Міжнародна науково-практична конференція

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

15 березня 2021 року, м. Харків

Ministry of Internal Affairs of Ukraine
National Academy of the National Guard of Ukraine

Ministry of Education and Science of Ukraine
Kharkiv National University radio electronics

International scientific and practical conference

"Application of information technologies in the preparation and operation of law enforcement forces"

March 15, 2021

Kharkiv

Міжнародна науково-практична конференція “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” / Збірник тез доповідей (м. Харків, 15 березня 2021 р.). – Харків. – 2021. – 132 с.

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 маркетингу Білоруського національного технічного 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, професор університету “Люблінська політехніка”, м. Люблін, Польща;

Безкоровайний В.В. – доктор технічних наук, професор, професор кафедри системотехніки Харківського національного університету радіоелектроніки;

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.

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.

УДК 623.618:519.686

Бекіров А. Е., Сєчіна А. С.

МЕТОД ПРОГНОЗУВАННЯ ВІДМОВ СПЕЦІАЛЬНОГО ОБЛАДНАННЯ НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ

Ефективне виконання бойових завдань екіпажами повітряних суден залежить від своєчасного та якісного інформаційного забезпечення. Завдання радіоелектронного обладнання літальних апаратів полягає в формуванні та наданні радіолокаційної, радіонавігаційної інформації та забезпеченні безперервного обміну повідомленнями.

Головним завданням інженерно-авіаційного служби є підтримання в постійній справності та бойовій готовності бортового обладнання. Для підтримання справності і працездатності нормативною документацією передбачені і виконують роботи, які передбачають виконання операцій по контролю показників обладнання у визначені часові інтервали. Але враховуючи застарілий парк авіаційної техніки, навіть в умовах виконання об’єму та періодичності робіт не завжди можливо спрогнозувати відмову конкретного обладнання.

Існуючи способи прогнозування відмов обладнання пов’язані з розрахунком статистичних показників. Іншим їх недоліком є те, що не забезпечується розрахунок напрацювання до конкретного елементу або блоку обладнання, а тільки напрацювання на відмову конкретного типу обладнання. В даному випадку використання розрахованих показників можливе при здійсненні планування на рівні посадових осіб відділів інженерно-авіаційної служби частин та з’єднань .

Запропоновано для вирішення задач прогнозування використання нейронних мереж. Проведено аналіз класифікації існуючих моделей та топології нейронних мереж. На основі аналізу обрана нейронна мережа тієї моделі та типу навчання, що найбільш підходить для вирішення задач прогнозування відмов бортового спеціального обладнання.

Розроблена система показників ефективності функціонування нейронної мережі із врахуванням особливості функціонування бортового спеціального обладнання. Ця система показників дає адекватну оцінку основних параметрів, які використовуються для порівняння і визначення найбільш ефективної нейронної мережі.

На основі аналізу умов експлуатації бортового обладнання сформульовано вектор вхідних параметрів, які впливають на працездатність об’єкту дослідження. На основі навчальної вибірки розроблено та проведено аналіз функціонування нейронних мереж. Так, представлено алгоритми, за якими проводяться навчання нейронної мережі, зокрема розглянуто та обрано для навчання нейронної мережі алгоритм Левенберга–Марквардта. Розроблено та проведена оцінка ефективності нейронної мережі на основі показників середньоквадратичного відхилення та дисперсії. На основі аналізу результатів оцінки можна зробити висновки про можливість використання розробленої моделі для вирішення задачі прогнозування бортового обладнання.

Полторак М. Ф., Черних Ю. О., Черних О. Б.

РОЛЬ ІНФОРМАЦІЙНОЇ КОМПОНЕНТИ ПІДГОТОВКИ КУРСАНТА В ЗАГАЛЬНІЙ МОДЕЛІ ВІЙСЬКОВОГО ФАХІВЦЯ

Інформатика є складовою частиною загальноосвітньої підготовки курсанта та одночасно першим етапом інформаційної підготовки офіцера в системі безперервної військової освіти. Включення інформаційної компоненти в зміст підготовки курсан-

та вищого військового навчального закладу (ВВНЗ) відповідає потребам сучасного етапу реформування Збройних Сил (ЗС) України та має стати предметом пильного вивчення і пошуку шляхів її реалізації в навчальному процесі ВВНЗ.

Відповідно до призначення ВВНЗ та необхідності подальшої інформатизації ЗС України виділяється пріоритетне завдання - організація і вдосконалення інформаційної підготовки науково-педагогічних працівників, курсантів та офіцерів, які проходять військову службу безпосередньо у військах (силах). При цьому під інформаційною підготовкою розуміється обов'язкова складова освітнього процесу, спрямована на підготовку фахівців, здатних ефективно використовувати засоби інформатизації та нові інформаційні технології для вирішення практичних завдань управління військами і зброєю в бойовій обстановці і повсякденної діяльності.

Інформатика – у цей час одна з фундаментальних галузей наукового знання, що формує системно-інформаційний підхід до аналізу навколишнього світу, що вивчає інформаційні процеси, методи і засоби отримання, перетворення, передачі, зберігання та використання інформації, стрімко розвивається і постійно розширює область практичної діяльності людини. Вона тісно пов'язана з використанням інформаційних технологій у військової справі. Тому, на наш погляд, можливо казати про становлення інформаційної підготовки фахівців для ЗС України, як однієї з важливих складових частин освітнього процесу.

Система військової освіти (СВО) повинна забезпечити підготовку військових фахівців, які володіють високою інформаційною культурою і здатних застосовувати засоби інформатизації, сучасні інформаційні технології при вирішенні практичних завдань бойової і повсякденної діяльності військ. Однак, фактичний стан та сукупна потужність обчислювальних ресурсів ВВНЗ ЗС України не у повній мірі забезпечують належну інформаційну підготовку курсантів. Тому, в більшості ВВНЗ інформаційна підготовка майбутніх офіцерів здійснюється за рахунок використання в навчальному процесі лише окремих компонентів новітніх інформаційних технологій, які дозволяють забезпечити тільки початковий рівень їх інформаційної підготовки. Це, в кінцевому рахунку, буде і далі посилювати процес відставання військових підрозділів (частин) та й ЗСУ в цілому в області застосування сучасних інформаційних технологій. Для вирішення всього комплексу проблем інформатизації СВО необхідне прийняття ряду заходів в масштабі ЗС, і серед них – вдосконалення інформаційної підготовки курсантів.

Таким чином, метою інформаційної підготовки курсантів у ВВНЗ є формування основ інформаційної культури майбутнього військового фахівця. Спільними завданнями вдосконалення інформаційної підготовки є: узагальнення та поглиблення теоретичних знань про основні поняття та методи інформатики; вивчення і засвоєння основ та способів подання, зберігання, обробки і передачі інформації із застосуванням комп'ютерів; формування умінь і навичок роботи на персональному комп'ютері; набуття практичних навичок із застосування нових інформаційних та телекомунікаційних технологій у професійній діяльності, яка визначається професійними стандартами.

Chernykh O., Chernykh Yu.

USES OF SIMULATION IN MILITARY TRAINING

The high level needs for effective training and protecting peoples’ lives are crucial for organizations such as military, police, catastrophe, etc in individual as well as international operations. Effective training means understanding and preparedness for how staff operates individually and together in teams. In these organizations there are frameworks and rules

for how to achieve objectives and these are of high importance when quick decisions are to be made. To operate safely and ensure safety for oneself, the team and third parties, implies that training must prepare for balanced and well grounded decision making. Balanced decision making can in one moment require a fast decision while in another situation means an elaborate and time consuming phase of deliberation before a justified decision can be made at all. These requirements lead us to a set of sub-requirements.

Firstly it leads us to requirement one. Simulation and simulation-based training have several benefits and render possibilities for individuals and teams to practice assessments of possible future events in safe circumstances. To optimize training and take into account individual differences it is of great value to use relevant tools available to make decision issues become concrete in ongoing training facilities. The simulation environment mediates events and makes it possible to distribute simulated events to several users who can interact individually. The individual interactions in collaborative contexts are rich in data.

Secondly it leads us to requirement two. The possible cognitive processes and plans operating in these contexts can be modeled in the form of beliefs, desires and intentions. The cognitive models then stand as a ground foundation in a simulation engine, whereas models created or adapted during operations call for plans that can be of use while interacting. Plans are called within the simulation cycle update to be able to match or solve shortcomings in an ongoing scenario. These updates can map actions, execute actions, fill gaps in mental operations, also read physiological responses in embodied actions within the real world and the simulated one. We can have agents copying humans but also prolong our own actions via remotely piloted vehicles or tools. This is, however, not enough. If we are serious about saving lives we need to know how we can learn from and mitigate experiences and actions that do not have expected outcomes, especially when lives are lost.

Finally it leads us to requirement third. Physiological sensor values can be input to a system to shape awareness about an individual state as well as the state of a team as whole; we can measure real world responses to provide inputs to tweak simulation challenges to become closer to the real world situation. Instrumentation including electroencephalogram, Heartrate/Pulse and galvanic skin response are all tools for making physiological interaction concrete as an additional way of understanding tasks and performance from a cognitive activity perspective, e.g. considering allocation of mental resources. An eyetracker interconnected with a simulation engine and, for example, software can show where attention has been allocated and what cognitive plans are needed in ongoing tasks. This can also be used as a gaze-directed control input. These tools can facilitate training and ensure higher awareness when tight and challenging situations occur. The glue of interaction and interoperability is the dialogue we use when exchanging and confirming information, which can either be of use or an obstacle in these situations.

These sub-requirements lead us to a middle level. Humans have cognitive limitations and technology and software agents can potentially fill these gaps in compensating for rich information flows that can otherwise end up in mental overload. If there is an under load we may also want to keep people stimulated so they can keep up their fitness curve.

How can simulation-based training challenge and become better? Better here means better preparing people and systems for tasks, based upon how we can get closer to a real world environment while we sit in a safe, de-contextualized contextualized environment.

The evaluation and improvement of the task performance process is a goal, so that team based training can achieve outcomes otherwise impossible to show, either retrospectively or directly. Improvement suggests building a system that can fulfill the evaluation of an ongoing process and provide active feedback during performance in the process. Are there ways where digital technology can provide the support that can be of help for individuals and teams in training and operational tasks, so the simulation-based training can reach closer to a real world context? Answering these questions and trying to find out what could

be of help is a great underlying motivation for this dissertation. The work explores plausible answers to these questions based upon field studies of an operational, simulation-based training environment.

This theses are concerned with training for cognitive processes, but not physical manipulation skills per se. The virtual simulation is used to prepare for certain skills and modular mental capacities for subsequent live simulations. The agent world implemented by the simulation can also be regarded as being close to a constructive simulation, responding to stimuli in the form of real human and machine inputs.

There is a need for cognitive process modeling in relation to gazed objects, but since we do not completely understand the inner workings of the human mind, it is easier to gather information about observed human reactions to certain situations than it is to represent the process of cognition. Intelligent agents with cognitive gaze control can potentially offer new solutions meeting the requirements summarized here.

To be more precise, we look at events, events that can be used to teach someone, events that can be used to teach someone how to do something, and the process of making such a model. The events that can be used to teach someone have two aspects. Firstly, the aim is to build a comprehension about human-human communication in decision-making under training in relation to observational tasks. Secondly it is to understand this human-human process so it becomes possible to sketch up cognitive models that can be the basis for an (inter-)agent architecture and agent interaction. Thirdly, this can either provide direct support for decision making in events and teams, or can be used for training opponents and digital colleagues. Training can consist of various tasks, from language and cultural issues to team training in routines and breakdowns.

Simulated events are running in a simulation/game engine and mediated and visualized through 3d graphics as representations of the world and its inhabitants. Steering of controllable objects happens through input devices, most commonly keyboards and the 3d graphics generated on computer screens or projections, the interaction between a human and the computer-mediated content.

Military organizations are heavily involved in the use of simulation and related technologies, especially for training purposes.

A technician provides a series of scenarios to the soldiers and teaches them how the tools work and how to change those scenarios to the extent the system will allow. The soldiers start 'playing' the scenarios, then they start adapting those scenarios to make them more realistic. They are not only learning the given scenarios, but teaching themselves to replicate real-life experiences to re-live and recreate what they've seen on their own missions. The argument is that users are able to take another look at specific events from a stress-free environment and provide developers with valuable input about the effectiveness of the training. Modern tools for training have spread beyond combat to medical and cultural scenarios. The military has also expanded its research to varied uses of artificial intelligence.

Lavrut O., Lavrut T.

APPROACHES TO DIAGNOSTICS OF MODERN MEANS OF COMMUNICATION IN POWER STRUCTURES OF UKRAINE ON THE BASIS OF NEURAL NETWORKS

In recent years, the power structures of Ukraine have been expanding and improving the system of communication and the automatic control of forces.

The requirement of reliable operation of electronic equipment in the system of complex automation of control processes with the use of complex multifaceted systems,

communication and automation tools (CAT) is especially acute. Therefore, the development of new, high precision and reliable faultfinding methods is becoming increasingly urgent.

A variety of research methods can used in the diagnostic system, which include theories of graphs, decision support systems, fuzzy sets, neural networks, multi-criteria optimization methods, expert methods.

The method of expert evaluation gives an objective description of the qualitative and quantitative aspects of the object of forecasting based on processing and analysis of a set of individual opinions of experts.

Neural networks and fuzzy logic are universal approximations of complex (nonlinear) functional dependencies in many intellectual cybernetics problems.

The main feature of neural networks is their ability to learn, which is implemented using specially designed algorithms.

The analysis of the literature showed that the use of neural networks for the diagnosis of communications (for example, during routine of technical maintenance, repair, as well as in a state of continuous operation) is today a poorly understood and relevant direction that will allow to solve this problem.

A neural network is proposed, which is built to diagnose communication equipment (an example of constructing a network for a task). The method of support vector networks or tracing is used during the construction. As inputs (standards) working effects are used: those that get on the device during its intended use, and those that are its main output parameters (you can also use specially generated test effects). At the output layer, the expected response to the defined input standard is formed.

During the calculations, it was assumed that all the same neurons perform the same transfer function, and the scales and thresholds realize equal and common capabilities.

Based on the calculations for the construction of the network, an appropriate table is compiled, which reflects the correct operation of the network when making different decisions. Analyzing the terms of the table, which correspond to reliable situations, it can seen that the maximum excitation is determined correctly enough. This allows us to assert that the neural network, designed directly for the task, is built correctly.

Technically, the process of diagnostics of various communication and automation tools can implemented by a single measuring and diagnostic complex based on a personal computer (PC). With a switching device that connects the outputs of the equipment to the PC input, the status recognition process takes seconds. The results of the construction of a neural network for solving the problem of diagnostics of modern communication and automation tools are given, which will allow reducing the time for conducting technical maintenance and the number of measuring instruments involved.

In the future, it is necessary to create a single package of applications for diagnostics of different types of communication devices based on neural networks, as well as a switching device by which the outputs of the equipment should connected with the input of the PC of the operator's workplace.

УДК 355; 629.7.052.

Гончар Р. О.

ПІДХОДИ ДО ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ДЛЯ ОХОРОНИ ВАЖЛИВИХ ДЕРЖАВНИХ ОБЄКТІВ

Виходячи з положень Закону України “Про Національну гвардію України” підрозділи та частини Національної гвардії України (НГУ) здійснюють охорону важли-

вих державних об’єктів (далі об’єкти). перелік яких визначається Кабінетом Міністрів України. В умовах збільшення диверсійно-терористичних загроз актуальним є питання впровадження сучасних технологій в систему охорони та оборони об’єктів. В загонах спеціального призначення та розвідки НГУ, успішно та ефективно використовують безпілотні літальні апарати (БПЛА) для виконання службово-бойових завдань. Сучасні технології безпілотних літальних апаратів дозволяють автоматизувати велику частину процесу польоту, перетворюючи БПЛА в рухому літаючу платформу, яка комплектується різними приладами в залежності від вимог. Однією з функцій безпілотних літальних апаратів є відеоспостереження та відео-фіксація. Моделюючі дії порушника (груп порушників) при спробі проникнення на об’єкт, ми можемо стверджувати що велика швидкість руху, мінімальний час вильоту БПЛА дозволить йому оперативно прибути до найвіддаленішого місця проникнення на периметрі об’єкту. Використання БПЛА в службово-бойовій діяльності частин та підрозділів НГУ з охорони важливих об’єктів дозволить:

- здійснити з’ясування первинної ситуації з метою виключення хибної тривоги;
- надати візуальні відомості начальникові варти для прийняття рішення для використання відповідних сил та засобів реагування;
- здійснити подальший пошук та супроводження дій порушника (груп порушників) при їх діях всередині периметру об’єкту;
- здійснювати відео-фіксацію дій порушників та груп реагування варти;
- надавати відеодані оперативної обстановки для організації оборони об’єкту та ін.

