спорту і призводять до значних спортивних результатів, досягає важкопередбачуваних величин довгострокової адаптації. Однак, ці навантаження часто є і причиною пригнічення адаптаційних можливостей, припинення зростання результатів, скорочення тривалості виступу спортсмена на рівні вищих досягнень, появи передпатологічних і патологічних змін в організмі (рис. 1) [1].

Для того щоб уникнути пригнічення адаптаційних можливостей спортсмена, необхідна адекватна діагностика стану нервово-м'язової системи [2, 3].

Перспективним підходом для підтримки динаміки функціонального потенціалу є застосування біотехнічного зворотного зв'язку. Контуром біотехнічної зворотного зв'язку передаються електричні параметри, що характеризують біологічний стан об'єкта. На основі цієї інформації відповідно до цільової функції проводиться автоматичне керування параметрами сигналу впливу. таким чином, здійснюється узгодження параметрів біооб'єкту і технічних компонентів системи, вироблення оптимального лікувального впливу [4, 5].

Стимуляція м'язової тканини здійснюється за допомогою спрямованого збудження і скорочення певної групи м'язів, причому збудження формується не одночасно, щоб по-

силити обмінно-трофічні процеси, які спрямовані на забезпечення роботи м'язів енергетичним запасом.

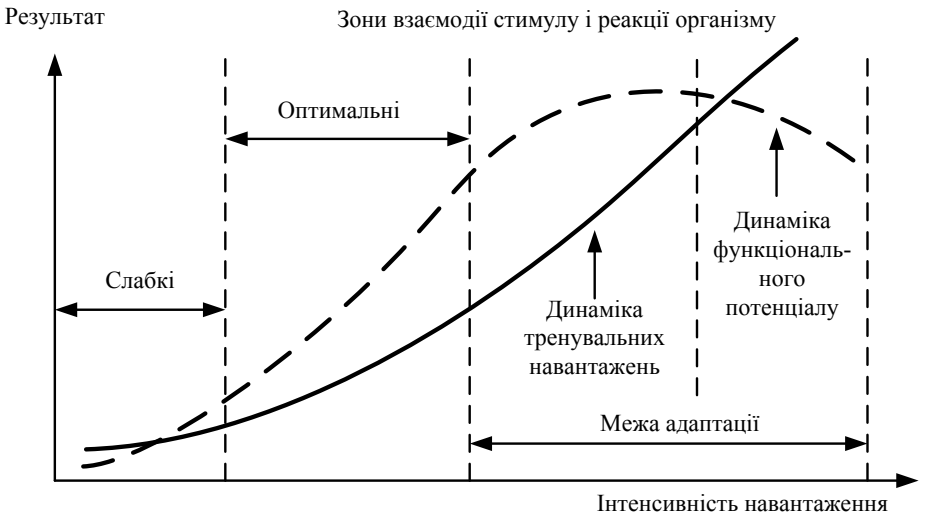


Рисунок 1 – Схема взаємодії тренувальних навантажень і функціонального потенціалу організму

Важливою властивістю нервово-м'язових структур під час подразнення електричними сигналами є залежність збуджуваності від швидкості зміни амплітуди стимулюючого сигналу [6].

Опір міжелектродного кола залежить від сили струму, характер залежності відповідає розчину електроліту – чим менше щільність струму, тим більше опір кола.

При проведенні електростимуляції нервово-м'язового апарату важливий раціональний вибір її режимів і поєднання тонічних і кінетичних скорочень; це суттєво впливає на збільшення маси, розвиток сили, підвищення збудливості і працездатності м'язів.

Таким чином, застосування електричної стимуляції нервово-м’язового апарата спортсмена системою з біотехнічним зворотним зв'язком дозволить краще дозувати фізичне навантаження, оптимізувати співвідношення між динамікою тренувальних навантажень та функціональним потенціалом м’язів, що може бути запорукою покращення спортивних результатів. Аналітичні залежності ефективності спортивних результатів від програми фізичних навантажень в даній системі потребують подальших досліджень.

Список використаних джерел

1. Платонов В. Н. Двигательные качества и физическая подготовка спортсменов. К.: Олимп. лит., 2017. 656 с.: ил.

2. Сивохов В. Л. Современные методы функциональной диагностики в спорте / В. Л. Сивохов, Е. Л. Сивохова // Вестник Красноярского государственного педагогического университета им. В. П. Астафьева. Красноярск, 2007. С. 68-74.

3. Цинкер В. М. Оценка адаптационного потенциала организма спортсменов на различных этапах спортивной тренировки / В. М. Цинкер, Д. В. Дугарова // Вестник Бурятского государственного университета. Педагогика. Филология. Философия. 2011, С. 159-162.

4. Дацок О. М. Побудова біотехнічної системи м’язової електростимуляції / О. М. Дацок, І. В. Прасол, О. А. Єрошенко // Вісник НТУ «ХПІ». Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2019. – № 13 (1338). – С. 165-175.

5. Осипов А. Н. Сложная биотехническая обратная связь в системах электростимуляции / А. Н. Осипов, С. К. Дик, К. Г. Сеньковский // Медицинская техника. Москва. 2002, № 6. С. 27-29.

6. Ерошенко О. А. Информационные технологии определения параметров стимулов систем электромиостимуляции / О. А. Ерошенко, И. В. Прасол // Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку: матеріали Міжнар. наук.-практ. конф. 14-15 бер. 2018 р., м. Харків: НАНГУ. 2018, С. 122-124.

Страшненко Г. М., Місроп'ян Є. І.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЛІКАРЯ-АНЕСТЕЗІОЛОГА ПРИ АБДОМІНАЛЬНОМУ РОЗРОДЖЕННІ

Вибір анестезіологічного забезпечення при кесаревому розтині (КР) в сучасному акушерстві набуває особливої актуальності, оскільки має сприяти адекватному захисту вагітної від операційного стресу та створити оптимальні умови адаптації плода. Анестезіолог в сучасному акушерстві грає набагато більшу роль, ніж просто ведення наркозу при КР і надання допомоги в найближчому післяпологовому періоді. Незважаючи на наявність численних схем анестезії при абдомінальному розродженні, до сих пір триває пошук альтернативних оптимальних методів та засобів. Велике значення для вирішення цього питання надається інформаційним технологіям.

Метою роботи є розробка інформаційної технології підтримки прийняття рішень лікаря-анестезіолога на базі методу вибору анестезіологічного забезпечення при абдомінальному розродженні з використанням аналітичних мереж.

Одним з ключових питань синтезу інформаційної технології підтримки прийняття рішень є розробка її математичного забезпечення.

Концепція методу вибору анестезіологічного забезпечення при абдомінальному розродженні базується на реалізації наступних етапів.

На першому етапі вибору оптимального методу анестезії як альтернативи виступають: багатокомпонентна загальна внутрішньовенна анестезія на тлі тотальної міоплегії з проведенням штучної вентиляції легень та спінальна анестезія. При консультації з практикуючими лікарями-експертами було визначено наступний перелік критеріїв (групи ознак), на підставі яких вибирається той чи інший метод анестезії: анамнез; соматичний статус; лабораторні дані; дані за шкалою анестезіологічного перинатального ризику; показання до оперативного розродження; стан плода (частота серцевих скорочень за 1 хв.). Підкритеріями виступають градації кожного діагностичного показника, які були визначені експертним шляхом.

Далі на підставі наведених вихідних даних та сформульованих критеріїв, будується мережна модель для вибору оптимального методу анестезії при КР і на основі експертних суджень формуються матриці парних порівнянь (МПП). За отриманими МПП визначаються вектори пріоритетів альтернатив, критеріїв та підкритеріїв. Для цього спочатку обчислюються локальні пріоритети та відбувається визначення узгодженості оцінок і помилки узгодженості в МПП.

На підставі отриманих векторів локальних пріоритетів формується суперматриця, яка приводиться до стохастичного виду та зводиться в граничні ступені. З граничної суперматриці для задачі вибору анестезіологічного забезпечення при КР визначаються граничні пріоритети.

На заключному етапі визначаються результуючі пріоритети альтернативних методів анестезії при КР та формується лікувально-діагностичний висновок.