Особливою перевагою БПЛА в попередженні проникнення (атаки) на об’єкт, є розширення зони спостереження за зовнішнім периметром більш як на 50 метрів, та тих важливих ділянок об’єкту, які не охоплюються наземною системою відеоспостереження. Для здійснення ефективної охорони об’єкту БЛА повинен володіти рядом необхідних характеристик: мати засоби візуального виявлення цілей, як в світлий, так і в темний час доби. Для візуального виявлення цілей в нічний час доби БПЛА обладнується тепловізорами; мати можливість вильоту в холодну і теплу пору року, при максимально широкому діапазоні температури повітря; мати можливість вильоту в дощ і сніг; мати відповідні характеристики супротиву вітру, характерного для конкретноїмісцевості. В той же час, БПЛА повинен бути інтегрований в єдиний комплекс з системою охорони та оборони об’єкту. Сигналом до зльоту БПЛА має служити сигнал від технічних засобів охорони об’єкту, з визначенням координат місця спрацювання. За цими координатами БПЛА автоматично або з підтвердженням команди оператора злітає зі стартового майданчика і в автоматичному режимі летить до місця спрацювання засобу виявлення. Для розміщення та функціонування БПЛА в режимі чергування чи патрулювання об’єкту слід вирішити ряд відповідних технічних задач.

Таким чином питання впровадження безпілотних літальних апаратів в службово-бойову діяльність підрозділів та частин НГУ які здійснюють охорону важливих державних об’єктів є актуальним та потребує подальшого наукового дослідження.

UDK 621.396.962

Herasimov S., Roshchupkin E.

USES OF LASER SIGNALING SYSTEMS WITH DIFFRACTIVELY REFLECTING COATINGS

Promising automatic systems for protecting objects and perimeters of the area from all kinds of intruders are being developed based on the use of laser alarm systems [1–5]. This

is due to the advantages of laser systems: the absence of physical and electronic contacts between the components, the accuracy of laser devices; light weight and small dimensions of lasers; high noise immunity and ease of installation and alignment of laser devices [1].

Laser alarm systems allow simultaneous blocking of the terrain area perimeter and of the protected object and conduct optical-electronic reconnaissance [2]. Thus, the use of laser signaling systems for solving the problems of protecting the area perimeters and objects and conducting reconnaissance is promising.

Laser alarm systems usually consist of a transmitter and receiver, which are located in a line of sight. In this case, the sensor of such an alarm generates an alarm signal when the laser beam is interrupted, falling on the receiving unit [3].

At the same time, laser alarm systems have a number of disadvantages. The main disadvantage is false alarms in difficult weather conditions, which reduce the transparency of the environment (eg fog, rain, snow). In this case, the reliability of laser alarm systems can be ensured by using multiple excess of the laser radiation energy over the minimum threshold value necessary for the system to operate.

In practice, when using laser signaling systems, it is necessary to take into account the cumulative effect of the radiation interaction with the atmosphere, which is simultaneously an absorbing, scattering and randomly inhomogeneous medium [4]. This influence can occur in a very wide range. Therefore, in order to ensure the required level of laser signaling systems reliability at a given distance, it is proposed to obtain a sufficient power reserve with the possibility of forming several "laser barriers".

One of the promising solutions to this problem is the use of diffractively reflecting coatings (as a reflective element) as part of a laser signaling system. Such coatings make it possible to redistribute the energy of the reflected laser radiation in space. This allows, when calculating the characteristics of a laser alarm system, to make the transition from uniform reflection, which is described by Lambert's law, to a substantially non-uniform distribution, which is characteristic of laser radiation reflection on diffraction gratings [5].

The use of diffractively reflecting coatings as part of a laser signaling system makes it possible to provide:

- multiple increase in the power of the reflected laser radiation;
- the possibility of forming a certain number of "laser barriers" along the diffraction maxima propagation directions of the scattering diagram of the diffractively reflected coating.

In practice, it is impossible to take into account absolutely all the factors affecting the quality of the fabrication of a reflecting coating diffractively (for example, the uniformity of the washout of the photoresist during the production of coatings by photolithography). With the same surface material and the same technology for its processing, each time the laser radiation reflection occurs from diffractively reflecting coatings that have the required surface profile, but not identical, but only similar to each other. Such coatings have the same statistical properties, but their surfaces are specifically described by different equations. The degree of their difference largely depends on the perfection of the modern technology for the manufacture of diffractive phase coatings.

Taken together, diffractively reflecting coatings obtained with the same technological processing form a single statistical ensemble, the full description of which is given by the density functional probability. This theoretic-probability approach to describing the statistical properties of a surface has been extensively developed [1, 4]. In practice, when describing errors, they are limited to the approximation of their fluctuations by some normal random process, the parameters of which are set by analyzing the effect of coating production conditions on the statistical characteristics of the errors that appear. Such an approximation turns out to be quite satisfactory, which is a consequence of the joint and additive influence of a large number of factors independent of each other on the process of manufacturing diffraction-reflecting coatings.

In the presence of errors in the manufacture of diffractively reflecting coatings (roughness), the radiation power corresponding to the weakening of the coherent component of the illumination signal is scattered in directions that do not correspond to the directions of the diffraction maxima formation of the angular of the radiation intensity distribution function reflected from the coating. The total power of laser radiation reflected from a diffractively reflecting coating has two components: specular (coherent) and diffuse (incoherent). The specular component is due to the reflection of the optical wave from the coating. The diffuse component is due to scattering by roughness. These components of the reflected radiation power are characterized by the corresponding intensities.

An analysis of the angular distribution functions of the coherent radiation intensity reflected from a diffractively reflecting coating of the "echelette" type, presented in the figures, allows us to draw the following conclusions:

- the form of the distribution function of the reflected radiation intensities substantially depends on the relationship between the values $\Delta\omega$ and 1/M2;
- in $\Delta\omega >> 1/M2$ the width of the diffraction maximum of the intensity distribution function is determined by the divergence of the illuminating laser radiation $\Delta\omega$;
- in $\Delta\omega << 1/M2$ the width of the main diffraction maximum of the intensity distribution function is determined on the value 1/M2 the angular size of the main diffraction maximum of the coating scattering pattern under laser illumination with $\Delta\omega \approx 0$.

In practice, as a rule, lasers are used in laser signaling systems, which are characterized on wavelengths $\lambda = (0.63 \dots 10.6)$ mkm and the laser radiation divergence $\Delta\omega = (10–3 \dots 10–4)$ radian in distances (3 … 10) km. Under such conditions, the angular width of the main diffraction maximum of the distribution function of the coherent radiation intensity reflected from a coating with a constant $d = (1 \dots 10)\lambda$, will be largely determined by the value of the divergence $\Delta\omega$ illuminating laser beam. Then this coating should be considered as a coating that re-reflects the laserradiatio illumination into the angular sector determined by the blaze angle.

The paper substantiates the prospects of using diffraction-reflecting coatings as part of laser signaling systems to improve reliability. An increase in the such alarm systems reliability occurs due to a power increase of reflected laser radiation and the possibility of forming a certain number of "laser barriers" in different directions.

A power increase of the reflected laser radiation as a result of the diffractively reflecting coatings use will lead to an expansion of these alarm systems of the range of diffractively reflecting coatings in (3 ... 5) times in comparison with existing laser alarm systems.

The formation of (5 ... 7) "laser barriers" will allow effective control over a certain area not only in one direction, as in the existing laser signaling systems, but in the whole sector of (40 ... 700) directions. In this case, the sector width is determined only by the parameters of the diffractively reflecting coatings, but additional sources of laser radiation are not required.

In general, laser signaling systems with diffractively reflecting coatings, in contrast to existing laser signaling systems, allow solving additional tasks of assessing the movement speed of objects in the protected area and determining their movement directions.

References

1. S. Herasimov, Y. Kozhushko, E. Roshchupkin, V. Dekadin, V. Djus, and Y. Melenti, **Evaluation of surface profile of holographic diffraction reflective coatings on scattering chart using in laser alarm systems**, *International Journal of Emerging Trends in Engineering Research*, vol. 8, is. 8, 2020, p.p. 4502-4507, https://doi.org/10.30534/ijeter/2020/74882020.

2. S. Herasimov, O. Tymochko, O. Kolomiitsev, G. Aloshin, O. Kriukov, O. Morozov, and V. Aleksiyev, **Formation Analysis Of Multi-Frequency Signals Of Laser**

Information Measuring System, *EUREKA: Physics and Engineering*, vol. 5, 2019, p.p. 19-28, https://doi.org/10.21303/2461-4262.2019.00984.

3. S. Herasimov, E. Roshchupkin, V. Kutsenko, S. Riazantsev, and Yu. Nastishin, **Statistical analysis of harmonic signals for testing of Electronic Devices**, *International Journal of Emerging Trends in Engineering Research*, vol. 8, is. 7, 2020, p.p. 3791-3798, https://doi.org/10.30534/ijeter/2020/143872020.

4. S. Herasimov, M. Pavlenko, E. Roshchupkin, M. Lytvynenko, O. Pukhovyi, and A. Salii, **Aircraft flight route search method with the use of cellular automata**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, is. 4, 2020, p.p. 5077-5082, https://doi.org/10.30534/ijatcse/2020/129942020.

5. S. Herasimov, V. Pavlii, O. Tymoshchuk, M. Yakovlev, D.Ye. Khaustov, Ye. Ryzhov, L. Sakovych, and Yu.A. Nastishin, **Testing Signals for Electronics: Criteria for Synthesis**, *Journal of Electronic Testing*, vol. 35, is. 148, 2019, p.p. 1-9, https://doi.org/10.1007/s10836-019-05798-9.

UDK 623.418:623.55

Kudryashov V., Litovchenko D.

IMPROVING THE FIRING EFFICIENCY OF ZU-23 THROUGH THE USE OF RADAR MILLIMETER WAVELENGTH RANGE

The results of numerical simulation of the range of detection by the personnel of the paired anti-aircraft gun ZU-23 and radar millimeter (mm) wavelength range in different conditions of combat use are given. The values of the static probability of detection of targets and projectiles by the personnel of ZU-23 and radar mm of the wavelength range are presented. We are considering firing ZU-23 on a typical target (TT) and on an unmanned aerial vehicle (UAV). An ”Forpost” type device was chosen as the UAV. Ranges of target detection by ZU-23 personnel $D_c(S,\xi_c,\xi_m,\xi_p,\xi_s,\hat{E}_c)$ with a probability of correct detection of 0.5 depend on various factors. The average range of detection of targets with the naked eye and its capture in the collimator sight ZU-23, for moderately trained personnel ZU-23, is 8.5 km. When using a small radar type ”Fox-3” (”Mangus”) significantly increases the detection range of various air targets $D_{ci}(\sigma)$. The probability of correct detection of personnel ZU-23 for typical target is $D_{\tilde{n}1}(6{,}8\cdot 10^3)\approx 0{,}5$, and on UAV $P_{c1}(1717)\approx 0{,}5$ in case of possible omission of the target by the personnel $P_{np}=0{,}4$. The probability of correct detection of radar mm in the wavelength range $P_{ci}(D)$ of the helicopter and UAV, respectively, without interference and with interference of high intensity is $D_{\tilde{n}3}(12\cdot 10^3)\approx 0{,}5$ and $D_{\tilde{n}4}(5914)\approx 0{,}5$. We noted the high probability of detecting the air target of the radar type ”Fox-3” (”Mangus”). When conducting a large-scale simulation of the effective scattering surface (ESS) of 23 mm projectile, used the known ESS 9M22, OF-462 and OF-25 in dicimeter and centimeter wavelength ranges. Large-scale modeling by the caliber and length of the projectile gave a radar wavelength of ~ 5,9 mm. Moreover, if the angle between the axis of the projectile and the normal to the pattern of the radar antenna is in the range 0°–45°, at an elevation angle of ε = 0°, then the ESS of the projectile is $\sigma_{23}\approx 0{,}12$ m^2 and if ε = 10° – $\sigma_{23}\approx 6{,}51\cdot 10^{-3}$ m^2. The results of calculations of the

angle between the axis of the projectile and the normal to the radiation pattern of the radar antenna were constructed by changing the height H from 10 m to 100 m. Simulations were performed at firing range $r_t \approx 2103$ m and azimuth of targets $\beta_t \approx 27^\circ$. We obtained that the reflected signal is formed mainly by the bottom cut of the projectile, where its ESS can be more than ~ 0,12 m^2 at the elevation angle ε = 0°. It follows that the possibility of stable detection of radar station mm wavelength range (~ 5,9 mm) 23 mm projectile in the firing zone ZU-23 at ε = 0° with a probability of at least 0,5.

The obtained results create conditions for the detection of various air targets and projectiles, along the routes of their flight. The probability of missing targets by ZU-23 personnel is significantly reduced. The introduction of adjustments during firing will increase the effectiveness of combat use ZU-23.

UDK 358: 623.76: 623.4

Kutsenko V., Kolomoyets M.

FACTORS AFFECTING FIRE CAPABILITIES OF ANTI-AIRCRAFT MISSILE ARTILLERY DIVISION BRIGADE PURPOSE OPERATIONAL NATIONAL GUARD OF UKRAINE

The set of issues that determine the state of the air defense system necessitates the presence of a special scientific apparatus, which allows you to assess the effectiveness of anti-aircraft air defense units that are part of the system and identify ways to improve it. The increasing complexity and responsibility for solving problems solved in all areas of human activity, primarily in the military, made it necessary to conduct a deep preliminary study and justify the decisions taken.

This is what leads to the need for the introduction and proper understanding of concepts such as the possibilities troops and effectiveness of the troops.

A more detailed look at the factors that affect fire capabilities anti-aircraft missile artillery division of brigade purpose operational National Guard of Ukraine.

First, the quantitative and qualitative indicators of military equipment that are part of the air defense system; the number of personnel in that military equipment. They quantifiable indicators display, convenient for use during calculations and justification of the decision which was adopted in battle.

Secondly, the level of combat training units, moral and psychological state of personnel, availability of combat experience, degree of military and special training and practical training. In real conditions, the influence of factors of this group is determined, as a rule, by the method of expert assessment.

Third, the type of hostilities, the nature of the enemy's resistance, the provision of material and technical means, geographical conditions, time of year and time of day. Their impact on hostilities is taken into account on the basis of analysis involving quantitative estimates and indicators.

Therefore, the possibility of air defense departments NGU of the tasks combat activity – a possibility of all units to implement certain of combat missions in specific circumstances. These possibilities depend on the number of personnel, the level of their training and moral and psychological condition, the availability and condition of weapons, equipment and special means of active defense. Command art in management of the troops, organizational structure of troops, provision of material resources, as well as the strength and nature of the opposite party (organized crime groups, crowds, illegal armed groups, the enemy, etc.) and many other factors. This concept is broader than the combat capabilities of troops, because

it takes into account the nature of the tasks of the NGU and the conditions of their implementation in contrast to, for example, the tasks of the Armed Forces Ukraine.

UDK 323. 4

Kovalenko S., Volkov A.

ENSURING THE COVER OF A SEPARATE MECHANIZED BRIGADE BY GROUND BASED AIR DEFENSE UNITS IN THE CONDUCT OF LOCAL CONFLICTS

Based on the tasks assigned to the ground based air defense (GBAD) to cover mechanized, motorized infantry and tank brigades of the Land Forces in the area of local conflicts, it is necessary to substantiate the possibility of their combat mission.

The substantiation is carried out to clarify the possibility of combat missions to be performed by GBAD in conditions that go beyond the combat purpose of these units, in accordance with the combat statutes.

In the area of local conflict, all units of the Land Forces are stretched along the front, which will lead to an increase in the positional areas of the brigades along the front and in depth. This will increase the load on the GBAD to cover these brigades from the air.

Therefore, determining the possibility of covering the GBAD units of a separate mechanized brigade on the new positional areas, which have changed in size and on the front and in depth is an urgent task. To do this, it is necessary to develop a methodology or model that would help the commander of the GBAD unit to make preliminary calculations on the effectiveness of the cover of units of the Land Forces. An indicator of the ability of GBAD units to perform or not perform their combat mission is to assign the effectiveness of unit cover (Рпр.ППО). For the analysis and calculations, the areas of cover of objects and the areas of cover zones of the currently available GBAD units, which are in service in Ukraine, for air cover were determined.

The proposed method is devoted to this question, which will help the unit commander to choose the best option for its location on the ground.

УДК 621.39

Олійник С. Е.

ПРОБЛЕМИ ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ МІЖ ПІДРОЗДІЛАМИ ЗБРОЙНИХ СИЛ УКРАЇНИ ТА ІНШИХ СИЛОВИХ СТРУКТУР

З початком ведення гибридної війни на сході України встало питання забезпечення стійкого та ефективного управління підрозділами Збройних сил України (ЗСУ) та правоохоронних органів, які виконували завдання за призначенням. На початку війни, у зв’язку з відсутністю достатнього фінансування у попередні роки, основу системи зв’язку ЗСУ і силових підрозділів складали аналогові засоби, які були не сумісні з державною цифровою телекомунікаційною мережею розгорнутою на базі “Укртелекому”. А різні відомчи організації ЗСУ та правоохоронних органів не мали можливості доступу та сумісного використання інформаційних носіїв, що ускладнювало їхню взаємодію і в цілому не відповідали сучасним вимогам. Тому, основою вирішення проблем питання можливості ефективної взаємодії різних структур ЗСУ та

правоохоронних органів, має бути перехід на сучасні інформаційні технології та забезпеченість цифровими засобами зв'язку провідних країн світу у відсутності власного виробництва.

Купівля сучасних цифрових засобів транкінгового зв'язку корпорації "Mototrbo" у 2014-2016 роках надало перший крок до вирішення проблем використання та взаємодії між підрозділами ЗСУ та правоохоронними органами.