Розроблений метод був покладений в основу інформаційної технології підтримки прийняття рішень лікаря-анестезіолога при абдомінальному розродженні. Для високорівневого опису інформаційної технології в функціональному аспекті були створені моделі в нотації IDEF0. Для побудови контекстних діаграм використовували середовище BPwin.

Застосування розробленої інформаційної технології в акушерській практиці дозволить забезпечити підтримку прийняття рішення в задачі вибору анестезіологічного забезпечення при абдомінальному розродженні, що необхідна практикуючим лікарям-анестезіологам та сприятливе вплине на зниження материнських та перинатальних ризиків.

УДК 621.396

Чумак Б. О., Ведмідь О. І., Кривчун В. І., Квіткін К. П.

ПОКАЗНИКИ ДОСТОВІРНОСТІ ТРАЄКТОРНОГО КОНТРОЛЮ РУХУ ЛІТАЛЬНИХ АПАРАТІВ В РАДІОТЕХНІЧНИХ ВИМІРЮВАЛЬНИХ СИСТЕМАХ

Для забезпечення контролю різноманітних літальних апаратів (ЛА) під час визначення та прогнозування їх траєкторій, а також управління їх рухом використовуються наземні радіотехнічні системи (РТС). Однак, на сьогоднішній день жодна з систем не виконує оцінки достовірності отриманої інформації, особливо в реальному масштабі часу при визначенні параметрів руху ЛА.

Авторами проаналізований процес встановлення відповідності між компонентами вектора стану ЛА та заданою нормою щодо них у відповідні моменти часу шляхом визначення навігаційних функцій, порівняння їх з межами допусків, формування та видачі вихідних даних про результати вимірювань та порівнянь. Показано, що при цьому мають бути вирішеними наступні основні задачі: одержання інформації про значення навігаційних функцій ЛА, що контролюється; порівняння цих значень з допустимими; видача результатів порівняння (обробка одержаної інформації).

Аналіз показує, що нажаль на сьогоднішній день відсутні засоби контролю, в яких реалізується вирішення другої та третьої задачі. Таким чином, для вірного вирішення наведених вище задач слід виконати такі функції як: вибір показників якості функціонування РТС в цілому, або її окремих елементів; визначення допустимих значень щодо меж величин параметрів руху ЛА та допустимих похибок їх визначення; розробити методику порівняння зазначених (або перерахованих у визначений простір) величин з урахуванням вимог оперативності визначення результату та прийняття певного рішення; провести дослідження корисності результатів виконання операцій, а також визначення кількісної оцінки показників ефективності системи контролю.

Аналіз моделі функціонування РТС комплексів контролю і управління ЛА в штатному режимі роботи показав, що ЛА як об’єкт траєкторного контролю в ній характеризується наступним: в залежності від режиму роботи засобів контролю кількість компонентів вектору стану, що контролюється має бути від 6 до 8 у кожний момент часу; обсяг вимірювань зростає безперервно під час сеансу зв’язку; вимірювані параметри руху мають досить великий діапазон змінювання значень; вимоги, щодо допустимих меж похибок вимірювань параметрів руху мають визначатися для кожного випадку окремо; балістичне забезпечення повинно мати в розпорядженні відповідні еталонні моделі руху ЛА з метою врахування особливостей руху різних типів ЛА; для вимірювань використовується велика кількість засобів, що володіють різними показниками якості функціонування; наявність завад та шумів призводить до того, що вимірювані параметри руху стають випадковими функціями часу.

Для такої моделі спостереження запропонований метод, при якому оцінюється відомий параметр, а саме: відстань між двома фазовими центрами антен ЛА. При цьому доведено, що знаючи закони розподілу вимірюваного параметру та погрішності їх вимірювань, можна визначати необхідну точність вимірювальних каналів РТС і допуски меж похибок вимірювань.

УДК 623.618:519.686

Залкін С. В., Хударковський К. І.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЯХ

Характерною рисою сучасної збройної боротьби у світі є постійне зростання ролі і значущості протиборства в інформаційній сфері, інтенсивний розвиток інформаційної інфраструктури збройних сил провідних країн світу, розширення спектру інформаційних загроз, під якими розуміються фактори або їх сукупність, що створюють небезпеку функціонуванню суспільства та збройних сил в інформаційному просторі.

На сьогоднішній день інформаційно-психологічні операції та інформаційно-психологічні впливи (ІПВ) є невід'ємною складовою збройної боротьби, а роль передових технологій в ході їх проведення важко переоцінити.

Методи, способи і прийоми використання радіо, телебачення та Інтернету для проведення інформаційно-психологічних операцій і здійснення інформаційно-психологічних впливів достатньо добре вивчені і широко застосовуються [1-4]. Інтернет і соціальні мережі, останнім часом, перетворилися в широко застосувавані інструменти маніпуляції думкою – сучасні технології дозволяють не просто поширювати дезінформацію, але й спрямовувати інформаційно-психологічний вплив на конкретні цільові аудиторії. Разом з тим, можливості таких технологій як Big Data та штучний інтелект до цього часу широкого використання в інформаційно-психологічних операціях ще не отримали.

Штучний інтелект – технічна система, як правило, комп'ютерна, що має певні ознаки інтелекту, тобто здатна: розпізнавати та розуміти; знаходити спосіб досягнення результату та приймати рішення; вчитися.

Взагалі, штучний інтелект – розділ комп'ютерної лінгвістики та інформатики, що опікується формалізацією проблем та завдань, які подібні до дій, які виконує людина. Експерти НАТО у своїй діяльності оперують спорідненими тлумаченнями штучного інтелекту[5]:

- "спроможність, що надається алгоритмами оптимального або неоптимального вибору з широкого простору можливостей, для досягнення цілей шляхом застосування стратегій, які можуть спиратися на навчання або адаптацію до навколишнього середовища";
- "системи, які створені людиною і діють у фізичному або цифровому світі, враховують складну мету і обирають найкращі дії (відповідно до заздалегідь визначених параметрів), які необхідно виконати для досягнення поставленої мети на основі сприйняття свого середовища, інтерпретації зібраних структурованих або неструктурованих даних та обґрунтування знань, отриманих з цих даних".

Використання технології штучного інтелекту є доцільним для розв'язання задач, для яких не існує відомих способів розв'язання або вони не коректні, потребують людського розуміння, оперування зі знаннями та приймання рішень в умовах невизначеності.

Застосування технологій штучного інтелекту для здійснення ІПВ суттєво збільшує можливості впливу на цільову аудиторію (об'єкт впливу), коригування ходу впливу та визначення його ефективності. Тож, технології штучного інтелекту поступово стають надзвичайно важливим компонентом стратегій національної безпеки для наддержав.

До основних напрямів використання технологій штучного інтелекту для здійснення ІПВ можуть бути віднесені [6]:

- створення "глибоких фейків" (deep fakes), тобто штучних образів на основі синтезу зображення та голосу людини (або відповідного шумового ряду). Створені таким чином відео можуть бути досить реалістичними, що може спровокувати будь-яку подію та призвести до певних, завчасно спрогнозованих наслідків;

- створення “підроблених людей” (fake people), тобто штучних образів реально неіснуючих людей, що надає необмежені можливості для створення і розповсюдження будь-яких інформаційних повідомлень (меседжів);
- створення точних психологічних портретів людей (об’єктів ІПВ) по профілях у соціальних мережах, що суттєво підвищить ефективність впливу;
- просування (поширення) в соціальних мережах інформаційного контенту певного спрямування із використанням чат-ботів;
- контент-аналіз інформаційного трафіку в Інтернеті (аналіз тональності) (sentiment analysis) на основі широкого спектру інформаційних джерел таких, як блоги, статті, форуми, опитування, що забезпечує виявлення ознак ІПВ, його спрямованості, інтенсивності тощо;
- прогнозування розвитку і наслідків ІПВ на основі аналізу певних подій, фактів, різноманітних факторів, які відображені в інформаційному просторі, що надає значні можливості для управління впливом і забезпечення його максимальної ефективності.

Тож, поєднання систем, побудованих на основі технології штучного інтелекту, технології Big Data та методів і прийомів ІПВ у найближчому майбутньому може призвести до генерування псевдореальності, тобто створення певної “матриці”, що виведе інформаційно-психологічні операції на якісно новий рівень.

Список використаних джерел

1. Пєвцов Г. В. Інформаційно-психологічна боротьба у воєнній сфері : монографія / Г. В. Пєвцов, А. М. Гордієнко, С. В. Залкін, С. О. Сідченко, А. О. Феклістов, К. І. Хударковський. – Х. : Вид. Рожко С. Г., 2017. – 276 с.

2. Пєвцов Г. В. Методичний підхід до формування сценарію проведення інформаційно-психологічного впливу на осіб, що приймають рішення / Г. В. Пєвцов, С. В. Залкін, С. О. Сідченко, К. І. Хударковський, // Системи обробки інформації. – 2019. – Вип. 1(156). – С. 74-81.

3. Пєвцов Г. В. Особливості формування сценарію проведення інформаційно-психологічного впливу в ході реалізації стратегічних комунікацій / Г. В. Пєвцов, С. В. Залкін, С. О. Сідченко, К. І. Хударковський // Наука і техніка Повітряних Сил. – 2019. – Вип. 3(36). – С. 40-46.

4. Пєвцов Г. В. Методичний підхід до аналізу інформаційно-психологічної операції противника. / Г. В. Пєвцов, С. В. Залкін, С. О. Сідченко, К. І. Хударковський // Наука і оборона. – К. : Видавничий дім “Стилос”. – 2016. – Вип. 3. – С. 27-31.

5. Slyusar, Vadym (2019). Artificial intelligence as the basis of future control networks. – [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/334573170_Artificial_intelligence_as_the_basis_of_future_control_networks.

6. Пашенцев Е. Н. Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации / Е. Н. Пашенцев // Государственное управление. Электронный вестник. – Вып. № 76. – 2019. – С. 279-300. – [Електронний ресурс]. – Режим доступу: https://cyberleninka.ru/article/n/zlonamerennoe-ispolzovanie-iskusstvennogo-intellekta-novye-ugrozy-dlya-mezhdunarodnoy-informatsionno-psihologicheskoy-bezopasnosti/viewer.

Меленті Є. О., Коломійцев О. В., Бугай Ю. Р., Третяк Д. В.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ СБУ ДЛЯ ЗАХИСТУ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ

Актуальність теми обумовлена стрімкістю розвитку інформаційних процесів у суспільстві та необхідністю суспільного реагування, у тому числі правового, на негативні аспекти їх прояву. У сучасному світі інформація є найціннішим глобальним

ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас зростає уразливість сучасного інформаційного суспільства від недостовірної (а іноді і шкідливої) інформації, її несвоєчасне надходження, промислового шпигунства, комп'ютерної злочинності тощо. З цією ж проблемою зіткнулися й правоохоронні органи у своїй діяльності щодо запобіганню та припиненню адміністративних правопорушень, виявленню та розкриттю злочинів, пошуку, затриманню злочинців. Удосконалення інформаційного забезпечення роботи правоохоронців дедалі стає одним з головних напрямків підвищення ефективності правоохоронної діяльності.

Інформаційні технології — це не просто сукупність методів і засобів, що використовуються для збору, зберігання, обробки і поширення інформації, а й на сьогодні технології постійно використовуються для життя і потреб сучасного суспільства.

Практика останніх десятиліть говорить про дедалі більш відчутне значення інформаційних операцій, інформаційних війн, що передують силовим діям у відносинах між державами або ж нерідко, дедалі більшою мірою, замінюють їх. На інформаційному рівні йдеться про чітко спрямовані операції, що мають за мету вплив на свідомість населення.

Я вважаю, що однією з головних причин низької ефективності боротьби зі злочинністю є незадовільний стан взаємодії підрозділів правоохоронних органів України в оперативно-розшуковій роботі, відсутність ефективної інтегрованої системи обміну інформацією, своєчасного її отримання працівниками всіх рівнів.

Навіть нинішній конфлікт України з Росією також є прикладом гібридної війни, тобто війни, яка поєднує традиційні і нетрадиційні методи реалізації військових дій. Зокрема, про це зазначається у Стратегії національної безпеки України, у Концепції розвитку сектору безпеки і оборони України, у Доктрині інформаційної безпеки України. Російсько-український конфлікт не тільки порушив регіональну стабільність, а й створив та підсилив глобальні ризики в країні. Агресія РФ проти України спричинила руйнівні наслідки для європейської та глобальної безпеки.

Дійсно, п'ять років війни в Україні наочно показали динаміку змін у процесі гібридної війни – як у методах нападу, так і у способах захисту та опору агресії. Враховуючи всі форми і методи, які використовуються в даному конфлікті, жертви і руйнування агресор завдає не лише прямим військовим вторгненням, а він все активніше застосовує засоби інформаційно-психологічного, економічного, політичного впливу.

Саме на сьогоднішій час у ході ведення Російською Федерацією «гібридної війни» проти України інформаційно-телекомунікаційні системи державних органів та органів місцевого самоврядування все частіше стають об'єктами кібератак, адже тепер здобути інформацію про будь-який об'єкт критичної інфрастуктури (ОКІ) чи навіть про посадових осіб державної влади стає все легше і легше, а людей, які можуть цю інформацію роздобути також стає все більше.

Звичайно, інформація відіграє досить важливу роль в діяльності СБУ для вирішення її конкретних завдань, повязаних з контррозвідувальним захистом державного суверенітету, конституційного ладу, територіальної цілісності, протидії розвідувальній, розвідувально-підривній та іншій протиправній діяльності спеціальних служб іноземних держав. Кібербезпека є одним з провідних завдань СБУ, вона є частиною інформаційної безпеки, діяльність її залежить від створення безпечних комп'ютерних систем.

Для вирішення всіх завдань і досягнення очікуваного результату СБУ повинна взаємодіяти з іншими складовими сектору безпеки і оборони, органами державної влади, установами та організаціями й надавати один одному достовірну інформацію для реалізації вирішення певних питань. Також необхідно встановити партнерський зв'язок зі спецслужбами іноземних держав відповідно до національного законодавства та міжнародних договорів, адже це значно посилить роботу наших спецслужб.

Робота СБУ повинна бути спрямована на вирішення таких проблем як витікання стратегічної інформації, або ж розміщення неправдивої інформації на офіційних електронних ресурсах органів державної влади, що в свою чергу може призвести до виведення з ладу робото здатності ОКІ. Також за допомогою інформації можливе шантажування та погрожування співробітникам стосовно їхніх членів сім'ї, підриву репутації серед співробітників, вербування та кіберпогрози, що може призвести до підриву морально-психологічного стану та паніки у суспільстві, приховане залучення до співробітництва громадян іноземних держав, котрі можуть бути використані для реалізації сценаріїв диверсії.

Слід зазначити, що якість державного нагляду за мережею Інтернет, а також регулювання «діяльності» мережі здійснюється згідно законів України: «Про інформацію», «Про телекомунікації», «Про національну програму інформатизації», «Про основи національної безпеки України».

На теперішній час важливими проблемами, що постають перед правоохоронними органами є: вдосконалення нормативно-правової бази, покращення організаційно-кадрового забезпечення, яке потребує докорінного вдосконалення, створення та розробка дієвої системи інформаційної безпеки органів внутрішніх справ, яка б визначила загальні положення, основні поняття, цілі, принципи й напрями запровадження та підтримку надійної системи інформаційної безпеки правоохоронних органів України.

Уповноважені для контролю й розвитку інформаційного законодавства органи: Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна експертна комісія України з питань захисту суспільної моралі, Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, Управління по боротьбі з кіберзлочинністю МВС України та інші – на сьогодні не встигають із законодавчими ініціативами за темпами розвитку інформаційних технологій.

Отже можна зробити висновок, що проблема вдосконалення інформаційного забезпечення діяльності правоохоронних органів України є багатогранною та потребує комплексного підходу до її вирішення: від нормативно-правових аспектів до матеріально-технічного та кадрового забезпечення.