Поступовий перехід ЗСУ на цифрові засоби зв'язку, які закуповуються в країнах-партнерах України по НАТО, а це цифрові радіостанції таких провідних корпорацій, як "Harris Corporation" США, Туреччини "Aselsan Elektronik Sanayi", та Їзраїльської "ELBIT", які допущені до експлуатації в ЗСУ, вирішує питання об'єднання систем управління та обміну інформації для вирішення ефективного управління при виконанні завдань за призначенням на сході країни та в повсякденній діяльності. Сучасні радіостанції можуть передавати не тільки голосові повідомлення, але і обмінюватися даними, в тому числі зображеннями і відео, з досить великою швидкістю. Такий широкий функціонал забезпечується використанням технології SDR (Software-Defined Radio). Радіостанція з програмованими параметрами SDR відкриває нові горизонти можливостей в умовах бою та повсякденним використання під час виконання завдань за призначенням. Принцип SDR технологій -злиття можливостей комп'ютера і радіостанції.

Радіостанція з SDR використовуючи кілька рівнів програмного забезпечення для виконання різних завдань, так само як і настільний комп'ютер, може, наприклад, проводити обробку тексту, забезпечити перегляд Інтернет-ресурсів, забезпечити відіоконференцзв'язок, а також управління базами даних в залежності від потреб користувача.

Сьогодні у ЗСУ величезна увага приділяється розвитку та вдосконаленню стаціонарної та польової компоненти системи зв'язку та автоматизації управління всіх рівнів ланок управління в частині їх повного переоснащення новітніми засобами, переходу на цифрові системи передачі та обробки інформації. Технологічно основою для реалізації даної системи стане єдина автоматизована система ЗСУ, яка буде інтегрувати автоматизовані системи бойового управління, обчислювальну техніку, засоби зв'язку, радіоелектронної боротьби, розвідки, навігації та засоби вогневого ураження.

Застосування новітнього високотехнологічного обладнання зв'язку дало змогу відмовитись від застарілих та слабоефективних принципів організації і забезпечення зв'язку та перейти до організації надання в інтересах пунктів управління якісних інформаційно-телекомунікаційних сервісів: IP-телефонія, відео та аудіо конференція, швидкісна передача даних, криптографічний захист інформації, обмін електронними повідомленнями, тощо.

Зараз ведеться робота щодо створення ефективної системи оперативного управління, зв'язку, розвідки та спостереження (C4ISR), яка б відповідала стандартам НАТО, та забезпечення її інтеграції з Єдиною системою управління оборонними ресурсами (Defense resources management information system – DRMIS).

Оперативна ціль 1.2. Удосконалення системи управління силами оборони.

Очікуваний результат: створено відповідно до євроатлантичних стандартів ефективну систему управління, що дає змогу проявляти ініціативу і надає більшу самостійність керівникам органів управління сил оборони усіх рівнів у прийнятті управлінських рішень, удосконалено координацію між складовими сил оборони та впроваджено механізм, що забезпечує їх консолідований розвиток, досягнуто необхідні оперативні спроможності для забезпечення оборони держави.

Оперативна ціль 1.4. Створення ефективної системи оперативного (бойового) управління, зв'язку, розвідки та спостереження (C4ISR).

Очікуваний результат: створено національну телекомунікаційну мережу, модернізовано та переведено на сучасні цифрові технології системи спеціального зв'язку, ві-

домчі інформаційно-комунікаційні мережі та системи зв'язку пунктів управління органів державної влади, а також створено автоматизовану систему C4ISR складових сил оборони, яка відповідає стандартам, доктринам і рекомендаціям НАТО, забезпечено її інтеграцію в систему управління оборонними ресурсами.

Оперативна ціль 1.5. Удосконалення системи кібербезпеки та захисту інформації.

Очікуваний результат: створено в Міністерстві оборони України, інших складових сектору оборони підрозділи з кіберзахисту, протидії технічним розвідкам, впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC.

Для забезпечення повного переходу підрозділів ЗСУ та правоохоронних органів на сучасні інформаційні технології необхідно:

- забезпечити використання тільки цифрових засобів телекомунікацій сертифікованих для військового призначення та правоохоронних оргінів;
- повністю відмовитись від використання цивільних корпоративних засобів зв’язку в інтересах забезпечення стійкого та ефективного управління підрозділами ЗСУ та правоохоронних органів;
- створити єдине інфотелекомунікаційне середовище у ЗСУ та інших силових структурах;
- забезпечити сумісність мереж військового зв'язку з мережами загального користування національних систем зв'язку і мережами інших силових структур;
- розробити новітні програми для забезпечення роботи на усіх рівнях користування;
- провести повну інтеграцію всіх телекомунікаційних засобів ЗСУ, силових оргінів та інших державних структур управління;
- забезпечити кібернетичний захист інформаційних мереж.

Це дасть можливість користування потрібною інформацією усіх зацікавлених структур для забезпечення швидкості збору та обробки інформації; швидкому вводу та пошуку необхідних даних у реальному відліку часу; перехід на використання сумістних зі стандартами армій НАТО інформаційних мереж. Підняти оборонну спроможність України на більш високий рівень. Здійснити повну інтеграцію України в блок НАТО.

УДК 654.01

Власов К. В.

ФЕДЕРАТИВНА МЕРЕЖА МІСІЙ – ОСНОВНІ ТЕРМІНИ, СТРУКТУРА, ПРИНЦИПИ ТА ОСОБЛИВОСТІ ДЛЯ ПОТРЕБ НАЗЕМНИХ ВІЙСЬК ТАКТИЧНОЇ ЛАНКИ НА СУЧАСНОМУ ЕТАПІ ЗА СТАНДАРТАМИ НАТО

Об’єднана мережа для проведення операцій *(en: Federated Mission Networking, FMN)* являє собою підхід НАТО до уніфікації коаліційних мереж для забезпечення обміну інформацією з використанням сервісів, спільного використання інформації між партнерами місії та керівництво встановленням зв’язків між мережами місій НАТО, держав – членів НАТО та не-НАТО структурами протягом проведення оперативних заходів під проводом НАТО.

Концепцію FMN було затверджено рішенням МСМ 0125-2012 NATO Future Mission Network Concept; 21 Nov 2012. Ця концепція містить загальні вказівки щодо формування спроможностей федеративної мережі місії, які дозволять забезпечити ефективний обмін інформацією між НАТО, країнами-членами НАТО та/або суб'єктами, що не входять до НАТО, в ході проведення операції.

Планом реалізації FMN НАТО (NFIP) передбачається: “Концепція (FMN) уявляє світ в якому командир операції отримує можливість підтримання ефективного зв'язку із кінцевими виконавцями, а також обміну інформацією в межах коаліції. Це реалізується шляхом спільного розуміння характеристик згаданих процесів та доступу до спільної інформації конфіденційного характеру. Командир має володіти спроможністю доводити накази, задум та вказівки до підрозділів тактичної ланки, а також подавати звіти та рекомендації до органів стратегічного рівня. Потреба у забезпеченні доступу до інформації для підрозділів коаліції виникає за будь-якого можливого сценарію майбутніх операцій. Відтоді особливого значення набуває формування довіри та прозорості серед учасників операції”. Механізм реалізації подібного бачення передбачає запровадження гнучкої та масштабованої CIS мережі місії серед учасників операції – незалежної системи управління. Обмін інформацією між учасниками операції відбувається у безперебійному режимі на рівні мережі місії. При цьому учасники можуть виходити або приєднуватися до мережі без впливу на стан забезпечення сервісів для решти учасників операції.

У концепції FMN зазначається: “Платформа FMN – це керована, контрольована та всеосяжна структура, що забезпечує всі необхідні процеси, плани, шаблони, корпоративну архітектуру, а також складові елементи спроможностей та інструменти для підготовки (зокрема, планування), розробки, розгортання, використання, розвитку та закриття мереж місії на підтримку операцій НАТО та багатонаціональних операцій в умовах динамічного або федеративного середовища”. З метою реалізації подальшого розвитку мережі місії, розвиток платформи FMN вбачає застосування спірального підходу до поступового розширення сервісів та спроможностей, які можна об'єднати в межах мережі місії. Кожні два роки здійснюється розробка специфікацій нової спіралі (FMN SpSp), що враховує нові бачення оперативних потреб по кожній спіралі, які пройшли відповідне погодження у партнерів по FMN.

Подальше керівництво процесом реалізації спіралі здійснюється відповідно до документу-концепції FMN SpSp на період 10 років та Дорожньої карти FMN SpSp, що визначає етапи розвитку спіралі для реалізації бачення FMN. В свою чергу, учасники зобов'язуються реалізувати положення останнього FMN SpSp у власних системах, провести самооцінку їх відповідності та поширити відповідну інформацію через платформу FMN в якості обов'язкового підтвердження.

Остаточним етапом підтвердження відповідності сервісів FMN встановленим специфікаціям вважається проведення спеціального заходу для перевірки готовності FMN, зазвичай, у вигляді багатонаціонального навчання. В ході навчання відпрацьовуються оперативні, адміністративні та технічні сторони вимог FMN SpSp.

УДК 621.396.96 (043.3)

Горєлишев С.А., Волков П.Ю., Баулін Д.С.

МЕТОДИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ХАРАКТЕРИСТИК РОЗСІЮВАННЯ ОБ’ЄКТІВ У ЗОНІ ПРИХОВАНОГО РАДІОЛОКАЦІЙНОГО БІСТАТИЧНОГО СПОСТЕРЕЖЕННЯ

Характеристиками розсіювання радіолокаційних об’єктів (РЛО) є електромагнітне поле (ЕМП), що розсіяне цим об’єктом, при заданої поляризації електромагнітної хвилі (ЕМХ), як функція частоти, просторових параметрів або часу;бістатичнаефективна поверхнярозсіяння (ЕПР) РЛО при заданої поляризації ЕМХ,як функція частотита просторових параметрів; сигнали, які відбиті РЛО (відповідні їм спектри); радіолокаційнідальнісні портрети (РЛДП) при фіксованих напрямах приймання та параметри спектрів ам-

плітудної модуляції сигналів, які відбиті.

Для отримання характеристик радіолокаційного розсіювання різних РЛО у даний час застосовуються методи фізичного і математичного моделювання. Ці методи розвиваються паралельно. На даний момент з усього різноманіття відомих методів фізичного моделювання найбільшого поширення набули:

- полігонні вимірювання ЕПР реальних об'єктів (зокрема вимірювальні системи 2 ЦНДІ МО, Російська Федерація; MVG MicrowaveVisionGroup, HowlandCompany, США);
- вимірювання ЕПР масштабних моделей в безлунних камерах.

Зрозуміло, що фізичне моделювання пов'язане зі створенням і використанням дорогих вимірювальних стендів, а для оцінювання характеристик засобів протиборчої сторони вимагає створення фізичних моделей цих засобів.

Швидкий розвиток комп'ютерної техніки у останні десятиліття призвів до появи ефективних математичних методів розрахунку характеристик радіолокаційного розсіювання. Враховуючи той факт, що їх застосування не потребує значних фінансових і матеріальних витрат, різноманітність сценаріїв радіолокаційного зондування, яку можна змоделювати у порівняно невеликий час, застосування методів комп'ютерного моделювання має ряд переваг у порівнянні із фізичним моделюванням. Разом із цим до математичних методів пред'являються жорсткі вимоги щодо точності відтворення характеристик розсіювання об'єктів радіолокації.

Обрання того чи іншого методу моделювання залежить від складності об'єкта, його електричних розмірів і матеріалів, з яких виготовлено його елементи, а також умов зондування. На практиці доводиться мати справу з РЛО, що мають металеву поверхню, з діелектричними розсіювачами і об'єктами, що містять як металеві, так і діелектричні елементи конструкції.Електричні розміри РЛО (відношення його характерного геометричного розміру а до довжини ЕМХ λ) можуть належати до низькочастотної (релеєвської, $a/\lambda<<1$), резонансної ($a/\lambda\approx1$) або високочастотної (квазіоптичної) областям ($a/\lambda>>1$).

Чисельну реалізацію точних методів представляють: метод власних функцій; метод кінцевих різниць у часовій області (finitedifferencetime-domain (FDTD) method); метод скінчених елементів (finiteelementmethod, FEM); метод дискретних джерел; метод дротяних моделей і метод інтегральних рівнянь (IP).Для вирішення дифракційних задач, пов'язаних з об'єктами великих електричних розмірів, розвиваються асимптотичні методи, більшість з яких можна віднести до методів: геометричній оптики (ГО); геометричній теорії дифракції (ГТД); фізичної оптики (ФО) та фізичної теорії дифракції (ФТД).

Серед перерахованого різноманіття чисельних методів найбільшими можливостями при розрахунку ЕМП, розсіяного РЛО складної форми і різних електричних розмірів, отримали методи FDTD, IP та асимптотичні.

Відомі асимптотические високочастотні методи дозволяють з досить високою точністю (про що свідчать порівняння результатів розрахунку з даними фізичних експериментів) моделювати характеристики РЛО великих електричних розмірів. У той же час високочастотні методи не дозволяють з достатньою точністю розраховувати характеристики об'єктів резонансних розмірів, до яких слід віднести такі повітряні РЛО, як ракети і їх складові частини, безпілотні літальні апарати (БПЛА), невеликі маловисотнимилітаки, наземні об'єкти - бронетанкова і автомобільна техніка , люди і ін. при застосуванні РЛС метрового діапазону довжин хвиль. Локація наземних РЛО має ряд особливостей в порівнянні з РЛО в повітряному просторі. Відбитий наземним РЛО сигнал спостерігається на тлі потужного відбиття від підстилаючою поверхні. Крім того застосування сигналів метрового діапазону довжин хвиль ефективно для виявлення об'єктів, прихованих рослинним покривом, в якому ЕМХ розглянутого діапазону мають гарну проникаючу здатність.

Таким чином, об’єкти наземної техніки і особовий склад є РЛО резонансних розмірів у метровому і дециметровому діапазонах довжин хвиль – діапазони робочих частот телевізійної і стільникової мереж в Україні. Тому, як свідчить детальний аналізможливостей відомих методів математичного моделювання, при моделюванні характеристик радіолокаційного розсіювання об’єктів, розміри яких порівняні із довжиною хвилі опромінення (резонансних об’єктів), рядом переваг володіють методи, засновані на розв’язанні інтегральних рівнянь (ІР).

ІР виходять з рівнянь Максвелла і граничних умов на поверхні об'єкту. ІР Стреттона-Чу, які отримані шляхом прямого інтегрування рівнянь Максвелла, дають можливість визначення розсіяного ЕМП в довільній точці простору через відомі поля всередині обсягу, займаного об'єктом, або на його поверхні. Суть методу ІР полягає в тому, що гранична задача зводиться до об'ємним або поверхневим ІР. Рішення дифракційної задачі полягає у визначенні щільності струмів на поверхні або ЕМП в обсязі розсіювача і їх подальшого інтегрування. У задачах, пов'язаних з дослідженням вторинного випромінювання РЛО довільної форми, зазвичай використовуються поверхневі ІР, які мають меншу розмірність задачі. В даний час використовуються ІР в просторово-частотному і просторово-часовому поданні. При розрахунках показників РЛО складної форми, як правило, застосовуються ІР в просторово-частотному поданні.

При вирішенні розрахункових задач стосовно об'єктів, які ідеальнопроводять, (засоби пересування для порушників, наземна техніка) резонансних розмірів, які з достатнім ступенем точності можуть бути представлені моделями, найбільше застосування знаходять ІР електричного або магнітного полів, а також ІР комбінованого поля, що представляє лінійну комбінацію ІР електричного поля і ІР магнітного поля. Стосовно до діелектричних розсіювачів (осіб-порушників) певними перевагами володіють системи ІР типу Мюллера. Найбільш ефективними методами вирішення ІР (систем ІР) є проекційні, інтерполяційні та ітераційні методи.

Важливою складовою частиною методу розрахунку характеристик РЛО складної форми є модель поверхні об'єкту. Від ступеня деталізації поверхні РЛО в значній мірі залежить точність остаточного результату.

У деяких роботах для моделювання використовуються комерційні моделі РЛО. Однак такі моделі досить дорогі і далеко не завжди доступні. У програмних продуктах ANSYS HFSS, FEKO використовуються вбудовані алгоритми створення цифрової моделі поверхні об'єкту. Складність рішення задачі розсіювання ЕМВ реальними РЛО вимагає, щоб використовувані моделі поверхонь були адаптовані до вживаного чисельному методу розрахунку.

Для рішення ІР пропонується використовуватифацетні методи, які дозволяють одержувати найбільш точний математичний опис поверхні розсіювачів складної форми. Відмінною рисою моделювання електромагнітного розсіювання, заснованого на застосуванні поверхневих ІР, є обмеження на кількість елементів дискретизації поверхні N, обумовлене можливостями сучасної комп'ютерної техніки, зокрема об'ємом пам'яті. Це пояснюється необхідністю формування і обернення матриці ядер ІР при розв'язанні СЛАР. Зокрема у випадку об’єкту, що ідеально проводить, розмірність матриці ядер становить $4N^2$ при розв'язанні СЛАР, а при розв'язанні перевизначеної системи $(2(N+N_1)x2N$. Розроблені методи створення моделей поверхонь резонансних об’єктів складної форми, адаптовані до створених у роботі методів розв'язання ІР. Запропоновані методи створення моделі поверхні дозволяють одержувати стійкі результати розрахунків характеристик розсіювання резонансних об'єктів складної форми при меншому числі елементарних ділянок N поверхні розсіювача, ніж інші методи. Пропонований метод ґрунтується на параметризації поверхні об'єкта ділянками у загальному випадку тривісних еліпсоїдів. Зокрема поверхня циліндра може бути поданою ділянками трьох еліпсоїдів, усічених у площині, перпендикуля-

рній осі циліндра. При параметризації поверхні об’єкту складної форми вибір частин еліпсоїдів задача більш складна.