УДК 621.396.4

Чумак Б. О., Бархударян М. В., Кулагін К. К., Нос І. А.

ШЛЯХИ СТВОРЕННЯ ПЕРСПЕКТИВНОГО ПОЛІГОННОГО ВИМІРЮВАЛЬНО-ОБЧИСЛЮВАЛЬНОГО КОМПЛЕКСУ

Сьогодні не існує єдиного підходу до побудови полігонного вимірювально-обчислювального комплексу (ПВОК), який би забезпечував заданий рівень ефективності проведення полігонних випробувань озброєння та військової техніки (ОВТ) та навчань з бойовою стрільбою. Не визначені основні вимоги до найважливіших показників ефективності функціонування усіх складових структури полігону як організаційно-технічної системи. Даний недолік призводить до в певній мірі довільного вибору структури побудови ПВОК, до зниження ймовірності виконання задач щодо управління військовою зброєю, до невизначеності вибору складу існуючих вимірювальних засобів при вирішуванні задач ПВОК, нарешті, до такої організації процесу навчань та випробувань, який може не забезпечити заданий рівень виконання бойової задачі та безпеки. При цьому суттєвим є відставання рівню методологічного та науково-технічного забезпечення зазначеного процесу, а також експериментально-технічної бази полігону.

Авторами зроблена спроба на основі єдиної методологічної основи сформувати підхід до побудови ефективної структури ПВОК, яка б могла забезпечити заданий рівень ймовірності виконання функціональної задачі при його застосуванні в тих чи інших умовах обставин, для тієї або іншої мети.

При цьому виявлена низка питань, що стосується розробки спеціальних технічних вимог до складових частин ПВОК, обґрунтування вимог до характеристик точності траєкторних вимірювань та обсягу і якості одержуваної інформації від засобів ПВОК, вирішення задач подальшого удосконалювання і розвитку як самого ПВОК, так і його засобів, а також ряд інших, які потребують свого подальшого вирішення.

Розглянуті питання щодо методології застосування ПВОК (як системи) та його засобів на усіх етапах навчань, раціональної взаємодії ПВОК і засобів стріляючих підрозділів, а також висування вимог до тактико-технічних характеристик ПВОК і його засобів для якісного забезпечення усіх завдань навчань військ. Показано, що доцільним є вирішення задачі забезпечення об’єктивного оперативного контролю бойових стрільб щодо питань дистанційної оцінки результатів бомбометань, ракетних та артилерійських стрільб.

Як показав досвід експлуатації полігону суттєвою особливістю обслуговування ОВТ із залученням вимірювальних засобів ПВОК є досить обмежений термін їх спостереження, а також обмежені можливості визначених засобів. Оскільки експлуатація зазначених систем потребує досить великих економічних витрат, то на стадії розробки і використання таких систем необхідно передбачити всі можливі засоби максимального підвищення ефективності їх цільового застосовування. Враховуючи високу динаміку руху ракет (при проведенні навчань або випробувань) і технічні можливості системи щодо спостереження на заданий час певного визначеного району, інтервал часу для прийняття рішення людиною на проведення певних операцій (наприклад, примусового знищення) суттєво обмежується. Тому, планування використання ОВТ за цільовим призначенням і прийняття визначеного рішення повинні базуватися на достовірно визначених параметрах його руху, в реальному масштабі часу і заданими показниками якості.

З урахуванням проведених досліджень доведено, що задачу підвищення ефективності використання ПВОК за цільовим призначенням слід вирішувати шляхом оптимізації процесу контролю і управління рухом літальних об'єктів на основі мінімізації функціоналу якості, який враховує найбільш вагомі фізичні явища, що впливають на якість процесу контролю і управління.

Визначені можливості щодо підвищення ефективності контролю руху літальних об’єктів полягають у комплексному використанні засобів ПВОК та стріляючих підрозділів, а також сучасних методів як первинної, так і вторинної обробки вимірювальної інформації. Підвищення якості обробки вимірювальної інформації в реальному часі дозволить не припускаючи великих матеріальних витрат, що в даний час для Збройних Сил України є надзвичайно важливим, забезпечити необхідну ефективність вирішення задачі визначення руху шляхом коректного вибору статистичних методів обробки вимірів, що дозволяють враховувати наявність апріорної інформації про оцінювані параметри, умови вимірів, властивості вимірювальної інформації і її статистичні характеристики.

При цьому існує необхідність наявності апаратури статистичної атестації радіоелектронних систем, що працюють в реальному масштабі часу. Цей факт потребує розробки нового покоління систем оптимальної обробки траєкторної інформації, які базуються на застосуванні парку електронно-обчислювальних машин.

Розроблені авторами пропозиції та підходи до побудови комплексів та систем на основі системно-концептуальних напрямів і елементів методології формування оперативно-тактичних і тактико-технічних вимог, що пред’являються до перспективних зразків ОВТ, дозволяють:

- провести подальші роботи щодо формування вимог, що пред'являються до функціональних можливостей і ефективності застосування ПВОК для виконання поставлених задач;
- перейти до формування:

а) технічного вигляду перспективного ПВОК, спроможного надати необхідний обсяг вірогідної інформації для забезпечення заданої ефективності випробувань номенклатури зразків ОВТ Збройних Сил України, а також навчань військ із застосуванням засобів ураження;

б) тактико-технічних вимог до ПВОК, основою яких є оперативно-тактичні вимоги, доповнені іншими вимогами, що витікають з науково-технічної і виробничо-економічної концепцій ПВОК;

- провести подальше оцінювання і підтвердження можливості практичної реалізації вимог, висунутих на етапах концептуальних досліджень і досліджень первісного обрису ПВОК.

При застосуванні розробок та висновків можливі як створення нової науково-технічної та методологічної продукції і експериментально-технічної бази, так і модернізація існуючої. При цьому будуть потрібні окремі розробки щодо виявлення можливості забезпечення визначених вимог існуючим складом озброєння та військової техніки на основі впровадження як натурних випробувань, так і перспективних методів моделювання.

Зазначені методичні розробки та наукові дослідження і висновки будуть досить важливими як під час експлуатації, так і при проектуванні перспективних ПВОК і зразків озброєння в умовах, коли необхідна модернізація існуючого ПВОК та його підсистем з метою досягнення необхідних показників ефективності функціонування.

УДК 004.85

Сальніков О. М.

ПРОБЛЕМИ ВИВЧЕННЯ ІНФОРМАТИКИ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ III-IV РІВНІВ АКРЕДИТАЦІЇ

На сучасному етапі в освітній галузі склалася склалась ситуація, коли у заклад вищої освіти поступають випускники шкіл с достатньо високим рівнем оволодіння інформаційними технологіями. В той же час навчальні програми з інформатики у закладах вищої освіти III-IV рівня акредитації, де ця дисципліна не є профілюючою, в значній мірі повторюють шкільні навчальні програми. Порівняльний аналіз навчальних програм з інформатики для загальноосвітніх шкіл, закладів вищої освіти I-II рівня акредитації та закладів вищої освіти III-IV рівнів акредитації свідчить про те, що вимоги до знань та вмінь випускників майже однакові. З цієї точки зору було б доцільним розподілити навчальний матеріал з інформатики між навчальними закладами різних рівнів з метою впровадження принципу оволодіння навчальним матеріалом від простого до складного, забезпечуючи постійне підвищення рівня комп'ютерної та інформаційної грамотності відповідно до підвищення рівня освіти.

Для цього існує два шляхи. Перший полягає у поглибленому вивченні навчального матеріалу, який вже вивчався на попередньому рівні. Тобто об'єкти навчання поглиблюють отримані раніше знання та навички. Але тут виникає питання, чи потрібно таке глибоке знання досить вузького кола інформаційних технологій для фахівця іншої галузі.

Другий підхід полягає у поширенні складу вивчених інформаційних технологій, тобто на кожному наступному рівні об'єкти навчання отримують знання та навички, яких у них не було на попередньому рівні навчання.

Аналіз динаміки розвитку апаратного та програмного забезпечення показує, що протягом року один-два рази змінюється модель мікропроцесорів з нарощуванням їхніх потужностей і, відповідно до цього, змінюється і програмне забезпечення. Для системи освіти суттєвим є те, що темпи розвитку прикладної інформатики настільки високі, що навіть найсучасніше на момент навчання програмне забезпечення до моменту випуску об’єктів навчання із навчального закладу взагалі перестає використовуватись.

Таким чином, основною метою вивчення інформатики є надання об’єктам навчання знань та навичок, які дозволяли їм успішно самостійно оволодівати новими для них інформаційними технологіями. Досягнення цієї мети забезпечується використанням нових підходів до викладання інформаційних технологій, нових методів та методик навчання, націлених саме на такий шлях розвитку інформатики, як навчальної дисципліни.

УДК 004.93

Ємельянов Ю. О., Дядюн С. В.

РОЗРОБКА ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ ДЛЯ РОЗПІЗНАВАННЯ ТА КЛАСИФІКАЦІЇ ДОРОЖНІХ ЗНАКІВ

З розвитком технологій підвищуються стандарти безпеки, особливо це стосується автомобільної безпеки. В умовах сучасного щільного трафіку та надлишку дорожніх знаків, водієві стає все важче орієнтуватись на дорозі та зберігати необхідну концентрацію для безпечного керування своїм транспортним засобом, можливостей людської пам’яті недостатньо для того, щоб у екстреній ситуації, яка виникла на дорозі, пам’ятати усі знаки з правил дорожнього руху.

Для цілей розпізнавання та подальшої класифікації дорожніх знаків було вирішено спочатку порівняти між собою найпопулярніші алгоритми штучного інтелекту для класифікації зображень, відеокадрів. Вибір був зроблений в користь використання згорткової нейронної мережі (Convolutional Neural Network). Найкращі результати в області розпізнавання осіб показала CNN (Згорткова нейронна мережа), яка є логічним розвитком ідей таких архітектур нейронних мереж, як когнітрону і неокогнітрона.

Успіх обумовлений можливістю обліку двовимірної топології зображення, на відміну від багатошарового персептрона. Згорткові нейронні мережі забезпечують часткову стійкість до змін масштабу, зсувів, поворотів, змін ракурсу і інших спотворень. Згорткові нейронні мережі об'єднують три архітектурні ідеї для забезпечення інваріантності до зміни масштабу, повороту зрушення і просторових спотворень:

- локальні рецепторні поля (забезпечують локальну двовимірну зв'язність нейронів);
- загальні вагові коефіцієнти синапсів (забезпечують детектування деяких рис в будь-якому місці зображення і зменшують загальне число вагових коефіцієнтів);
- ієрархічна організація з просторовими підвибірками.

На даний момент згорткова нейронна мережа та її модифікації вважаються кращими по точності і швидкості алгоритмами знаходження об'єктів.

Згорткова нейронна мережа для даного програмного модуля має таку архітектуру:

- вхідний шар. Вхідні дані кожного конкретного значення пікселя нормалізуються в діапазоні від 0 до 1;
- згорточний шар. Згорточний шар являє собою набір карт (інша назва – карти ознак, в побуті це звичайні матриці). Розмір у всіх карт згорточного шару – однаковий;
- підвиборочний шар також, як і згортковий, має карти, але їх кількість співпадає з попереднім (згортковим) шаром. Мета шару – зменшення розмірності карт попереднього шару. Якщо на попередній операції згортки вже були виявлені деякі ознаки, то для

подальшої обробки настільки докладне зображення вже не потрібно, і воно ущільнюється до менш докладного;

- повнозв'язний шар. Останній з типів шарів це шар звичайного багатошарового персептрона. Мета шару – класифікація, моделює складну нелінійну функцію, оптимізуючи яку, поліпшується якість розпізнавання;
- вихідний шар. Вихідний шар пов'язаний з усіма нейронами попереднього шару. Кількість нейронів відповідає кількості розпізнаваних класів дорожніх знаків.

З метою розроблення програмного модуля для поліпшення керування був проведений детальний аналіз предметної області за допомогою методології IDEF0 та діаграми потоків даних DFD [1].

Розроблено математичну постановку задачі, проведено аналіз різних методів її вирішення, проведено огляд бази, яка використовувалась для навчання моделі класифікації, спроектована діаграма класів та діаграма станів.

Розроблена специфікація вимог до програмного модулю, побудована діаграма варіантів використання за допомогою мови UML [1].

Сегментація застосовується в багатьох областях, наприклад, у виробництві для індикації дефектів при складанні деталей, в медицині для первинної обробки знімків, також для складання карт місцевості по знімках із супутників. Одною з головних задач обробки і аналіза зображень є сегментація, тобто поділ зображення на області, для яких виконується певний критерій однорідності, наприклад, виділення на зображенні областей приблизно однакової яскравості.

Сегментація зображень проводиться за такими ознаками: форма дорожнього знаку (круг, трикутник и т.д.); колір; текст на дорожніх знаках. Для сегментації зображень розроблено кілька універсальних алгоритмів і методів. Згорткові нейронні мережі підходять найкраще всього для ефективного вирішування цієї задачі в даній предметній області.

Розглянуті основні алгоритми вирішення задачі класифікації дорожніх знаків, зроблено детальний аналіз кожного алгоритмічного рішення та їх порівняння між собою, аналізуються переваги та недоліки розглянутих математичних моделей.

На відміну від ручного способу сегментування при використанні згорткової нейронної мережі процес сегментації проходить повністю автоматизовано без безпосередньої участі користувача. В цілому даний метод показав високу працездатність, продуктивність та точність, за допомогою нього можна вирішити широкий спектр завдань пошуку об'єктів, сегментації і розпізнавання, детектування об'єктів на зображеннях, а не тільки класифікації.

Даний програмний модуль розроблявся за допомогою високорівневої мови програмування Python та допоміжних бібліотек та фреймворків [2].

При розпізнаванні образів дана архітектура штучних нейронних мереж показує кращу точність, ніж метод опорних векторів (Support Vector Machine), котрий має більш просту архітектуру [2].

Даний програмний модуль в першу чергу має облегшити складність в прийнятті рішень водієві при маневрі на дорозі, для уникнення порушень правил дорожнього руху або уникнення ДТП, яка може статися внасідок некоректного руху авто при забороненому знаку.

Список використаних джерел

1. Буч Г. Объектно-ориентированный анализ и проектирование с примерами приложений / Г. Буч, Р. Максимчук, М. Энгл и др.; пер. с англ. – М. : ИД "Вильямс", 2008. – 720 с.

2. Франсуа Шолле. Глубокое обучение на Python. – СПб. : Питер, 2018. – 400 с.: ил. – (Серия «Библиотека программиста»).

УДК 681.5.015

Дядюн С. В., Саввін Д. В.

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ РЕЖИМІВ ФУНКЦІОНУВАННЯ СИСТЕМ ВОДОПОСТАЧАННЯ

При експлуатації реальних систем водопостачання (СВ) виникає задача аналізу усталеного потокорозподілу (УПР) в СВ. Для її вирішення потрібно мати математичну модель водопровідної мережі спільно з активними джерелами.

При побудові математичної моделі будемо дотримуватись таких припущень [1]:

- система водопостачання структурно може бути представлена у вигляді великого числа взаємопов'язаних підсистем трьох типів: навантажень, або споживачів, активних елементів, ліній зв'язку. Причому в якості споживача в системі розглядається реальна або еквівалентна ділянка, яка називається фіктивною і спрямована від будь-якого вузла графа СВ до деякої точки з нульовим тиском. До активних елементів, або джерел, слід віднести насосні станції (НС). Лінії зв'язку (пасивні елементи) представляють собою ділянки трубопроводу. Оскільки зі збільшенням витрати за таким ділянці втрата напору зростає, а при рівних, але протилежних по напрямку витратах вона однакова по абсолютній величині, але протилежна за знаком, залежність втрати напору від витрати є монотонно зростаючою і непарною функцією. До пасивних елементів слід також віднести різні регульовані і нерегульовані засувки (запірну арматуру);
- кожна підсистема характеризується двома змінними величинами: послідовною (витратою) і паралельною (втратою напору), рядом параметрів, а також обраним напрямом. Втрата напору являє собою різницю тисків, під якою знаходиться вода на початку і кінці і-го ділянки трубопроводу;
- взаємозв'язок між основними елементами СВ, тобто її структура може бути представлена у вигляді лінійного графа;
- загальний потік води, що подається в систему, дорівнює сумарному потоку, потребляемому з неї;
- в системі виконуються два закони Кірхгофа: 1) алгебраїчна сума витрат в будь-якому вузлі графа системи дорівнює нулю; 2) сумарна втрата напору по будь-якому замкнутому циклу цього графа також дорівнює нулю.