УДК 621.396

Думетраш В. О., Бондаренко О. Є., Сергієнко А. В., Мусієнко В. А.

НАПРЯМОК РОЗВИТКУ СИСТЕМ ЗВ’ЯЗКУ НАТО

В останні роки США ведуть інтенсивні розробки по створенню єдиної багатофункціональної інформаційно-управляючої системи, яка інтегрує функції управління військами, зброєю, розвідкою, радіоелектронною боротьбою, а також зв’язку, навігації, орієнтування й впізнання (C^4ISR). Ця система реалізується фінансуванням програми створення інформаційної мережі поля бою (WIN-T). Її метою є зменшення бойового і чисельного складу підрозділів з одночасним зростанням її бойової ефективності за рахунок підвищення мобільності, досягнення абсолютної переваги над противником в інформаційному забезпеченні і розвідувальних можливостях.

Військове керівництво НАТО в якості одного з основних напрямків своєї діяльності, щодо підвищення бойових можливостей об’єднаних збройних сил і підготовці їх до спільних операцій визначило концепцію ведення військових дій в єдиному інформаційному просторі або з використанням об’єднаних інформаційно-керуючих мереж – концепція “мережецентричних військових дій” або “мережецентричної війни” NCW (Net work Centric Warfare).

З метою забезпечення реалізації концепції ведення бойових дій в єдиному інформаційному просторі, для спільного використання й обміну інформаційними ресурсами між усіма видами збройних сил США на всій території ведення бойових дій у будь-який час військове керівництво США та країн НАТО проводить активні роботи зі створення глобальної інформаційної мережі GIG (Global Information Generation). Розгортання мережі GIG дозволить здійснити інтеграцію засобів спостереження, розвідки, зв’язку, управління бойових засобів на всіх рівнях за допомогою обміну різними видами інформації (мовні та факсимільні повідомлення, відеозображення, електронна пошта та ін.).

Важливою умовою побудови глобальної мережі GIG є впровадження відкритої архітектури системи зв’язку ТСА (Transformational Communications Architecture) об’єднаних оперативних формувань ЗС США, які будуть трансформуватися в залежності від обстановки та завдань. З цією метою здійснюється перехід від різнотипних незалежно функціонуючих підсистем до інтегрованих систем зв’язку та передачі даних як сукупності уніфікованих багатофункціональних широкодіапазонних радіостанцій і комутаційних пристроїв, які апаратно й функціонально сполучені, об’єднані єдиною системою управління потоків різнотипної інформації.

Загальні тенденції впровадження концепції інтегрованих систем зв’язку та передачі даних полягають в наступному:

- заміна різнорідних спеціалізованих засобів зв’язку на уніфіковані радіостанції широкого частотного діапазону з багатьма функціями та комутаційні пристрої, які апаратно й функціонально поєднано, що забезпечують програмне управління радіостанціями, формування сигналів із потрібними параметрами (діапазон робочих частот, вид та форма сигналу, вихідна потужність) й реалізацію протоколів обміну даними між різнотипними мережами та засобами зв’язку без додаткового сполучення;
- використання багатократного дублювання й резервування каналів та вузлів зв’язку, адаптивної маршрутизації пакетів, супутникового зв’язку, широкодіапазонних радіостанцій, повітряних ретрансляторів;

- застосування завадостійких режимів роботи, які поєднують переналаштування робочих частот із використанням широкосмугових сигналів, адаптивне управління параметрами передавача, використання завадостійких кодів із високою здатністю виправляти помилки;
- забезпечення одночасного обміну всіма видами інформації (мовні повідомлення, дані, графічні та відео зображення), в тому числі таємною, в реальному масштабі часу одними й тими ж самими каналами зв'язку;
- побудова мобільних мереж радіозв'язку в тактичній ланці на основі принципів самоорганізації (MANET) із можливістю роботи будь-якої радіостанції мережі ретранслятором, яка дозволяє адаптуватися до умов навантаження й завадової ситуації;
- використання готових комерційних апаратно-програмних засобів, стандартів і протоколів зв'язку, які сертифіковані в ЗС США. Реалізація вказаних завдань здійснюється в рамках програм створення сімейства нових універсальних засобів зв'язку для тактичної ланки "Об'єднана система тактичного радіозв'язку". (Join Tactical Radio System – JTRS) під час розробки перспективної автоматизованої системи зв'язку "Тактична інформаційна мережа учасника бойових дій" (WIN-T).

Концепція американської програми JTRS використовувалася з метою розробки аналогічних європейських програм: ESSOR2 (European Secure Software Defi ned Radio). Європейське оборонне агентство реалізує проект програмованих радіостанцій ESSOR, в якому беруть участь Іспанія, Італія, Польща, Фінляндія, Франція й Швеція. Зокрема, компанією SELEX Communications (Італія) створено серію універсальних радіостанцій,які сумісні з радіостанціями, що розробляються за програмою JTRS згідно роботи. З аналогічними можливостями компанією Thales (Франція) розроблено серію радіостанцій ElexNet, як це зазначено в роботі. За німецькою національною програмою, яку створено компанією Ronde & Schwarz, серію радіостанцій SVFuA призначено для бундесвера Німеччини.

Найважливішою особливістю мереж радіозв'язку перспективних розвідувально-сигнальних систем США та країн НАТО є можливість об'єднання датчиків у само організовані мережі на основі використання перспективних радіостанцій серії JTRS (Joint Tactical Radio System – військова радіосистема зв'язку) в умовах прямої видимості або за допомогою супутникового зв'язку в разі її відсутності.

З метою реалізації такої можливості необхідна управляюча структура, яка забезпечить динамічний перерозподіл частотних каналів і режимів роботи радіостанцій з урахуванням умов сигнально-завадової обстановки. З метою опису радіосистем, що мають вказані властивості, використовується термін "система когнітивного радіозв'язку", під яким розуміється інтелектуальна система зв'язку, яка здатна аналізувати завадово-сигнальну інформацію й адаптуватися до неї, реагуючи на зміни в ефірі в реальному часі зміною своїх власних параметрів (діапазону частот, виду й форми сигналу, вихідної потужності) із метою збільшення ефективності використання спектрального ресурсу.

Основними тенденціями розвитку систем військового зв'язку у провідних країнах світу є: інтеграція всіх видів трафіка (мова, дані, відео, відеоконференція); повна мобільність всіх абонентів і елементів мережі; забезпечення заданої якості обслуговування користувачів (QoS) на значних географічних територіях в умовах застосування як звичайної, так і ядерної, біологічної та хімічної зброї; гарантована засекреченість усіх видів інформації; мінімальна участь людини в питаннях планування й ведення зв'язку.

УДК 351.741+004

Коршенко В. А., Пашнєв Д. В.

ВИКОРИСТАННЯ СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ У ПІДГОТОВЦІ КАДРІВ ДЛЯ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ УКРАЇНИ

Одним із пріоритетних напрямків вдосконалення підготовки кадрів для сил охорони правопорядку України залишається впровадження в освітній процес новітніх досягнень інформаційних і телекомунікаційних технологій та інформатизація процесів навчання.

Дистанційне навчання це навчальний процес, при якому всі, або більша частина навчальних процедур здійснюється з використанням сучасних інформаційних і телекомунікаційних технологій через територіальну роз'єднаність викладача і слухачів.

До початку пандемії короновірусної інфекції дистанційне навчання поступово впроваджувалось в навчальні процеси закладів вищої освіти України, переважно у вигляді вебінарів та відео-лекцій, які мали монологічну форму спілкування з аудиторією. Однак епідеміологічна ситуація 2020 року досить серйозно вплинула на систему освіти в Україні та внесла різкі і неминучі корективи. Зважаючи на високі ризики поширення короновірусу, заклади вищої освіти були вимушені екстрено здійснити повний перехід на дистанційну форму навчання.

При дистанційному навчанні викладач і слухач територіально відокремлені один від одного, що вносить суттєві відмінності в навчальні процеси в порівнянні з класичним очним навчанням. Однак за допомогою особливих прийомів побудови навчального курсу використовуючи можливості інформаційних і телекомунікаційних технологій можливо максимально налагодити процес взаємодії викладача із слухачами.

В першу чергу, дистанційне навчання повинно бути побудоване на певній платформі, тобто електронній системі дистанційного навчання. Однією з таких платформ є система дистанційного навчання Moodle, яка вже декілька років успішно використовується в процесі навчання в Харківському національному університеті внутрішніх справ, в процесі відбору нових кадрів в Національну поліцію України, в процесі переатестації співробітників Національної поліції України, та в багатьох інших сферах. Головними перевагами використання системи дистанційного навчання Moodle є те, що вона безкоштовна (розповсюджується за принципом Open Source) та WEB орієнтована, тобто дозволяє здійснювати доступ до системи з різних платформ та операційних систем, включаючи мобільні комунікаційні пристрої такі як планшети та смартфони, що значно розширює можливості її використання. Однак в ній застосовується асинхронний вид онлайн-навчання, що виключає прямий контакт учня з викладачем. Для повноцінного дистанційного навчання цього замало. Потрібно використовувати весь арсенал інструментарію онлайн-освіти, який дуже різноманітний: електронна пошта, відкриті онлайн-курси, освітні платформи широкого профілю, навчальні мобільні додатки, моделювання ситуацій у форматі комп'ютерної гри, програми групового зв'язку та відеоконференції (Skype, Zoom, тощо), віртуальні клас-руми з викладачами та багато іншого. Головне завдання - зрозуміти як правильно комбінувати формати і інструменти, синхронні та асинхронні види онлайн-навчання щоб домогтися найкращого результату. Зважаючи на те, що при підготовці кадрів для сил охорони правопорядку викладаються дисципліни, викладання яких є неможливим або недоцільним в дистанційному форматі (наприклад дисципліни з обмеженим доступом), актуальним питанням є поєднання контактно-аудиторної освіти та дистанційного навчання в так звану гібридну модель навчання, тобто поєднання мережевих онлайн технологій з очними заняттями.

Отже, навіть в умовах дистанціювання можливо побудувати максимально практи-

чну і ефективну взаємодію викладача із слухачами. Комп'ютерні, інформаційні та телекомунікаційні технології дозволяють вивести процес підготовки кадрів для сил охорони правопорядку України на якісно новий рівень, розкривають додаткові можливості навчання та сприяють підвищенню якості та доступності професійної освіти, перепідготовки та підвищення кваліфікації сил охорони правопорядку України.

УДК 004.01

Алфімова Л. Д., Душкін В. Д., Мельник В. М.

ВИКОРИСТАННЯ ВЕБСЕРВІСУ GOOGLE CLASSROOM ПРИ ВИВЧЕННІ ТЕМИ "ЛІНІЙНА АЛГЕБРА"

Опитування курсантів, яке було проведено, довело, що в якості джерела необхідної інформації прагнуть використовувати інтернет та системи дистанційного навчання ніж традиційні "товсті підручники" та власні конспекти. Цьому також сприяє особливість навчання в військовому навчальному закладі: відірваність від бібліотеки під час знаходження в учбовому центрі, пропуск занять у зв'язку зі знаходженням у наряді та хворобою. Тому для вивчення окремих модулів, зокрема модуля "Лінійна алгебра", було вирішено використовувати вебсервіс Google Клас для вільного доступу до матеріалів з відповідних розділів курсу.

До переваг вебсервіса потрібно в першу чергу віднести можливість автономної роботи з матеріалами кожного учасника учбового процесу. Це забезпечує можливість для курсантів спілкування з викладачем та звернення до учбових матеріалів. не тільки під час занять та самостійної підготовки, а у будь-який момент часу.

Google Клас дає можливість обмінюватись не тільки текстовими файлами, він дозволяє курсантам отримувати доступ до представлених презентацій, відеороликів і.т.і. У разі виникнення потреби вони можуть передивитись ці матеріали декілька разів.

У вільному доступі до модуля "лінійна алгебра" викладачами кафедри було розмішено матеріали, що стосуються кожного лекційного, практичного, та групового заняття з наведенням необхідного теоретичного матеріалу, прикладів розв'язання практичних занять. Також у відповідній папці курсу було розміщено довідкові матеріали, посібники, та скановані розділи підручнику [1], який був рекомендований у якості основної літератури.

У роботах [2] - [3] зверталась увага на необхідність створення засобів для самостійної перевірки курсантами окремих кроків виконання завдань під час самостійного опрацювання учбового матеріалу. Тому викладачі кафедри скористались можливостями вебсервісу Google Classroom для створення тестових завдань: "Матриці", "Визначники", "Мінори та алгебраїчні доповнення", "Формули Крамера".

Здобувачам освіти надавалась можливість багаторазового проходження тестів та ознайомлення з правильністю виконання окремих завдань. На думку утворювачів цих тестів вони є засобом самовдосконалення знань та умінь курсантів, але не є засобом для проведення поточного та підсумкового контролю.

Список літератури

1. Дубовик В.П., Юрик І.І. Вища математика: навчальний посібник. – К. А.С.К., 2006. – 648 с.

2. Алфімова Л.Д. Мельник В.М. Професійно орієнтоване навчання вищої математики при підготовці майбутніх офіцерів Національної академії Національної гвардії України./ Молодь і ринок , Дрогобицький державний педагогічний університет імені

Івана Франка. – 9 (176). – 2019. – С. 133-137

3. Душкін В.Д., Мельник В.М., Сидоренко І.І. Використання MS EXCEL при самостійному опрацюванні питань з лінійної алгебри / Тези міжнародної науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 14-15 березня 2018 року, м. Харків, с. 41

Приходько Ю. І.

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМИ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ

Актуалізація проблеми підготовки військових фахівців з вищою освітою на теперішній час зумовлена такими чинниками: 1) викликами, що постали перед державою, Збройними Силами (далі – ЗС) України у зв'язку із проведення операції Об'єднаних сил, іншими докорінними змінами у зовнішньому та внутрішньому безпековому середовищі держави, визначеними Законом України "Про національну безпеку", Державною програмою розвитку ЗС України на період до 2020 року, Стратегічним оборонним бюлетенем [1-3]; 2) потребою подальшого розвитку основних складових сектору безпеки і оборони, сумісними з певними структурами країн-членів НАТО; 3) необхідністю використання та запровадження в освітній процес досвіду військових навчальних закладів провідних країн-членів НАТО з підготовки офіцерських кадрів; 4) недостатнім рівнем якості підготовки офіцерських кадрів з вищою освітою для ЗС України. Система військової освіти має оперативно реагувати на викладені чинники.

Основними завданнями розвитку військової освіти мають стати:

- створення організаційно-правових, фінансово-економічних і матеріально-технічних умов для задоволення потреб ЗС України у компетентних військових фахівцях з урахуванням європейських освітніх стандартів та особливостей розвитку основних складових сектору безпеки і оборони України щодо їх сумісності зі структурами країн-членів НАТО;
- удосконалення системи допризовної підготовки молоді, її військово-професійної орієнтації, національно-патріотичного виховання та відбору кандидатів на навчання у вищі військові навчальні заклади та військово-навчальні підрозділи закладів вищої освіти (далі – ВВНЗ);
- оптимізація всіх складових системи військової освіти (мережа ВВНЗ; рівні та ступені (кваліфікації) освіти; галузі знань, напрями, спеціальності і спеціалізації; освітні та наукові програми; стандарти освітньої діяльності та стандарти освіти; учасники освітнього процесу; органи, що здійснюють управління у сфері військової освіти);
- забезпечення якості військової освіти та освітньої діяльності у ВВНЗ;
- інформатизація освітньої діяльності, приведення змісту та технологій підготовки військових фахівців у відповідність із сучасними вимогами до подальшого розвитку ЗС України з пріоритетами військово-професійної спрямованості та національно-патріотичного виховання;
- провадження наукової, інноваційної діяльності шляхом активізації наукових досліджень, здійснення підготовки наукових кадрів вищої кваліфікації і використання отриманих результатів в освітньому процесі, забезпечення органічного поєднання в освітньому процесі ВВНЗ освітньої, наукової, науково-технічної та інноваційної діяльності;
- активізація міжнародного співробітництва в сфері військової освіти з провідними країнами світу та відповідними структурами країн-членів НАТО.

Система військової освіти має забезпечувати підготовку військових фахівців, здатних на високому професійному рівні вирішувати бойові та оперативні завдання в умовах мирного і воєнного часу, успішно співпрацювати зі штабами багатонаціональних сил НАТО, а саме:

- спроможних з високою ефективністю виконувати нормативно-правові акти держави, директиви та накази щодо безпеки та оборони Вітчизни, захисту її територіальної цілісності, національних інтересів, управління військами (силами) в бою (операції);
- експлуатувати та застосовувати найскладніші системи озброєння та військової техніки;
- навчати й виховувати підлеглий особовий склад на засадах національного патріотизму, відданості Батьківщині, психологічної стійкості, формувати стійкий морально-психологічний клімат у підрозділах і частинах;
- спроможних розвивати власну наукову, творчу, лідерську індивідуальність, наполегливо здобувати та засвоювати нові знання протягом військової служби;
- ефективно діяти у міжнародних операціях з підтримання миру та безпеки під егідою ООН, гідно виконуючи покладені на них міжнародним співтовариством обов'язки.