Нехай $G(V,E)$ – граф СВ, що моделює її структуру і відображає взаємозв'язки між окремими елементами. Тут V, E – безліч всіх вузлів і дуг СВ. З'єднаємо всі входи і виходи графа $G(V,E)$, через які вода надходить в мережу і відбирається з неї, з нульовою фіктивної точкою. Позначимо L – безліч НС, тоді елементами цієї множини будуть фіктивні дуги, що з'єднують нульову точку зі входами всіх НС; M – безліч магістральних ділянок СВ, що є реальними дугами графа; N – безліч вузлів СВ з приєднаними до них споживачами, тобто фіктивних дуг моделі СВ. Введемо також безліч $K = \bigcup_{j \in L} L_j$, що характеризує загальну кількість дуг з насосними агрегатами (НА) на всіх НС СВ. Виберемо дерево графа СВ таким чином [1], щоб до нього увійшли магістральні ділянки мережі і ділянки з насосами (що належать різним НС СВ), а також одна фіктивна гілка, що з'єднує нульову точку зі входом деякої з НС. Дамо їй номер 1. При цьому всі фіктивні ділянки, інцідентні вузлам СВ, які є входами НС (крім першого), а також ділянки зі споживачами будуть віднесені до хорд, магістральні ж ділянки і ділянки з насосами частково стануть хордами, а частково – гілками дерева. Вважаємо, що індекс 1, присвоєний безлічам L, M, N, K, E, характеризує приналежність їх елементів до гілок дерева, а індекс 2 – до хорд. В результаті такого вибору безліч усіх дуг графа СВ предста-

вимо як $E = E_1 \cup E_2$, де $E_1 = M_1 \cup K_1 \cup L_1$, $E_2 = M_2 \cup K_2 \cup L_2 \cup N_2$, $L_1 = \{1\}$, $N_1 = \varnothing$, $N_2 = N$.

Позначимо q_i – витрата води в і-й дільниці мережі, $i \in M$; r_i – гідравлічний опір і-ї ділянки мережі, $i \in M$; $h_i^{(r)}$ – перепад геодезичних відміток початку і кінця і-ї ділянки; h_i – втрата тиску на і-й дільниці мережі, $i \in M$.

З урахуванням зробленого вибору дерева графа СВ, а також того факту, що сума перепадів геодезичних висот по будь-якому замкнутому циклу, який містить магістральні ділянки мережі, дорівнює нулю, тобто

$$h_i^{(r)} + \sum_{r \in M_1} b_{1ri} h_r^{(r)} = 0, \quad i \in M_2, \tag{1}$$

математична модель усталеного потокорозподілу в СВ матиме вигляд [2]

$$f_r = \operatorname{sign} q_r \, r_r |q_r|^2 + \sum_{i \in M_1} b_{1ri} \operatorname{sign} q_i \, r_i |q_i|^2 = 0, \quad r \in M_2 ; \tag{2}$$

$$f_r = H_{BX1} + \Psi_{0k} + \Psi_{1k} |q_k| + \Psi'_{2k} q_k |q_k| - h_r - \sum_{i \in M_1} b_{1ri} \left(\operatorname{sign} q_i \, r_i |q_i|^2 + h_i^{(r)} \right) = 0, \tag{3}$$

$$r \in N, \quad k \in K_1;$$

$$f_r = H_{BX1} - H_{BXr} + \sum_{k \in K_1} \left[\operatorname{sign} q_k \left(\Psi_{0k} + \Psi_{1k} |q_k| + \Psi'_{2k} q_k |q_k| \right) \right] - \\ - \sum_{i \in M_1} b_{1ri} \left(\operatorname{sign} q_i \, r_i |q_i|^2 + h_i^{(r)} \right) = 0, \quad r \in L_2^{(a)}; \tag{4}$$

$$q_i = \sum_{r \in M_2} b_{1ri} q_r + \sum_{k \in K_2} x_k q_k + Q_i^+, \quad i \in M_1 \cup L_1 \cup K_1, \tag{5}$$

$$x_i = \begin{cases} 1, & \text{якщо і-й насос включено,} \\ 0, & \text{якщо і-й насос вимкнено,} \end{cases} \quad i \in K_1 \cup K_1;$$

$Q_i^+ = \sum_{k \in N \cup L_2} b_{1ki} q_k = \text{const}$; H_{BX1}, H_{BXk} – тиск на вході 1-ї та к-ї НС; b_{1ri} – елемент цикломатичної матриці B_1. Величина, позначена індексом «+» , є заданою.

Проаналізуємо умови можливості розв'язання системи рівнянь математичної моделі системи водопостачання. Система рівнянь математичної моделі СВ може бути вирішена, якщо задані граничні умови роботи СВ у вигляді комбінації значень змінних витрат і тисків на її входах і виходах.

Дана математична модель використовується при управлінні системами водопостачання для аналізу якості функціонування СВ при реалізації керуючих впливів на НС, а також для контролю правильності прийнятих рішень з управління процесами подачі та розподілу води.

Список використаних джерел

1. Евдокимов А. Г., Тевяшев А. Д. Оперативное управление потокораспределением в инженерных сетях. – Харьков, 1980. – 144с.

2. Дядюн С. В. Математическое моделирование установившегося потокораспределения в системах водоснабжения. // Радиоэлектроника и информатика. – Харьков, ХНУРЭ, 2000, №4, С.54-56.

Дудар З. В., Кобзєв В. Г.

ПЕРЕВАГИ ВИКОРИСТАННЯ СТЕКУ ELK ДЛЯ ОБРОБКИ ВЕЛИКИХ ДАНИХ

Однією з найпоширеніших є парадігма розподіленої обробки даних MapReduce, яка розрахована на участь кластерів з багатьох комп'ютерів у зберіганні, кількох етапах обробки та відображенні великих обсягів даних. Величезні обсяги, складність, мінливість, слабка структурованість та різноманітність є характерними рисами даних, що підлягають кількісному та якісному аналізу і сприйнятному відображенню, у різних сферах людської діяльності протягом останніх десятиліть. Збір, зберігання та аналіз даних з вказаними особливостями являють собою доволі складну проблему, впоратися з якою можна тільки завдяки технологіям Big Data.

Інший підхід базується на використанні ELK-стеку, який має три складові (Elasticsearch, Logstash та Kibana), створений у 2010 році як потужна система гнучкого пошуку, зберігання та візуалізації даних. Протягом останніх п'яти років вона стала дуже популярною серед аналітиків Великих даних завдяки своїм можливостям, простоті освоєння і застосування. Ця система здатна збирати та аналізувати десятки мільйонів даних за день, що саме й розуміють під поняттям Big Data.

Підсистема Logstash має можливості передати дані, витягнути їх з бази даних, з файлу, або з встановленого клієнту, що збирає логи, а також може перетворити їх на потрібний формат чи структуру та завантажити у будь-яке сховище даних. Крім того, вона має змогу у будь-який час передати дані до підсистеми Elasticsearch.

За виконуваними функціями Logstash – це доволі простий інструмент, який передає дані з одного чи багатьох входів та виводить їх на один, чи декілька виходів. Входами можуть бути будь-які джерела даних, такі як файли журналів або логи. Після того як вхідні дані будуть зчитані, logstash аналізує їх за допомогою кодеків, таких як JSON.

Під час переміщення даних з джерела в сховище, фільтри Logstash аналізують кожну подію, ідентифікують назви полів для побудови структури та перетворюють їх у загальний формат для прискорення та полегшення аналізу. Підсистема Logstash динамічно готує та трансформує дані незалежно від формату або складності: розшифровує географічні координати, створює структуру з неструктурованих даних, анонімізує дані. Простота обробки даних не залежить від джерела, формату чи схеми даних. Крім того, блок Logstash відстежує введені дані, які він обробляє. Таким чином, можна перезапустити його без шкоди дублювання даних.

Хоча Logstash створений в Ruby, працює він дуже швидко. Пакетна версія запускається на JRuby, і вона використовує можливості JVM в потоці, даючи десятки потоків для паралельної обробки даних.

Блок Logstash може зберігати дані у блоці ElsaticSearch, який також запущений на машині, де працює Logstash. Підсиситема ElsaticSearch виконує роль сховища даних. Але це не база даних, яка буде сприймати все, що користувач забажає помістити до неї. Блок ElsaticSearch масштабує дані, коли це потрібно.

Стан Elasticsearch відображається у один рядок і містить інформацію про статус, очікування інформації, зайнятий обсяг пам'яті, тощо. За допомогою простої команди можна побачити наступну інформацію: стан індексу, статус, назву, об'єм, кількість рядків, розмір на диску, тощо.

Останнім кроком проведеного аналізу є відображення отриманих результатів, яке виконується підсистемою Kibana. Вона вже пов'язана з ElasticSearch, тому всі індекси вже знаходяться в ній, тож треба лише вибрати той, який у подальшій роботі дозволить виконати необхідний аналіз.

Kibana - єдиний компонент, який не резервується, тому що вихід його з ладу не впливає на процеси збору і обробки інформації. Kibana має добрий інтерфейс для візуалізації величезної кількості даних і дозволяє краще зрозуміти дані через аналіз та візуа-

лізацію, що можна створити за лічені хвилини. Незважаючи на простоту вказаних інструментів, вони дуже потужні. Наявність шаблонів розгортання дозволяє легко вибрати апаратні та архітектурні профілі, які найкраще відповідають потребам користувача.

Підсистема Kibana дозволяє будувати аналіз за такими напрямками, як геолокація, кількість, часові проміжки, тощо. Окрім цього, всі зображення мають гарну графіку. Їх можна об'єднувати у інформаційні панелі, завдяки чому весь необхідний аналіз може бути зібраний на одній сторінці. Окрім яскравої та зрозумілої графіки, Kibana може виводити згруповані та відсортовані дані у таблицях, метриках або рядках.

Стек ELK є системою, що відстежує інформацію у реальному часі. Тому після запуску усіх компонент, якщо джерело входу інформації буде поповнюватися новими даними, то усі компоненти будуть відстежувати їх, додавати у сховище та відображати на візуалізаціях без перезапуску їх самих. Це дуже зручно, якщо дані надходять постійно.

ELK-стек добре захищений та швидко працює, що дуже важливо для систем обробки Великих даних. Швидкість роботи та візуалізації за допомогою ELK-стеку дійсно вражає. Аби завантажити дані про приблизно 30 мільйонів об'єктів та побудувати зрозумілі графіки, знадобилося дві години. ELK-стек дозволяє будувати не тільки кругові або стовпчикові діаграми, але й дає змогу чітко візуалізувати дані з географічними полями на детальній мапі світу.

Дана система надає можливості реалізації унікальних розрахунків та послідовності переходів, які необхідні для створення комерційних звітів.

Ще однією безсумнівною перевагою стеку ELK є можливість автоматичного опрацювання нових даних без додаткового настроювання.

Таким чином, ELK-стек є доступним, високоякісним, надійним і простим у обслуговуванні інструментом, який надає можливість за лічені хвилини доставити, впорядкувати та візуалізувати Великі дані, що стосуються, наприклад, сфери туристичного бізнесу чи продажів автомобілів.

Слупська С. Ю., Кобзєв В. Г.

ТЕХНІКИ ПРІОРИТИЗАЦІЇ ЗАДАЧ ПРИ ПЛАНУВАННІ ПРОЕКТУ

Пріоритизація задач – один з найважливіших процесів при плануванні проектів.

Процес визначення пріоритетності завдань – це процес будування задач в порядку їх пріоритету, тобто визначається в якій послідовності буде проходити реалізація задач, що буде випущено в першій версії продукту, що може бути включено в наступні поставки, а що може бути залишено на той випадок, якщо залишиться час.

Процес визначення пріоритетності завдань базується на різних умовах, виходячи з різних цінностей. Для цього процесу існує безліч технік/методів, кожна з яких бере до уваги той чи інший аспект/критерій значущості завдання [1].

У Agile-підході найефективнішим підходом буде застосування і комбінування різних методів пріоритизації.

Найпопулярніші методи/підходи: MoSCoW, WSJF, Story Mapping, RICE, Kano Model.

Метод MoSCoW [2] сьогодні знають у всьому світі і застосовують достатньо широко в різних областях управління. Відповідні літери акроніму MSCW – це ступені пріоритетності:

M (must) – завдання і вимоги, які мають найвищий пріоритет і повинні бути першочергово застосовні до продукту в першу чергу. Без них реліз не буде виконано;

S (should) – важливі вимоги, але не з найвищою пріоритетністю. Зазвичай вони не мають вирішального значення, але все одно є обов'язковими до виконання;

C (could) – вимоги і завдання, бажані для релізу;

W (would) – найменш критичні вимоги, їх можна проігнорувати або перенести до наступних релізів.

Метод WSJF (Weighted Shortest Job First – найбільш коротка задача виконується першою) ґрунтується на обчисленні наступного показника [3]:

$$WSJF = \frac{CD}{JS} = \frac{UBV + TC + RO}{JS},$$

де: CD (Cost of delay) – вартість затримки, JS (Job size) – розмір роботи.

Вартість затримки CD має наступні складові: UBV (User Business Value – Користувальницьке значення) – Яке відносне значення для замовника чи бізнесу? Чи віддається перевага саме нашим користувачам? Який дохід впливає на наш бізнес? Чи можливе покарання чи інший негативний вплив, якщо ми зволікаємо?

TC (Time criticality – Часова критичність) – Як вартість користувача/бізнесу занепадає з часом? Чи є фіксований термін? Існує можливість зачекати або необхідно переходити до іншого рішення? Чи впливають на це впливові віхи на критичному шляху? Який сучасний вплив на задоволення клієнтів?

RO (Risk reduction-opportunity enablement value – Значення можливостей зменшення ризику) – Що ще це робить для нашого бізнесу? Чи знижується ризик цієї чи майбутньої доставки? Чи є цінність інформації, яку ми отримаємо? Чи дасть ця функція нові можливості для бізнесу?

Після усіх обчислень задачі з найбільшими показниками виконуються першими.

Метод Story Mapping [2] став відомий на початку століття зі статті Джеффа Паттона. Сенс методу в тому, що списку задач недостатньо для визначення пріоритетів в роботі. Паттон вважає, що необхідна більш розгорнута структура і пропонує наступну конструкцію:

Горизонтальна вісь представляє послідовність використання. Завдання на ній розміщуються в послідовності, в якій вони виконуються користувачем.

Вертикальна вісь означає критичність. По вертикалі завдання розташовуються зверху вниз у відповідності до їх важливості. Однаково важливі завдання можна визначати на одній висоті.

Сильні сторони методології Story Mapping: відносно просте візуальне уявлення, яке дозволяє команді, клієнтам, замовнику або іншим зацікавленим сторонам ділитися загальним розумінням того, що відбувається. Метод чітко визначає, як поступово випускати ітерації продукту.

Метод RICE [4] був розроблений в Intercom та ґрунтується на наступних факторах:

- Reach (охоплення) - скільком користувачам ми покращимо життя?
- Impact (ефект) - наскільки ми покращимо життя нашим користувачам?
- Confidence (впевненість) - наскільки ми впевнені, що взагалі можемо щось покращити?
- Effort (зусилля) - скільки часу нам знадобиться, щоб реалізувати задумане?

Пріоритетність списку завдань визначається за співвідношенням цих 4 факторів.