Трансформаційні процеси в системі підготовки військових фахівців мають базуватися на таких принципах:

- відповідності нормативно-правової бази військової освіти державним освітнім стандартам та особливостям розвитку основних складових сектору безпеки і оборони України щодо їх сумісності зі структурами країн-членів НАТО;
- інтеграції військової освіти у загальнодержавну систему освіти;
- інтеграції системи військової освіти України в Європейській військово-освітній простір за умови збереження та розвитку досягнень і прогресивних здобутків національної військової школи, органічного зв'язку військової освіти зі світовою та національною історією, культурою, традиціями;
- доступності та конкурентності здобуття військової освіти;
- пріоритетності військово-професійної спрямованості та національно-патріотичного виховання військових фахівців в освітній діяльності ВВНЗ;
- ступеневості системи підготовки військових фахівців, неперервності освіти та самоосвіти протягом усієї служби;
- випереджального характеру підготовки військових фахівців відносно потреб розвитку ЗС України;
- забезпечення інтеграції освітнього процесу з науковою, науково-технічною та інноваційною діяльністю, розвитку наукових шкіл;
- гуманізації та гуманітаризації військової освіти, пріоритетності загальнолюдських цінностей;
- незалежності здобуття військової освіти від впливу політичних партій, громадських та релігійних організацій;
- органічного зв'язку функціонування ВВНЗ з діяльністю військ (сил);
- відповідальності ВВНЗ за якість підготовки військових фахівців щодо забезпечення їхньої здатності та готовності ефективно виконувати службово-бойові функції у військах (силах) в умовах мирного та воєнного часу на посадах за призначенням.

Рушійними механізмами подальшого розвитку системи підготовки військових фахівців є такі: а) застосування теорії та методології трансформації систем [4]; б) реалізація суперечностей, що мають місце в системі військової світи; в) інноваційна діяльність; г) моніторинг військової освіти на всіх ієрархічних рівнях управління.

Список літератури

1. Про національну безпеку України : Закон України № 2469-VIII від 21 червня

2018 р. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19.

2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Державну програму розвитку Збройних Сил України на період до 2020 року" : Указ Президента України № 73/2017 від 22 березня 2017 р. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/73/2017#n2.

3. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України" : Указ Президента України № 240/2016 від 6 червня 2016 р. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/240/2016#n251.

4. Приходько Ю. І. Трансформація систем: основи теорії та методології // Науковий журнал Національного університету оборони України "Сучасні інформаційні технології у сфері безпеки та оборони". – 2019. – 1(34). – С. 5–12.

УДК 621.396

Баранник В. В., Краснорyцький А. О., Шульгін С. С., Олексін О. О.

АЛГОРИТМ ВИЯВЛЕННЯ СЕГМЕНТІВ ЗОБРАЖЕННЯ З РІЗНОЮ ИНФОРМАТИВНІСТЮ НА ОСНОВІ ТЕХНОЛОГІЇ ДВУХКАСКАДНОЇ ІДЕНТИФИКАЦІЇ

Для оперативного забезпечення системи управління візуальною інформацією існує цільовий відеосервіс зі зростаючою тенденцією впровадження інформаційно-технічних бортових комплексів відео і фотореєстрації на платформі безпілотних літальних апаратів (БПЛА). Ключовим сегментом ефективності інформаційного забезпечення тут є час доставки інформації у вигляді аерофотознімків. Базовим сектором такого процесу є показники якості з позиції достовірності інформації і роздільної здатності отриманого аерофотознімка. Однак бортова обробка, яка має на меті адаптацію відеопотоку до існуючих бортових каналів передачі відеоінформації, не дозволяє виконати доставку оперативної інформації, що веде до зниження ефективності роботи всієї системи управління. Так, існуюча бортова обробка, для скорочення часу доставки відеоінформації, застосовує інформаційні технології з платформою JPEG. Такі технології зменшують інформаційну інтенсивність за рахунок спотворення і руйнування інформації про ключові ознаки дешифрування, що веде до зниження вірогідності отриманих аерофотознімків.

Обґрунтовується шляхи вирішення проблематики дисбалансу між достовірністю отриманого аерофотознімка і оперативністю його доставки.

Концептуальним аспектом рішення проблематики надання аерофотознімків з використанням бортових комплексів моніторингу є запропонована інформаційна технологія доставки дешифровочної інформації.

Ґрунтується така технологія на ідеї дешифровочного кодування сегментів аерофотознімків з урахуванням ступеню їх семантичної інформативності в умовах зменшення інформаційної інтенсивності бітового потоку.

Пропонована методологія базується на технології дешифровочне кодування, в основі якої поставлена ідея інтелектуальної обробки аерофотознімків з виділенням ключових ознак дешифрування.

Унікальність представленої технологія полягає в прагненні максимального виявлення та збереження ключової інформації семантичного змісту окремих сегментів аерофотознімка в інтересах дешифрування.

Кільдеров Д. Е., Пригодій М. А.

ІНФОРМАТИЗАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ В СИСТЕМІ ПЕДАГОГІЧНОЇ ОСВІТИ

Домінуючою тенденцією подальшого розвитку сучасної цивілізації, є перехід від індустріального до інформаційного суспільства, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному та особистому розвиткові.

Інформатизація – це сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб, реалізації прав громадян і суспільства на основі створення, розвитку, використання інформаційних систем, мереж, ресурсів та інформаційних технологій, побудованих на основі застосування сучасної обчислювальної та комунікаційної техніки [1]. Головною метою Національної програми інформатизації [2] є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави.

Інформатизація вищої освіти є однією із найважливіших умов успішного, сталого розвитку суспільства, оскільки саме в сфері освіти готуються та виховуються фахівці, котрі не тільки формують інформаційне середовище, але й яким також належить самим жити й працювати у цьому новому середовищі. Як визначено "Стратегією розвитку вищої освіти в Україні на 2021-2031 роки" – "місією вищої освіти є забезпечення сталого інноваційного розвитку України через підготовку висококваліфікованих фахівців, створення та поширення знань, формування інтелектуального, соціального та духовного капіталу суспільства, готового до викликів майбутнього [3].

Водночас, у системі вищої освіти існує низка проблем, які разом із суттєвими зовнішніми та внутрішніми викликами створюють ризики та негативно впливають на можливості її розвитку, зокрема, – цифровізація освіти [3]. На нашу думку, основними проблемами інформатизації національної системи освіти, окрім недостатнього фінансування, недосконалої матеріально-технічної бази, є наукові та організаційно-управлінські засади освітнього процесу, підготовка навчально-методичних комплексів, програмних продуктів і навчальних засобів нового покоління, застосування інноваційних технологій, формування принципово нової культури праці педагогічних, науково-педагогічних працівників, навчально-пізнавальної діяльності студентів.

Проникнення в освіту нових інформаційних технологій потребує розглядати підготовку фахівців в системі педагогічної освіти як процес інформаційний, що зумовлюється такими чинниками: комп'ютеризацією та автоматизацією всіх складових політичної, соціально-економічної, наукової, освітньої і гуманітарної сфер діяльності; зміною поглядів на управлінські процеси в різних предметних галузях; конструюванням та побудовою інфраструктурних об'єктів, різноманітного промислового обладнання, особливостями їх функціонування та експлуатації; необхідністю системного формування змісту освіти та компетенцій фахівців; 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 тощо.

Інформатизація освітнього процесу в системі педагогічної освіти являє собою систему та процес забезпечення всіх складових освітнього процесу теорією, методоло-

гією, технологією щодо створення та оптимального використання психолого-педагогічних, навчально-методичних, програмно-технологічних, матеріально-технічних продуктів, орієнтованих на реалізацію засобами існуючих інформаційно-комунікаційних технологій. До засобів інформаційно-комунікаційних технологій відносяться: 1) програмні, програмно-апаратні та різноманітні технічні пристрої і комплекси на базі мікропроцесорної, обчислювальної техніки (навчальні середовища, моделі, роботи, структури на основі штучного інтелекту тощо); 2) сучасні засоби і системи з функціями збору, накопичення, зберігання, обробки, передачі інформації, доступу до інформаційних ресурсів локальних і глобальних мереж. Дидактика інформатизації освітнього процесу в контексті викладеного вище по суті є інноваційно-інформаційною технологією з такими складовими: проектувальна: комунікативно-процесуальна; контрольно-діагностична; коригувальна; моніторингова.

Серед загальних тенденцій, що простежуються у процесі інформатизації освіти, можна виділити такі: використання національних і світових інформаційних освітніх ресурсів; виникнення нових форм підготовки та перепідготовки фахівців; поява інноваційних засобів навчання; використання засобів 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 освітньо-управлінської діяльності.

До основних напрямів діяльності з інформатизації освітнього процесу в ситемі педагогічної освіти можна віднести такі: розроблення інструктивних, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних передумов процесу інформатизації підготовки фахівців; створення бази інформаційних ресурсів; розвиток локальних та глобальних мереж інформаційного забезпечення освітнього процесу; підвищення якості підготовки фахівців на основі широкого використання інформаційно-комунікаційних і особистісно орієнтованих технологій; продукування та запровадження інноваційно-інформаційних продуктів і послуг; інтеграція педагогічної освіти в національний і світовий інформаційний простір; ефективне запровадження системи моніторингу освітнього процесу.

В процесі інформатизаії підготовки фахівців в системі педагогічної освіти мають здійснюватися такі управлінські функції: інформатизація всіх сфер діяльності з підготовки фахівців; захист авторських прав, 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 забезпечення системи інформатизації підготовки фахівців.

Пріоритетні завдання інформатизації педагогічної освіти: забезпечення розвитку особистості майбутнього фахівця, розкриття його творчого потенціалу; формування інформаційної культури, спрямованості на навчання протягом життя, професійної діяльності; удосконалення управління освітою; створення інформаційних мереж і баз даних; модернізація матеріально-технічної бази; інтенсифікація науково-технічних, психолого-педагогічних і науково-методичних досліджень; запровадження нових форм навчання, підготовки, перепідготовки та підвищення кваліфікації педагогічних, науково-педагогічних працівників.

Список літератури

1. Закон України “Про Концепцію Національної програми інформатизації” від 4 лютого 1998 року N 75/98-ВР (Із змінами, внесеними згідно із відповідними Законами України (2006-2020 рр.). Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/Z980075.html.
2. Закон України “Про Національну програму інформатизації” від 4 лютого 1998 року № 74/98-ВР (Із змінами, внесеними згідно із відповідними Законами України (2001-2020 рр.). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text.
3. Стратегія розвитку вищої освіти в Україні на 2021-2031 роки. [Електронний ресурс]. – Режим доступу: http://www.reform.org.ua/proj_edu_strategy_2021-2031.pdf.

УДК 621.39

Сальніков О. М., Воронін О. І.

МОЖЛИВОСТІ ВИКОРИСТАННЯ ЗАГАЛЬНОДОСТУПНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ НГУ

Функціонуванні будь-якої силової структури держави залежить від системі її управління. Ефективність функціонування систем управління залежить від якісних показників інформаційного обміну, як в середині так і зовні цих систем управління. Однією з основних показників якості інформаційного обміну це здатність зберігати в таємниці зміст інформації, яка циркулює в системі управління.

На сьогоднішній день існує велика кількість програмних засобів захисту інформації за допомогою систем шифрування. Вони відрізняються методами та алгоритмами шифрування та розшифрування, складністю використання, надійністю, тощо. Враховуючи потужність сучасних комп’ютерів та ступінь розвитку криптографічних методів, майже будь-який шифр рано чи пізно може бути зламаний. Тому основною метою шифрування є збільшення часу, потрібного для дешифрування, до значення, коли зашифрована інформація перестає бути актуальною. Отже з таких програмних засобів і слід вибирати потрібний. На сьогоднішній день існує велика кількість подібних програм. Найбільш розповсюдженими с них є: Folder Lock; PGP Desktop; Cebersafe Top Secret; DriveCripy; Files Cipher та інші.

Метою доповіді є обґрунтування можливості зберігання в таємності змісту інформації, яка передається між структурними підрозділами у повсякденній діяльності по загальнодоступних каналах передачі даних за рахунок використання відкритих програмних засобів шифрування повідомлень мережі Інтернет.

У Національній академії Національної гвардії України на протязі останніх шести років розробляється та удосконалюється методика створення та експлуатації системи захищеного скритого обміну даними між структурними підрозділами с використанням загальнодоступних кагалів передачі даних та відкритого програмного забезпечення. З метою коректного використання в рамках програму PGP розроблена інструкція з встановлення та налаштування програмного комплексу для здійснення цього обміну даними .

Для підвищення скритності системи управління будь-якого військового чи правоохоронного формування доцільно використовувати у повсякденній діяльності не спеціальні засоби обміну інформацією, а загальнодоступні канали передачі даних і безкоштовні загальнодоступні програмні засоби захисту інформаційного обміну при

використанні загальнодоступних інформаційних систем для потреб силових структур України а саме існуючі програми шифрування даних.

На сучасному етапі розвитку інформаційних технологій майже будь-який шифр може бути дешифрований, але для цього потрібен деякий час. Основна вимога до програм шифрування даних – час потрібний на дешифрування має перевищувати час, коли інформація ще не втратила своєї актуальності. Ця вимога цілком задовольняється програмами, які створені на базі метода PGP і вони можуть використовуватися для захисту інформаційного обміну при використанні загальнодоступних інформаційних систем для потреб силових структур України.

Програма PGP досить доступна, проста у використанні і не потребує значних апаратних ресурсів. Для її використанні достатньо встановити її на комп'ютерах підрозділів які обмінюються даними. Ніяких додаткових витрат матеріальних чи людських ресурсів (спеціально підготовлений персонал) не потрібно, тому такий спосіб захисту інформаційного обміну при використанні загальнодоступних інформаційних систем для потреб силових структур України забезпечує скритність обміну даними у повсякденній діяльності і може бути реалізований у існуючій СІКТС НГУ, або будь-якої іншої силової структури України.

УДК 004.6::355

Скорик А. Б., Галицький О. Ф., Моргун Є. В., Гайбадулов Б. В., Камчатний М. І.

СИСТЕМНО-КОНЦЕПТУАЛЬНІ ОСНОВИ ТЕОРІЇ ДАТА-ЦЕНТРИЧНИХ ОПЕРАЦІЙ

Теорія дата-центричних операцій (data-centric operations, DCO) – це нове бачення поведінки бойових систем, це перенесення 4D екстенсіоналізму на операційний рівень, це метаморфізм, хмарні обчислення і сервіс орієнтована архітектура не тільки у віртуальних мережах, але і на полі бою, Дата-центричні системи-систем (data-centric system of systems, DCSoS) – це системи "метаморфи", які не мають постійного "тіла" (структури), що постійно змінюються, серце яких (командні пункти) важко виявляються і недоступні противнику, частина з них може перебувати у віртуальних структурах – хмарах. Такі бойові системи важко знищити звичайною (літальною) зброєю.

Перехід від концепції мережево-центричної війни (network-centric warfare, NCW) до концепції дата-центричної операції відображає перехід до мультирозумних систем на основі соціокультурної моделі.

В основі теорії DCO лежать концепти:

- метаморфізму – мінливості і гнучкого розвитку;
- 4D екстенціоналізму і дуалізму дата-центричних систем-систем.

Теорія DCO – припускає (основна гіпотеза), що застосування ключових факторів 6-го технологічного укладу підвищує як ефективність, так і результативність операцій за рахунок:

- переходу до парадигми мультирозумних систем на основі соціокультурної моделі;
- динамічної реконфігурації цільової системи і систем операційного оточення, залежно від зміни умов навколишнього середовища;
- розширення меж дата-центричної системи-систем шляхом реалізації децентралізованого управління поведінкою систем, що входять до її складу.

Під метаморфізмом розуміється адаптивний просторово-часовий синтез і реконфігурація структури DCSoS, що забезпечує найбільшу ефективність проведення операції в конкретних умовах.

Методологія (метод) адаптивного просторово-часового синтезу і реконфігурації структури DSoS безпосередньо пов'язана з поняттям 4D-екстенціоналізма. У рамках цього підходу розглядаються ті об'єкти, які мають місце в просторі-часі (4D-підхід по Ейнштейну). Чотиривимірний об'єкт існує в часі так само, як і у просторі. При цьому об'єкт один, але в ньому виділяються інші об'єкти – його темпоральні частини, по аналогії зі звичайними просторовими частинами.

Поточна структура DCSoS визначається необхідними на поточний часовий інтервал можливостями, DCSoSмає дуальний характер, її можна розглядати одночасно і як цільову систему і, як мережеві ресурси. Такі системи можуть змінювати свою структуру не тільки за рахунок власних ресурсів, але і за рахунок динамічного зв'язування мережевих ресурсів у рамках завдання, яке виконуються системою на даному проміжку часу.

UDK 621.396

Djus V., Reznichenko A., Chmil Yu., Skopintsev O., Zaberezhniy D.

SOFTWARE MODEL OF THE WORKPLACE OF THE OPERATOR OF RADAR MEANS OF THE ANTIAIRCRAFT MISSILE COMPLEX OF AVERAGE RANGE AT WORK ON THE SINGLE PURPOSE

The arsenal of existing modern information and training systems used in the practical training of anti-aircraft missile forces is constantly in need of updating and replenishment. To increase the level of training of such specialists, special software has been developed that simulates the jobs of medium-range anti-aircraft missile system service operators when working on air targets.