Метод Kano Model [2] розробив японський вчений Норіакі Кано. Він ґрунтується на емоційному сприйнятті користувачем тієї або іншої функціональності. Кано виділяє наступні типи реакції користувача:

- Must Be – мінімальні вимоги, якщо їх немає - користувач не задоволений.
- Indifferent – функціонал, який викликає неоднозначну реакцію. Користувачам все одно, чи він існує.
- Satisfiers (Performance) – функціонал, який викликає радість, якщо він виконаний добре, або розчарування - якщо якість низька.
- Exciters (Attractive) – функціонал, що підвищує задоволеність користувача, якщо він є. Якщо його немає – невдоволення не виникає.

Зазвичай на практиці спочатку фокусуються на реакціях Must be, потім на Satisfiers і на останок на Exciters.

Наводяться приклади практичного застосування вказаних методів визначення пріоритетності задач при плануванні сучасних ІТ-проектів. Також ілюструється можливість комбінації/чередування декількох методів на різних фазах/ітераціях проекту.

Список використаних джерел

1. https://doitsmartly.ru/all-articles/management/99-agile/116-backlog-prioritization. html
2. https://habr.com/ru/company/hygger/blog/351238/
3. https://www.scaledagileframework.com/wsjf/
4. https://dou.ua/lenta/articles/prioritization-approach/

ЗМІСТ

АБЕТКОВИЙ ПОКАЖЧИК АВТОРІВ ПУБЛІКАЦІЙ

Харківський національний університет імені В. Н. Каразіна

Берднік П. Г.	- кандидат технічних наук, доцент кафедри	***57***
Дядюн С. В.	- кандидат технічних наук, доцент, доцент кафедри	***193, 195***
Рассомахін С. Г.	- доктор технічних наук, професор, завідувач кафедри	***173***
Сербин В. В.	- старший викладач кафедри	***173***

Харківський національний університет міського господарства імені О. М. Бекетова

Маслий Л. А.	- завідувачка лабораторії кафедри	***62***
Метешкин К. А.	- доктор технічних наук, професор, професор кафедри	***62***

Харківський національний університет Повітряних Сил імені Івана Кожедуба

Бархударян М. В.	- кандидат технічних наук, с.н.с., доцент кафедри	***190***
Бекіров А. Е.	- кандидат технічних наук, старший викладач кафедри	***30***
Борозинець І. О.	- кандидат технічних наук, старший викладач кафедри	***54***
Ведмідь О. І.	- кандидат технічних наук, доцент, провідний науковий співробітник Наукового центру Повітряних Сил	***186***
Головняк Д. В.	- заступник начальника штабу університету	***54***
Даневський М .Р.	- курсант	***71***
Демідов Б. О.	- доктор технічних наук; професор, провідний науковий співробітник Наукового центру Повітряних Сил	***157***
Дроб Є. М.	- кандидат технічних наук	***55***
Ємцев О. І.	- курсант	***71***
Залкін С. В.	- кандидат військових наук, с.н.с., провідний науковий співробітник Наукового центру Повітряних Сил	***187***
Захарченко В. В.	- викладач кафедри	***73***
Захарченко І. В.	- кандидат технічних наук, викладач кафедри	***53, 56***
Квіткін К. П.	- науковий співробітник Наукового центру Повітряних Сил	***186***
Ковтуненко Н. М.	- курсант	***30***
Кривчун В. І.	- науковий співробітник Наукового центру Повітряних Сил	***186***
Кудряшов В. Є.	- кандидат технічних наук, с.н.с., доцент кафедри	***41***
Кулагін К. К.	кандидат технічних наук, с.н.с., начальник науково-дослідного відділу Наукового центру Повітряних Сил	***190***
Кучеренко Ю. Ф.	- кандидат технічних наук, с.н.с., провідний науковий співробітник Наукового центру Повітряних Сил	***157***
Ларін В. В.	- кандидат технічних наук, доцент кафедри	***51***
Литвинчук Д. В.	- науковий співробітник науково-дослідної лабораторії	***55***
Литовченко Д. М.	- кандидат технічних наук, старший викладач кафедри	***41***
Лютий А. В.	- курсант	***51***
Маркуш В. О.	- курсант	***72***
Матющенко О. Г.	- ад'юнкт науково-організаційного відділу Наукового центру Повітряних Сил	***157***
Нос І. А.	- кандидат технічних наук, старший науковий співробітник Наукового центру Повітряних Сил	***190***
Осієвський С. В.	- кандидат технічних наук, доцент кафедри	***52***
Павленко В. М.		***57***
Павленко М. А.	- доктор технічних наук, доцент, начальник кафедри	***57, 80***
Пархоменко Д. О.	- кандидат технічних наук, старший викладач кафедри	***73, 74***
Петров О. В.	- кандидат технічних наук, старший викладач кафедри	***80***
Руденко В. М.	- викладач кафедри	***57***
Самокіш А. В.	- ад'юнкт	***55***
Симоненко О. В.	- старший викладач кафедри	***72***
Сироватко О. В.	- курсант	***72***
Скопінцєв О. О	- доцент кафедри	***42***
Тимочко О. І.	- доктор технічних наук, професор, професор кафедри	***52, 56***
Турінський О. В.	- кандидат технічних наук, начальник університету	***52***
Хмелевська О. О.	- кандидат технічних наук, с.н.с., провідний науковий співробітник Наукового центру Повітряних Сил	***80***
Хмелевський С. І.	- кандидат технічних наук, с.н.с., заступник начальника кафедри	***56, 80***
Хударковський К. І.	- кандидат технічних наук, с.н.с., доцент, науковий співробітник Наукового центру Повітряних Сил	***187***
Худов Г. В.	- доктор технічних наук, професор, начальник кафедри	***54***
Чумак Б. О.	- кандидат технічних наук, доцент, старший науковий співробі-	***186, 190***

	тник Наукового центру Повітряних Сил	
Шило С. Г.	- кандидат технічних наук, доцент, викладач кафедри	***54***
Herasimov S.	- доктор технічних наук, с.н.с., заступник начальника кафедри	***39***
Roshchupkin E.	- кандидат технічних наук, с.н.с., старший викладач кафедри	***39***

Харківський національний університет радіоелектроніки

Безкоровайний В. В.	- доктор технічних наук, професор, професор кафедри	***134, 159***
Васильцова Н. В.	- кандидат технічних наук, с.н.с., доцент, професор кафедри	***174***
Дацок О. М.	- кандидат технічних наук, доцент, доцент кафедри	***183***
Дудар З. В.	- кандидат технічних наук, доцент, завідувач кафедри	***197***
Ерошенко О. А (Єрошенко О. А).	- аспірантка	***178, 179, 183***
Зибіна К. В.	- асистент кафедри	***172***
Іванюк О. А.	- студентка	***159***
Кобзєв В .Г.	- кандидат технічних наук, с.н.с., доцент кафедри	***23, 197, 198***
Козлов Ю. В.	- кандидат технічних наук, доцент, доцент кафедри	***23***
Куценко Є. Є.	- магістрант	***24***
Мощенко І. О.	- кандидат технічних, старший викладач кафедри	***23***
Останіна В. Д.	- студентка	***158***
Пастушенко М. С.	- кандидат технічних наук, професор, професор кафедри	***24***
Перетятко М. В.	- студентка	***136***
Прасол И. В. (Прасол І. В.)	- доктор технічних наук, доцент, професор кафедри	***178, 183***
Слупська С. Ю.	- магістрантка	***198***
Сотник С. В.	- кандидат технічних наук, доцент, доцент кафедри	***134***
Тарасов Р. О.	- студент	***172***
Широкопетлєва М. С.	- старший викладач кафедри	***136***

Наукове видання

Міжнародна науково-практична конференція

“ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ ТА ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ”

Збірник тез доповідей

Відповідальний за випуск *О. Ю. Іохов*

В авторській редакції.
Упорядники: *В. Є. Козлов, О. О. Новикова*
Комп’ютерна верстка: *О. О. Новикова*

Формат 60х84/16. Ум. друк. арк. 9,62. Тираж 30 пр. Зам. № 11.

Видавець і виготовлювач Національна академія Національної гвардії України
Майдан Захисників України, 3, м. Харків, 61001.
Свідоцтво суб’єкта видавничої справи ДК № 4794 від. 24.11.2014 р.