The main attention in the development of this software was paid to the visualization of the processes of radar operation when working on a single target and obtaining targets from different sources. The main options for conducting combat operations by servicing medium-range anti-aircraft missile systems for a single target have been selected. These options provide all possible elements of the service for a single purpose. Options take into account the peculiarities of combat operations in obtaining targets from various sources. The implementation of options involves the visualization of the processes of automatic and manual capture of the target for tracking, tracking the target in the presence or absence of information about the speed and range of the target. Based on the results of the analysis of the selected options for conducting work on a single target by the maintenance of anti-aircraft missile systems, the scenarios for training with the operator of radar means of medium-range anti-aircraft missile systems are determined.

The application of these scenarios in training and practical classes allows to form in cadets of senior courses of the faculty of anti-aircraft missile forces primary skills of conducting work on a single target at the appropriate workplace. The composition, purpose and procedure for the use of controls, the purpose of indications and indicators at the workplace of the guidance operator, which are used when working on a single purpose. Features of information display and target visualization on indicator scans in these conditions are considered in detail. The model of a workplace of the operator of guidance of radar means of an antiaircraft missile complex of average range at work on the single purpose is offered. A mathematical apparatus has been developed that describes the order of displaying information and marks from individual targets on the screens of guidance indicators. The structure of the model, functional purpose and the order of interaction of its elements in the visualization of combat work of the guidance operator are described. On the basis of the described model the special software for visualization of a workplace of the

operator of guidance of radar means of the antiaircraft missile complex of average range is developed. The requirements to the PC for high-quality functioning of the developed software are resulted. Features of application are shown, the context menu is described and features of realization of the special software at visualization of various modes of work of radar means on a workplace of the operator of guidance at work on the single purpose are resulted.

Methodical recommendations on the introduction of special software in the organization of the educational process at the Faculty of Anti-Aircraft Missile Forces of Ivan Kozhedub Kharkiv National Air Force University have been developed. They provide an improvement in the quality of practical training of cadets of the faculty in the study of military-special disciplines of the curriculum, namely the acquisition and improvement of skills to perform operations in the workplace. Further development of special software that implements the workplace of the radar guidance operator of the medium-range anti-aircraft missile system provides integration with the information and training complex "VIRAZH-RD" and participation in the combat operations of units in difficult air and interference conditions.

UDK 621.396

Grechka A., Kalugin D., Batkovskiy S., Muhartov A., Sikachov O.

WAYS TO IMPROVE THE EFFICIENCY OF MONITORING AND DIAGNOSING THE TECHNICAL CONDITION OF RADIO-TECHNICAL MEANS OF AIR DEFENSE SYSTEMS

Modern air defense systems are complex technical systems that consist of radio-electronic elements, structurally built in the form of modules, cells, standard replacement elements of various physical design and purpose. One of the main requirements for the radio-electronic means (REM) of anti-aircraft missile systems is their high reliability, which depends on many indicators, among which the determining ones are the mean time to failure and the mean recovery time. The restoration of the air defense system of the air defense missile system is carried out with the help of technical diagnostics (TD), which monitor the technical condition (TC) and localize the malfunction with an accuracy of electronic components. But today unified approaches to the creation of means of TD REM and the principles of obtaining diagnostic information by means of TD REM have not yet been developed.

The report discusses ways to improve the efficiency of monitoring and diagnosing the technical condition of the air defense system. The results of the analysis of recent studies and publications on improving the efficiency of monitoring the technical condition of radio-technical means (RTM) of the air defense missile system are presented. The necessity of increasing information about the reliability of the real state of the RTMand reducing the time costs is substantiated, which leads to a decrease in the cost of diagnosing technical RTMsystems. At the same time, the wrong choice of control parameters leads to an increase in non-productive costs, a decrease in the reliability of control and the effectiveness of using RTMfor its intended purpose.

To increase the efficiency of monitoring and diagnostics, it is proposed to determine the necessary ensemble of parameters for each RTM, which will increase the efficiency of monitoring and diagnosing the technical state of the air defense system.

UDK 621.396

Taran M., Shulezhko V.

APPLICATION OF THE GAME THEORY APPARATUS IN THE ALGORITHM FOR CONSTRUCTING THE OPTIMAL COMBAT ORDER OF A MIXED GROUP OF ANTI-AIRCRAFT MISSILE DIVISIONS

An important factor influencing the quality of the task of covering objects or troops (forces) is the option of building a combat order of a mixed group of anti-aircraft missile divisions. Existing methods of calculating possible options for building a combat order of a mixed group of anti-aircraft missile divisions, used by the headquarters, do not meet the current conditions of hostilities. This is due to the fact that the possibility of restoring the combat capability of anti-aircraft missile divisions with the optimal equipment of spare parts, the possibility of providing radio communications and noise protection are not taken into account. Thus, there is a need to develop new methods of building the combat order of a group of anti-aircraft missile divisions using modern software and information technology. To this end, the main indicators and criteria for assessing the effectiveness of combat operations of a group of anti-aircraft missile divisions were determined. Based on them, an algorithm for constructing a combat order of a mixed group of anti-aircraft missile divisions using game theory was developed, which provides a solution to the antagonistic mathematical game of two players (group of anti-aircraft missile divisions (side A) and a group of air attack means (side B)) for party A, the application of the most probable strategy, which will correspond to a reasonable result in the conflict with party B, taking into account its behavioral uncertainty of action strategies.

UDK 621.396

Herasimov S., Kukobko S., Roshchupkin E., Roshchupkina A.

THE STROBES SIZES JUSTIFICATION DURING IDENTIFYING INFORMATION IN A MULTI-POSITION SURVEY RADARS SYSTEM

Combining information from single system separate sources is a promising direction for accuracy and information content improving. There are a number of works devoted to this area. At the same time, there are cases when information from survey radars, each of which does not continuously track an air target, is subject to consolidation. In this case, information consolidation is possible at the level of combining traces or at the level of combining single measurements, the algorithms of which are discussed in sufficient detail in the relevant literature.

This raises the problem of identifying information received by individual sources of the system. In most works for identification, certain features (polarization, scattering, spatial, high-speed, etc.) are used, which make it possible to separate targets from each other in the corresponding strobe. In this case, the size of the strobe is selected based on the estimates of the primary coordinates measurement errors (range, elevation, azimuth and radial velocity) and the characteristics of the target movement.

However, in practice, there are additionally errors in topographic reference, orientation, leveling and time synchronization of the survey radars included in the system. The influence of the ensemble of the given errors on the characteristics of the system, and in particular, on the strobe size when identifying targets, was not given in the literature known by authors.

The report contains relations characterizing the influence of the above errors on the accuracy characteristics of the system. It is shown that in some cases (a system of highly mobile survey radars, for example), the influence of the corresponding errors can be very significant, and leads to the need to increase the identification strobe size by several times. The algorithm for "adaptive" changes in identification strobes, which allows one to estimate and take into account the errors of topographic location, orientation, leveling and time synchronization, based on the results of previous measurements by the system at the same positions, is presented.

UDK 621.396

Kriuchkov D., Pavlenko M., Pluzhnik O., Kovalenko V., Kuzmenko D.

PREDICTION OF THE TECHNICAL STATE OF RADIO EQUIPMENT USING THE APPROXIMATION OF CHANGES IN THEIR PARAMETERS BY ORTHOGONAL CHEBYSHEV POLYNOMIALS

The quality of military equipment is realized when used for its intended purpose, it is maintained and restored through maintenance and repairs. The beginning of the operation of a military equipment item is the moment when it enters the operational unit, and the end is the moment when the decision on the impossibility or otherwise of further exploitation of the item is documented. The calendar duration of this step is the complete service life of the product. It is not possible to carry out the necessary calculations in a timely manner without knowledge of the technical condition of the funds. This leads to the search for new methods for reliable and efficient forecasting and the establishment of appropriate forecasting systems.

In the general case, the forecasting system should provide storage, processing and delivery of large amounts of information in a dialogue mode with the user. The obtained results of measurements of the values of each of the parameters (diagnostic standards) are stored in the database. The processes of changing the predicted parameters in the forecasting system are modeled using the module for generating models, which provides the necessary data for extrapolating the processes of the consumption of parametric redundancy in the approximation module.

The report proposes to choose an approximating polynomial in the form of Chebyshev orthogonal polynomials for unequally spaced points, which is associated with an arbitrary time for obtaining estimates of diagnostic standards for diagnostic parameters. The Chebyshev polynomial of degree n is the one that deviates least from the "zero" of the given function values than any other field of the same degree.

УДК 004.6::355

Скорик А. Б., Гайбадулов Б. В., Сургай М. В., Титаренко Р. В., Борисов В. В.

МЕТОД РОЗРОБКИ АРХІТЕКТУРИ ДАТА-ЦЕНТРИЧНОЇ ЕКОСИСТЕМИ ОВТ

В процесі життєвого циклу (ЖЦ) відбувається послідовна зміна стану систем ОВТ. Ці зміни відбуваються в рамках відповідних практик (процесів): визначення вимог до системи ОВТ, розробки, створення дослідних зразків, серійного виробництва, експлуатації і утилізації. Всі ці практики здійснюються системами забезпечення:

конструкторськими бюро, виробничими підприємствами, військовими частинами.

Індустріально розвиненими країнами і ключовими учасниками міжнародного ринку в теперішній час формується нова культура створення і застосування складних систем-систем, заснована на засадах соціокультурних моделей побудови організацій і мультирозумних систем.

Перехід до соціокультурних моделей побудови організацій передбачає кардинальну зміну структурної організації і поведінки систем забезпечення. Між ними складаються відносини, що дозволяють казати не про окремі системи забезпечення, а про єдину систему-систем підтримки ЖЦ ОВТ. Така система у впродовж свого власного життєвого циклу змінює цілі функціонування, структуру у часі і просторі. Раніше, такий підхід був пов'язаний з побудовою мономіст, що створюються для вирішення якоїсь великої науково-промислової проблеми. Надалі, коли актуальність даної проблеми падала, багато з таких мономіст приходили в занепад, що викликало значні соціальні проблеми. Однак досвід формування навколо цільової системи розвиненої сервісної інфраструктури є дуже важливим. І на сьогоднішній момент цей досвід відроджується, але тільки на новому науковому і організаційному рівні – створенні штучних екосистем. Створення екосистеми ОВТ на базі використання сучасних інформаційних технологій дозволить досягти більшого ступеня інтеграції систем підтримки ЖЦ, однак не зажадає великих витрат на інфраструктуру і соціальну сферу, що було необхідно в рамках створення мономіст.

В доповіді розглядається модель архітектури системи інтеграції і розвитку можливостей по створенню екосистеми ЗРС і обґрунтовується загальна структура методу створення архітектури екосистеми ЗРС. В рамках якої передбачається зміна об'єкту управління. Існуюча системно-концептуальна модель управління життєвим циклом зразка ОВТ передбачає, що об'єктом управління є життєвий цикл зразка ОВТ і сам зразок ОВТ (його компонентний склад). З огляду на, що в рамках сучасного уявлення про життєвий цикл ЗРС окремі стадії ЖЦ можуть за часом накладатися одна на одну, це призводить до паралельного існування різних систем забезпечення ЖЦ ЗРС. Архітектура екосистеми ЗРС, а не сам зразок ОВТ та його життєвий цикл, починають виступати у якості об'єкту керування.

Формування архітектури екосистеми ЗРС має здійснюватися на базі процесного представлення ЖЦ. Перехід до процесів (практик) - це перехід до обговорення в першу чергу функціонального аспекту робіт і тільки потім до їх виконавців. Життєвий цикл представляється як послідовність виконання стандартизованих практик.

УДК 623.462.22

Помогаєв І. В., Таршин В. А., Скорик А. Б., Коробков Ю. В., Губін С. Д.

УДОСКОНАЛЕННЯ СПОСОБУ НАПІВАКТИВНОГО САМОНАВЕДЕННЯ ЗЕНІТНИХ КЕРОВАНИХ РАКЕТ ЗА РАХУНОК ВИМІРЮВАННЯ ДАЛЬНОСТІ РАКЕТА-ЦІЛЬ

Необхідність удосконалення зенітних ракетних комплексів (ЗРК), як складової системи протиповітряної оборони країни обумовлена зміщенням акцентів розробки та застосування засобів повітряного нападу (ЗПН) у останніх війнах та збройних конфліктах у бік високоточних керованих засобів ураження (КЗУ). Широке застосування малорозмірних, малопомітних, маловисотних КЗУ обумовлює необхідність виконання наукових робіт щодо підвищення ефективності існуючих та розробки нових сучасних ЗРК. Вимога підвищення автономності систем управління, реалізація принципу “вистрілив - забув” визначило широке застосування активних головок са-

монаведення (ГСН) зенітних керованих ракет (ЗКР). Втілення цифрової обробки сигналів у сучасних радіолокаційних головках самонаведення (РГС) забезпечило обробку сигналів близьку до оптимальної. Відповідно до цього, подальший розвиток способів наведення ЗКР пов'язують із застосуванням комплектованих ГСН, які забезпечують напівактивно-активне самонаведення. Обґрунтовуються можливості удосконалення способу напівактивного ЗКР за рахунок вимірювання дальності ракета-ціль по відбитому від цілі частотно-модульованому сигналу(ЧМ). Запропонований спосіб ґрунтується на використанні додаткової інформації про просторове положення цілі та ракети під час самонаведення на повітряну ціль. Як додаткова інформація розглядається відстань між ЗКР та повітряною ціллю у процесі напівактивного самонаведення. Реалізація запропонованого способу передбачає застосування у процесі наведення ЗКР комбінації монохроматичних (МХ) та ЧМ сигналів підсвічування. На користь запропонованого способу напівактивного самонаведення свідчать наведені результати оцінки середньоквадратичних похибок вимірювання дальності ракета – повітряна ціль. Використання сигналу забезпечує високу роздільну здатність за дальністю, як наслідок більшу точність наведення ракети на ціль і, відповідно, більшу імовірність поразки цілі. Окрім того, враховуючи властивості узгоджених фільтрів ЧМ, може бути розглянутий варіант обробки комбінованих ЧМ (ЧМ+МХ) сигналів однотипними пристроями.

УДК 004.056.3

Жовтун А. А., Артемчук М. В., Сівоха О. М.

ОЦІНКА ВІДНОВЛЕННЯ ПОСТІЙНОЇ ГОТОВНОСТІ СИСТЕМИ УПРАВЛІННЯ ВІЙСЬКАМИ ПІСЛЯ ВПЛИВУ ВІРУСУ-ШИФРУВАЛЬНИКА НА ЕЛЕМЕНТИ ЗАСОБІВ УПРАВЛІННЯ

Система управління військами – це організаційно-технічна основа управління військами (силами). Вона включає: органи управління; пункти управління; засоби управління – зв'язок та комплекси автоматизованого управління, а також інші спеціальні засоби. Виведення з ладу однієї зі складових унеможливить дотримання основних вимог до управління військами: постійна готовність системи управління, стійкість, безперервність, оперативність, якість та прихованість.

Приведення у непрацездатний стан засобів управління можливе не тільки у разі виходу з ладу обладнання але й у разі пошкодження їх програмного забезпечення.

Програмне забезпечення – це набір кодованих інструкцій для керування обладнанням (комп'ютером, сервером і т.п.) та/чи іншими програмами. Програмне забезпечення являє собою інформацію, яка зберігається на матеріальних носіях у вигляді файлів. У разі модифікації або знищення файлів (інформації) задана робота програмного забезпечення, до якого належать файли, порушується або припиняється, що призводить до часткової або повної відмови в роботі засобів управління, вказаний стан визначається як непрацездатний, тобто засіб нездатний виконати хоча б одну із заданих функцій.

Вірус-шифрувальник – шкідливе програмне забезпечення, яке шифрує файли (інформацію) користувача і вимагає викуп за їх розшифровку, в зв'язку із чим даний вірус ще називають "вірус-вимагач". Шифруванню можуть підлягати: як цілий жорсткий диск так і його частина, як цілі файли (за визначеними ознаками) так і їх частини.

Найчастіше вірус-шифрувальник розповсюджується через поштові вкладення, у цьому випадку зараження відбувається тільки при запуску файлу, який додається до електронного листа. Рідше зараження відбувається після встановлення "заражених"

(з інтегрованим шкідливим кодом) програм чи оновлень вже інстальованого програмного забезпечення. “Заражені” файли (програми, оновлення) можуть бути занесені не тільки із зовнішньої мережі але і з внутрішньої, як з необережності так і навмисно.

Після зараження вірусом-шифрувальником за певних умов (при перезавантаженні, при вимкненні, при настанні визначеної події або ж одразу і т.п.) розпочинається процес шифрування інформації. Процес шифрування, у більшості випадків, “невидимий” для антивірусів, а сам вірус не сприймається як шкідливе програмне забезпечення, тому що він використовує алгоритми роботи, які застосовуються у багатьох легальних програмах. Також вірус здатний до самостійного розповсюдження, тому під час резервного копіювання даних можливе зараження сховища [1].

Небезпека такого вірусу полягає в тому, що переважна більшість випадків розшифровки власними силами неможлива, оскільки використовуються надзвичайно складні алгоритми шифрування. У дуже рідкісних випадках файли можна розшифрувати, якщо відбулося зараження вже відомим типом вірусу, для якого виробники антивірусів випустили дешифратор, але навіть в цьому випадку не гарантується відновлення інформації на 100%. Іноді вірус має ваду в своєму коді і дешифрування стає неможливим в принципі, навіть автором шкідливої програми.

Аналіз наявної у відкритому доступі інформації свідчить, про те що особливо уразливими є мережі із великою кількістю користувачів, так званий “людський фактор” (з необережності або навмисно), а також ніякі кошти та зусилля не здатні забезпечити 100% захист від проникнення шкідливого програмного забезпечення, у тому числі від зараження вірусом-шифрувальником.

Отже, метою дослідження слід вважати оцінку можливості відновлення у найкоротші терміни втраченої інформації “з нуля” з метою приведення засобів управління системи управління військами в справний стан (відповідність усім вимогам, обумовленим технічною документацією, при якому всі параметри, що визначають працездатність і характеризують стан засобу та його зовнішній вигляд, перебувають у заданих межах, і, крім цього, засіб не має відмов резервних вузлів та елементів).

Розглядається два пов’язаних між собою основних параметри відновлення постійної готовності системи управління військами після втрати інформації на елементах засобів управління: вартість відновлення; час відновлення. Показником вважається відношення вартості до часу відновлення. Значення показника розподіляються наступним чином:

- чим більше число – тим менший час відновлення, однак більша вартість;
- чим менше число – тим більший час відновлення, однак менша вартість.

Також при виробленні критерію оцінки слід врахувати час, при якому із заданою імовірністю вважається, що системою управління військами забезпечено виконання основних вимог: постійна готовність системи управління, стійкість, безперервність, оперативність, якість та прихованість.

Отже результатом дослідження вважати створення плану відновлення постійної готовності системи управління військами після втрати інформації на елементах засобів управління. Розробка методики оцінювання відновлення постійної готовності системи управління військами після втрати інформації на елементах засобів управління в залежності від ступенів важливості розпоряджень з управління військами (силами).

Зараження вірусом-шифрувальником хоча б одного з елементів засобів управління системи управління військами призводить до шифрування інформації що унеможливлює доступ до неї, відбувається втрата інформації, тобто виконання програмного забезпечення з метою керування визначеними процесами стає неможливим, в результаті чого заражена складова системи управління військами нездатна виконати хоча б одну із заданих функцій, а отже – переходить у непрацездатний стан та вимагає часу на відновлення справного стану шляхом відновлення втраченої інформації

або заміни елементу без відновлення втраченої інформації. Зауважимо, що імовірність відновлення інформації, доступ до якої став неможливим у зв'язку із дією вірусу-шифрувальника – дуже низька. Зважаючи на основні вимоги до управління військами, серед яких: постійна готовність системи управління, стійкість, безперервність, – підтримання (відновлення у найкоротші терміни) справного стану засобів управління є головним завданням.

Список літератури

1. Вірус шифрувальник оновлення. Вірус-шифрувальник - що це, чим небезпечний. Куди звернутися за гарантованої розшифровкою. [Електронний ресурс] // Платформа "Montazhtv" – 2017р. – Режим доступу: https://montazhtv.ru/uk/virus-shifrovalshchik-obnovlenie-virus-shifrovalshchik-chto-eto-chem-opasen/ (07.02.2021р.).

Пастухов В. В., Корнієнко О. В., Поліщук А. М., Сівак О. І.

ОСНОВИ КІБЕРБЕЗПЕКИ

Питання захисту ІТ мереж вийшло на новий рівень. За роки війни значно активізувався процес створення системи кібернетичної безпеки ІТС ЗС України. Водночас, незважаючи на зростаючий рівень технологічності нових викликів та кібернетичних атак, значна їх частина розрахована не на подолання складної системи кібернетичного захисту, а на пересічного користувача. Зокрема на його недосвідченість та необізнаність у питаннях кібернетичної безпеки та захисту інформації як під час виконання службових обов'язків, так і вдома.

На перший погляд може здатися, що кібератаки не можуть завдати великої шкоди та не забирають людських життів. Але це лише на перший погляд, до яких наслідків може призвести кожна з кібератак:

- вандалізм – атака, яка, звісно, не вбиває людей, але завдає удару по авторитету держави як у світі, так і серед населення, простими словами, завдає репутаційних втрат;
- пропаганда – розсилка спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору та дезорієнтації 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.

Використовуючи кіберпростір, хакери можуть зламати захищені мережі та отримати необхідну інформацію, тому ми мусимо спрямувати зусилля на захист своїх мереж і забезпечити їх безпеку, використовуючи такі рівні захисту інформації:

- запобігання – доступ до інформації та технології надається тільки для персоналу, який отримав допуск та має відповідні фахові навички;
- виявлення – забезпечується раннє виявлення злочинів і зловживань, навіть якщо механізми захисту були обійдені;
- обмеження – зменшується розмір втрат, якщо злочин все-таки відбувся, незважаючи на заходи щодо його запобігання та виявлення;
- відновлення – забезпечується ефективне відновлення інформації за наявності документованих і перевірених планів з відновлення.

Зважаючи на значний прогрес і досвід Європейського Союзу і НАТО у виробленні й удосконаленні механізму забезпечення кібербезпеки європейських країн, Україна і її Збройні Сили повинні стати активним учасником цих безпекових процесів.

Правильно розроблена стратегія щодо співпраці з ЄС і НАТО у сфері кібернетичної безпеки, безумовно, призведе взаємовигідного партнерства у вирішенні проблемних питань щодо забезпечення національних інтересів у сфері кібербезпеки.

УДК 004.056.5

Терещенко Т. П., Штонда Р. М., Артемчук М. В.

УМОВИ ТА ПОРЯДОК ПРОВЕДЕННЯ НЕЗАЛЕЖНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІЙСЬКОВИХ ЧАСТИН (УСТАНОВ) ЩОДО ЕФЕКТИВНОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Незалежний аудит інформаційної безпеки (далі – НАІБ) – один з найбільш ефективних на сьогоднішній день інструментів для отримання незалежної і об’єктивної оцінки поточного рівня захищеності військових частин (установ) від кіберзагроз. Тому для ефективного проведення НАІБ умовно поділимо етапи проведення незалежного аудиту на [1]:

- внутрішній незалежний аудит (далі – ВНАІБ);
- зовнішній незалежний аудит (далі – ЗНАІБ);
- технічний незалежний аудит (далі –ТНАІБ);
- позаплановий незалежний аудит (далі – ПНАІБ).

Перед проведенням ВНАІБ узгоджуються питання щодо:

- цілей, меж та методів проведення НАІБ;
- отримання доступу до документів, необхідних для планування НАІБ;
- порядку доступу до інформації, що циркулює в військовій частині (установі);
- визначення супроводжуючої особи від військової частини (установи).

На першому етапі проведення ВНАІБ аудитор інформаційної безпеки складає внутрішній план проведення НАІБ військової частини (установи) на основі аналізу отриманих документів та результатів попередніх НАІБ (за наявності).

При складанні внутрішнього плану проведення НАІБ військової частини (установи) аудитор інформаційної безпеки:

- визначає нормативні вимоги (політики, стандарти, керівні принципи та процедури), за якими побудовано захист об’єктів інформаційної діяльності військової частини (установи);
- визначення завдань, об’єктів та календарного плану НАІБ;
- визначає необхідні ресурси для НАІБ.

На другому етапі проведення ВНАІБ для отримання відомостей аудиту інформаційної безпеки аудитор інформаційної безпеки:

- проводить опитування та спостереження за діями персоналу;
- переглядає та аналізує параметри інформаційно-телекомунікаційних систем, автоматизованих систем (далі – ІТС) безпосередньо під час зустрічей із відповідальними співробітниками;
- використовує попередні аудиторські звіти та аналізує системні журнали, журнали реєстрації подій програмного і програмно-апаратного забезпечення;
- аналізує організаційно-технічну (експлуатаційну) документацію;
- аналізує налаштування ІТС;
- аналізує організацію обробки інформації в ІТС військової частини (установ).

На заключному третьому етапі проведення ВНАІБ відповідно до встановлених строків проведення аудиту, аудитор інформаційної безпеки складає Звіт проведення НАІБ військової частини (установ) щодо ефективності забезпечення кібербезпеки (далі – Звіт аудиту).

Перед проведенням ЗНАІБ військової частини (установ) проводиться збір та аналіз необхідних даних для проведення НАІБ.

На першому етапі проведення ЗНАІБ, аудитор інформаційної безпеки складає план проведення НАІБ військової частини (установи).

При складанні плану проведення НАІБ військової частини (установи) аудитором інформаційної безпеки враховуються всі аспекти перевірки:

- перелік об'єктів перевірки їх IP адреси;
- програмні, програмно-апаратні засоби, які будуть задіяні до НАІБ;
- перелік тестів на проникнення, які будуть проводитись.

На другому етапі проведення ЗНАІБ здійснюється віддалене тестування на проникнення з використанням програмно-апаратних засобів пошуку та аналізу вразливосте, можливості реалізації виявлених вразливостей.

На заключному третьому етапі проведення ЗНАІБ відповідно до встановлених строків проведення аудиту, аудитор інформаційної безпеки складає Звіт аудиту.

Наступним кроком є проведення ТНАІБ. Перед проведенням ТНАІБ узгоджуються питання щодо:

- цілей, меж та методів проведення НАІБ;
- отримання доступу до документів, необхідних для планування НАІБ;
- порядку доступу до інформації, що циркулює в військовій частині (установі);
- визначення супроводжуючої особи від військової частини (установи).

На першому етапі проведення ТНАІБ аудитор інформаційної безпеки складає внутрішній план проведення НАІБ військової частини (установи) на основі аналізу отриманих документів та результатів попередніх НАІБ (за наявності).

При складанні внутрішнього плану проведення НАІБ військової частини (установи) аудитор інформаційної безпеки:

- визначає нормативні вимоги (політики, стандарти, керівні принципи та процедури), за якими побудовано захист об'єктів інформаційної діяльності військової частини (установ);
- визначення завдань, об'єктів та календарного плану НАІБ;
- визначає необхідні ресурси для НАІБ.

На другому етапі проведення ТНАІБ для отримання відомостей НАІБ, аудитор інформаційної безпеки проводиться сканування мереж та обладнання з метою виявлення вразливостей.

На заключному третьому етапі проведення ТНАІБ відповідно до встановлених строків проведення аудиту, аудитор інформаційної безпеки складає Звіт аудиту.

Проведення ПНАІБ проводиться з врахуванням проведення умов та порядку, які зазначені під час проведення ВНАІБ, ЗНАІБ, ТНАІБ.

Підводячи підсумки хотілось б зазначити, що НАІБ військових частин (установ) проводиться згідно з нормами чинного законодавства України, національних стандартів та з урахуванням рекомендацій міжнародних стандартів аудиту. Проведення НАІБ є обов'язковим для всіх військових частин (установ). Однак необхідно розуміти, що НАІБ – це не разова процедура, він повинен проводитися на регулярній основі. Тільки в цьому випадку НАІБ буде приносити реальну віддачу і сприяти підвищенню рівня інформаційної безпеки військових частин (установ).

Список літератури

1. Штонда Р.М. Завдання та етапи проведення незалежного аудиту інформаційної безпеки військових частин (установ) щодо ефективності забезпечення кібербезпеки / Р.М. Штонда // Перспективи розвитку та застосування сучасних систем і засобів зв'язку в інтересах управління військами. – Харків. – Науково-практична конференція. – 2021. – с. 22-23.

Корнієнко О. В., Болцарівський А. І., Дзюба А. О., Левкович П. В.

ВИКОРИСТАННЯ ТЕЛЕГРАМ-БОТІВ ДЛЯ ПОКРАЩЕННЯ РІВНЯ НАВЧАННЯ ТА ОЦІНЮВАННЯ КУРСАНТІВ ВВНЗ

Однією з сучасних вимог щодо організації навчального процесу не лише у військових вишах, а й в усіх решта закладах є вимога інноваційності. Якщо у цивільних колег у більшості випадків з інноваційностю проблем немає, то у військових закладах введення інноваційної складової викликає певні ускладнення насамперед пов'язаних з таємність певної кількості інформації.

Розглянемо поняття інноваційності, та досвід українських вищих навчальних закладів щодо його впровадження. Великий тлумачний словник української мови трактує поняття "інновація" як "нововведення", тобто інновація - це втілення результату певного дослідження, що містить в собі корисну новизну для відповідної галузі. Інноваційність навчального процесу повинна змінювати відношення викладача та того хто навчається з старої системи навчання "суб'єкт" - "об'єкт", в якій студент є пасивним учасником освітнього процесу в новітню "суб'єкт" - "суб'єкт", де той хто навчається є повноцінним, активним співучасником даного процесу. В деяких ВНЗ України, таких як СумДУ, де Інноваційність подання інформації є одним з ключових показників якості навчання, введенні інтерактивні системи, системи доповненої реальності та системи онлайн навчання. В інших ВНЗ, таких як Кам'янець-подільський аграрно-технічний університет, віддають перевагу поєднанню традиційних систем навчання з новітніми.

В Україні, зважаючи на останні тенденції, з'являються нові тренди, застосовуючи які, можна максимально ефективно використовувати час та можливості того хто навчається. І одним з таких трендів є соціальні мережі, месенджери, зокрема Телеграм. Як уже відомо, спілкування з допомогою додатків значно спрощує комунікацію викладач-курсант/студент. Введення даної інновації безпосередньо в освітній процес у вигляді чат-ботів далі (ЧБ). ЧБ – це програма, що здатна імітувати спілкування одного співрозмовника з іншим, чи навіть кількома одночасно. ЧБ створюються на базі більшості сучасних додатків, але саме в телеграмі вони досягли найбільшого поширення, функціоналу та простоти створення. Віртуальний ЧБ може бути створений навіть без залучення відповідних програмістів, а їх основною ідеєю є автоматизація рутинних, повторюваних процесів з допомогою інтерактивної системи взаємодії з користувачем. Тобто при впровадженні ботів в освітній процес ВНЗ можна значно підвищити рівень зворотної реакції курсантів на різних етапах навчання. При наявності особистого ЧБ у викладача з'являється можливість автоматичного сповіщення курсантів про майбутні важливі події у дисципліні, особистий рівень успішності кожного курсанта, проведення автоматизованих "зрізів знань", аналіз рівня задоволеності наповненістю матеріалами та багато інших функцій, на розсуд самих викладачів. Для ВНЗ це чудова можливість адміністративної підтримки викладачів та іншого персоналу, зв'язку з здобувачами вищої освіти та громадськістю, складання навчальних планів з урахуванням інтересів студентів, проведення опитувань щодо рівня професійної майстерності викладачів та загального рівня задоволеності навчання, що є одним з важливих критеріїв оцінювання освітньої програми при її реалізації. Також це позбавить ВНЗ складання, заповнення та розповсюдження маси непотрібних паперів, що є застарілим, хоч і досі використовуваним підходом. Підсумовуючи, необхідно згадати, що у зарубіжних колег уже є практика застосування ЧБ, наприклад, у Технологічному інституті Джорджії в Вікторії є віртуальний помічник викладача – Джил Уотсон. Система здатна коректно відповідати на запитання студентів, а похожу практику уже впроваджують по усьому світу.

Отже, застосування ЧБ в освітній сфері це ефективний інструмент для істотного зростання рівня викладання та навчання у ВНЗ.

УДК 342.7 + 004.7

Пастухов В. В., Корнієнко О. В., Левкович П. В., Сівак О. І.

КОНЦЕПЦІЯ КІБЕРБЕЗПЕКИ СУЧАСНОСТІ НА ПРИКЛАДІ США

Дослідження показали, що за останній рік трафік кібератак збільшився з тривожними темпами. Це можна пояснити величезним сплеском кількості пристроїв IoT, що використовуються у всьому світі. У 2021 році справа стане дедалі цікавішою.

Обраний президент США Джо Байден заявив, що має намір зробити кібербезпеку "головним пріоритетом на кожному рівні управління" з моменту вступу на посаду. Причиною даної реакції став чітко спланований, складний хакерський напад , який в грудні 2020 року вразив Пентагон, кілька американських агентств, атомну лабораторію та всесвітньо відому компанію Fortune. Ймовірно, виконавець даної операції- Російська Федерація. Вказана масштабна активність з боку РФ, повинна простимулювати, знищивши інертність держави в даному напрямку та розпочати зусилля щодо захисту конфіденційних даних.

Майбутнє безпеки полягає в ініціативному підході. Проактивний підхід до безпеки призначений для запобігання атакам, а не реагування після нападу. Дні очікування виявлення нападу, а потім вжиття заходів щодо його карантину минули. Що пропонують та втілюють США? Активні розробки в галузі безпеки, такі як мікросегментація та концепція архітектури "Zero Trust", що зменшать поверхню атаки до мінімуму.

Тобто на ринку з'являється новий продукт, бренд. Придбання у користування індивідуальних технологій безпеки призводить до поодинокого підходу. Споживачу потрібна уніфікована платформа, яка може забезпечити активний захист, який не досягнеться традиційними точковими рішеннями. Це прогнозовано зростаюче уподобання до єдиної уніфікованої платформи перед традиційними точковими рішеннями буде продовжуватися у 2021 році та пізніше.

Оскільки віддаленість представників як військового так і цивільного організму є новою нормою сучасності, безпека більше не може бути зосереджена на центрі обробки даних, а натомість повинна перейти до тенети, мережі. Відповідно, прослідковується слабке місце, яке схильне до злому. Тобто, хто залишається відданим локальному, апаратному та програмному забезпеченню, врешті-решт має більші можливості щодо протидії.

Пропонується перехід до хмари, що означає переобладнання мережі організації на мікросервіси та власні хмарні, в тому числі захищенні додатки. Архітектура безпеки також повинна розвиватися і надавати доступ лише до трафіку між автентифікованими користувачами, пристроями та програмами в розподіленій організації.

Слід зазначити, що традиційна безпека по суті довіряє користувачам, кінцевим точкам, програмам та робочим навантаженням у межах певного периметра. Неодноразово цей підхід виявлявся неефективним, дозволивши будь-якій загрозі всередині мережі рухатися і залишатися не виявленим протягом тривалого часу. Щоб забезпечити моніторинг та перевірку кожного користувача, робочого навантаження та потоку мережі, організації застосовують архітектуру Zero Trust для забезпечення політики безпеки на рівні хоста з підходом „Нічого не довіряй, все перевіряй".

Вищезазначені тенденції свідчать про те, що слід бути більш стратегічними щодо контролю безпеки. Потрібно випереджати зростаючі та нові технології.

Здоренко Ю. М., Лаврут О. О.

ЗАБЕЗПЕЧЕННЯ QOS В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ НА ОСНОВІ МЕТОДІВ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ З ВИКОРИСТАННЯМ ANFIS

Основою будь-якого протоколу динамічної маршрутизації є використання метрик маршруту, з використанням яких приймається рішення про маршрут передавання потоку даних. Для інформаційно-телекомунікаційних мереж (ІТМ) військового призначення характерним є динамічна топологія пов'язана з специфікою функціонування таких мереж. Зміна конфігурації таких мереж може бути викликана множиною випадкових факторів, а саме: зміна місця розташування маршрутизаторів у зв'язку з характером бойових дій; виходом з ладу обладнання у зв'язку з знищенням противником; виходом з ладу через діагностичну несправність та інші. Тому протокол динамічної маршрутизації для таких мереж повинен базуватися на метриках, що враховують надійність проміжних вузлів передавання інформації (маршрутизаторів).

Існуючі протоколи динамічної маршрутизації для розрахунку метрик маршрутів використовують множину показників, до яких належать: затримка, пропускна здатність лінії, ймовірність втрат, надійність, завантаженість та інші. Сучасні ІТМ військового призначення потребують обов'язкового використання апріорної інформації про значення показника надійності для розрахунку метрик маршрутів протоколом динамічної маршрутизації. Тому пропонується удосконалити існуючи методи динамічної маршрутизації шляхом розробки та застосування систем прогнозування для отримання завчасної інформації про зміни в топології мережі та оновлення метрики маршрутів на її основі. Статистика про надійність вузлів ІТМ військового призначення може бути класифікована за класами можливих відмов, наприклад, через несправність обладнання (програмні чи апаратні збої) або з відмовами пов'язаними з інтенсивністю та характером бойових дій (знищення вузлів) та іншими класами періодичних чи випадкових факторів. Для кожного такого класу відмов пропонується реалізувати свою ANFIS. Результатом її роботи має стати прогнозоване значення кількості відмов відповідного *k*-го класу в найближчий часовий інтервал. В якості вхідних даних будуть використані зібрані дані про кількість відмов протягом попередніх періодів часу. Отримані, на основі прогнозування, дані про кількість відмов, використовуються для проведення розрахунків показника надійності вузла ІТМ військового призначення в наступному часовому інтервалі. Показник надійності в подальшому використовується для оновлення метрики маршруту.

Таким чином в роботі запропонований підхід для оновлення метрик маршрутів з використанням апріорних даних по надійності маршрутизаторів ІТМ, який оснований на використанні ANFIS. Це дозволяє завчасно прийняти рішення про використання резервних маршрутів в наступному часовому інтервалі у випадку несправності вузла та сприяє забезпеченню кращих параметрів QoS.

Мельник В. М., Нефедов О. П., Сидоренко І. І.

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРОТКОХВИЛЬОВОГО ЗВ'ЯЗКУ В УМОВАХ НЕСТАБІЛЬНОСТІ ХАРАКТЕРИСТИК СЕРЕДОВИЩА РОЗПОВСЮДЖЕННЯ

Проблема захисту каналів зв'язку від перешкод природного або штучного походження при застосуванні короткохвильових радіоканалів має дуже важливе значення

не тільки у військовій, але й у цивільній області. Оскільки важливість інформації, що надається між абонентами, постійно зростає в сучасних умовах обстановки, то актуальність проблеми забезпечення стійкості постійно зростає.

У теперішній час відомо дуже багато монографій та статей з приводу вказаної проблеми в усіх технічно розвинених країнах. Значну кількість з них займають ті, де розглядаються питання боротьби з впливом природних причин погіршення зв'язку, а саме завмиранням сигналів в каналах з параметрами, що змінюються (наприклад, іоносферний та тропосферний зв'язок).

Розглядаються принципи адаптивної компенсації перешкод з використанням просторових, поляризаційних та частотних розрізнень сигналів та перешкод. Велику увагу приділяється адаптивним антенним системам з кореляційними оберненими зв'язками. Такий підхід дозволяє реалізувати адаптивну просторову резекцію перешкод.

Аналізуються основні цифрові та аналогові алгоритми обчислення вагових коефіцієнтів. Розглядаються особливості формування опорних сигналів та питання швидкої дії та стійкості пристроїв, що реалізують ці алгоритми.

Прямі методи обчислення вагових коефіцієнтів засновані на використанні оцінки оберненої кореляційної матриці перешкод. Це дозволяє найбільш повно використати інформацію про перешкоди у процесі само налаштування. Вказується, що останні значно складніше у реалізації, ніж адаптивні пристрої з кореляційними оберненими зв'язками.

Значну увагу приділено градієнтним алгоритмам з кореляційними оберненими зв'язками. Випадкові зміни характеристик сигналів та перешкод приводять до декореляції електрорушійних сил, яка виникає в окремих елементах адаптивних антенних систем. Це призводить до зниження ефективності автокомпенсації. Наводиться оцінка цієї деко реляції і її вплив на ефективність авто компенсації в умовах завмирань.

Особлива увага приділяється до специфіки побудування адаптивних компенсаторів перешкод у каналах короткохвильового зв'язку. Аналізуються різноманітні способи розв'язання задачі виключення сигналу з ланцюгів адаптації, що засновані на використанні просторових, часових та частотних розбіжностей сигналу та перешкод.

Розглядаються найбільш перспективні напрямки розв'язання проблеми захисту каналів зв'язку – розробка пристроїв адаптивної компенсації перешкод. Аналізуються їх переваги та недоліки, робляться висновки.

УДК 621.397

Ковтун І. В.

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ В ЗАВДАННЯХ СТИСКУ ЗОБРАЖЕНЬ

З розвитком телекомунікаційних систем і мультимедійних технологій неухильно ростуть об'єми передаваних медіаданих, а разом з ними підвищуються і вимоги до ефективності роботи систем кодування інформації, у тому числі до алгоритмів стискування відеоконтенту. Крім того, збільшуються і середні об'єми передаваних відеоданих у зв'язку зі збільшенням дозволу зображень в сучасних форматах цифрового відео. Також необхідно враховувати, що загальний об'єм відеоданих в інтернет трафіку збільшується за рахунок широкого використання сервісів потокового телемовлення, систем хмарного зберігання даних, збільшення числа камер безпеки і інших пристроїв, що здійснюють передачу відео через інтернет.

В той же час пропускні здібності каналів передачі даних ростуть не так швидко. У зв'язку з цим для побудови складних інформаційних систем критично важливо коду-

вати відеодані як можна компактніше, що дозволяє передавати більше даних по тому ж самому інформаційному каналу, збільшуючи швидкість роботи таких систем.

Одним із способів пониження об'ємів вихідного бітового потоку при кодуванні візуальних даних є використання дискретних ортогональних перетворень. Дискретні ортогональні перетворення активно використовуються в усіх сучасних стандартах стиску зображень і відео, наприклад, в таких як H.264, H.265, JPEG і багатьох інших. Одним з дискретних ортогональних перетворень, що дозволяють досягати значних мір стискування, є дискретне вейвлет-перетворення, яке використовується в таких стандартах стиску, як JPEG2000, відеокодеках Dirac та інші.

Використання багатоканальних схем дискретного вейвлет-перетворення в системах відеокодування є новим і перспективним підходом, який дозволяє збільшити міру стиску при збереженні якості відновлених зображень, проте практично в усіх існуючих дослідженнях розглядається лише двоканальна схема, що поступається по ефективності кодування багатоканальному аналогу.

Сучасні технології компресії зображень і відео включають як методи стиску інформації без втрат, такі як кодування ентропії, міжкадрове і внутрішньокадрове прогнозування, так і методи стиску інформації з втратами, наприклад спільне використання дискретних перетворень і квантування. Перші методи дозволяють однозначно відновити стислі дані, але вони поступаються по мірі стиску другим, які, проте, вносять неусувні при відновленні втрати початкової інформації.

Стиск візуальної інформації з втратами ґрунтоване на недосконалості людського зору – їм в середньому краще сприймаються зміни в низьких частотах яскравісних і кольорорізницевих складових зображення, чим у високих. При цьому велика частина енергії зображення, зазвичай, концентрується в низьких частотах, що дозволяє компактніше представляти сигнал. Для цього необхідно перевести дані з яскравісного і кольорорізницевого просторового представлення зображень в частотне. Саме з цією метою використовуються дискретні ортогональні перетворення в завданнях стиску зображень.

У роботі були досліджені властивості вейвлет-перетворення і особливості його використання в завданнях стиску зображень, сформульовані і перевірені методи підвищення ефективності стиску візуальної інформації за рахунок використання багатоканального вейвлет-розкладання зображень, а також досліджувалися можливості побудови ефективних відеокодуючих систем на їх основі.

Даник Ю. Г.

МЕТОД ВИБОРУ ТА ОБҐРУНТУВАННЯ БАЗОВОЇ СИСТЕМИ ІНДИКАТОРІВ КІБЕРБЕЗПЕКИ

Зростання ролі і значення успішного вирішення завдань забезпечення кібербезпеки (КБ) держави обумовлено стрімким інноваційним розвитком інформаційних, електронних та кібер- технологій, лавиноподібним зростанням об’ємів інформації що зберігається, обробляється і передається в кіберпросторі, ускладненням систем управління та взаємодії між ними. При цьому, для своєчасного і якісного їх вирішення необхідно мати обґрунтовану базову систему індикаторів КБ, як для глобального і загальнодержавного рівнів так і для відомчого і об’єктного. Першочерговими об'єктами дестуктивних кіберінформаційних впливів, як в сучасних умовах, так і на майбутнє є об’єкти критичної інфраструктури (ОКІ), а серед них – ОКІ сектору безпеки і оборони держави (СББ). Тому, особлива специфіка при виборі і обґрунтуванні систем індикаторів КБ має місце при їх формуванні для СББ та для об’єктів критичної інфраструктури.

Кібервразливість об’єктів критичної інфраструктури СББ обумовлена низкою

об’єктивних факторів сьогодення обумовлених тенденціями розвитку високих оборонних технологій. А саме: глобальною інформатизацією та початком всебічної роботизації військових формувань і створення високо інтегрованих систем управління, які, в свою чергу, стають об'єктами деструктивних інформаційних та кібер- впливів і вимагають розвитку інноваційних форм і способів виявлення та протидії реалізації цих загроз; зростанням інтенсивності конфліктів в інформаційному та кіберпросторах, за участі спеціально створених для цього спеціалізованих структур та формувань протиборчої сторони; можливістю домінування будь-якої країни і недержавних акторів у веденні деструктивних дій через інформаційний та кібер- простори; використанням світових інформаційних мереж та електронних засобів масової інформації для маніпулювання свідомістю та досягнення когнітивних трансформацій як окремих спільнот і населення країн так і світової громади; постійним зростанням кількості та можливостей комп’ютерних та електронних засобів, що задіяні в зберіганні, обміні і обробці інформації і під час прийняття управлінських рішень з подальшою інтеграцією засобів штучного інтелекту та обробки великих масивів даних в системах оборонного призначення; інтеграцією на основі продуктів високих технологій систем розвідки, управління та ураження від підрозділу (одиниці бойової техніки) до командування всіх ланок управління.

Для побудови дійсно ефективної системи КБ необхідно мати адекватну модель загроз і оцінки ризиків їх реалізації, а в особливості обґрунтовану базову систему індикаторів КБ, яка надасть можливість забезпечення необхідного рівня КБ.

Аналіз теорії, практики і досвіду вирішення завдань управління ризиками реалізації загроз КБ держави у провідних державах світу свідчить, що основною тенденцією і проблемою при його здійсненні є забезпечення його адаптивності з врахуванням інтенсивних змін в умовах високого ступеню невизначеності, як у розвитку технологій так і впливу великої множини зовнішніх і внутрішніх факторів. Кіберзловмисники активно використовують весь відомий спектр вразливостей об'єктів, на які здійснюється деструктивні впливи, діють швидко, а головне - часто змінюють стратегії, тактики і засоби здійснення впливів. Безпосередня загроза складних цілеспрямованих впливів спонукає фахівців, які відповідають за КБ по-новому розглядати й оцінювати ефективність систем захисту, технології та засоби виявлення атак, їх запобігання та протидії ним. Головне завдання будь-якої системи КБ - максимально швидко, з використанням високоінтелектуальних засобів захисту, що дозволяють вирішувати завдання з своєчасного виявлення атак і інцидентів (наприклад, застосовуючи security information and event management (SIEM), network traffic analysis (NTA), комплексні antiAPT рішення) виявити атаки і їх агентів в системі, своєчасно блокувати їх, щоб вони не встигли нанести неприпустимої шкоди (ability to detect).

При цьому основним елементом вирішення завдань управління ризиками реалізації загроз КБ держави є їх своєчасне виявлення та ідентифікація.

Також важливою проблемою на шляху вирішення питання оцінки стану кібербезпеки є формування системи вимірювання (метрики) та системи індикаторів для кількісного та якісного оцінювання цього надзвичайно складного явища. Головні вимоги до зазначеної системи — її інформаційна повнота й адекватність.

В доповіді запропоновано методику виявлення, ідентифікації та обґрунтування базової системи індикаторів кібербезпеки.

Системний підхід до їх вибору дозволяє виділити наступні складові, які є базовими для обґрунтування системи індикаторів кібербезпеки: законодавчу: законодавча, нормативно-правова; освітньо-наукову; кадрову; технологічно-промислову; системно-структурну: система, структура і завдання органів (підрозділів), що забезпечують кібербезпеку; організаційно-технічну: організаційно-технічні заходи, методи і засоби; програмно-апаратно технічну: програмно-апаратно-технічні засоби і способи забезпечення кібербезпеки.

Тому кібербезпеку можна характеризувати двома основними складовими: її потрібним станом (CSR) і якістю його забезпечення (CSP). Ґрунтуючись на цій концепції, узагальнену міру (індекс) кібербезпеки можна подати за допомогою кватеріона {CSQ}:

$$\{CSQ\}=j\ CSR+ CSP(I_z, I_{on}, I_k, I_{tp}, I_{ss}, I_{ot}, I_{pt}).$$

Кватеріон {CSQ} містить уявну, скалярну частину j CSR , яка описує потрібний стан кібербезпеки і дійсну скалярну частину, у вигляді проекції норми радіус вектора CSR на ідеальний вектор з координатами (1; 1; 1, 1; 1; 1, 1), який описує якість її забезпечення у просторі семи вимірів: законодавчого (I_z), освітньо-наукового (I_{on}), кадрового (I_k),), технологічно-промислового (I_{tp}),), системно-структурного (I_{ss}), організаційно-технічного (I_{ot}), програмно-апаратно технічного (I_{pt}). При цьому j набуває значення дійсної одиниці за наявності необхідного стану забезпечення кібербезпеки. При цьому, за CSR > 0, але якщо система кібербезпеки її не забезпечує має місце конфлікт (CSR = 0):

$$j = \begin{cases} 1, \text{якщо CSR} > 0; \\ \sqrt{-1}, \text{якщо CSR} = 0. \end{cases}$$

Як показали проведені дослідження серед факторів, які слід враховувати при виборі індикаторів КБ в сучасних умовах та на майбутнє основоположними є: ступінь відповідності засад державної політики, наявних, як загальнодержавних так і відомчих, концепцій, стратегій (доктрин), нормативно-правових актів, завдань, та функцій військово-політичної діяльності суб'єктів КБ з питань планування її забезпечення на всіх рівнях відповідно до Плану оборони держави та ступінь їх узгодженості із законами держави та міжнародним правом з питань КБ та правом війни; відповідність стану формування та реалізації політики Міністерства оборони та Збройних Сил щодо забезпечення КБ існуючим та прогнозованим загрозам для забезпечення можливості їх запобігання та нейтралізації; наявність та якість засад застосування Збройних Сил та інших військових та спеціальних формувань для комплексного і узгодженого виконання завдань безпеки; наявність, достатність та стабільність бюджетного фінансування програм розвитку, утримання та всебічного забезпечення системи КБ; наявність та ефективність єдиного органу управління призначеного для реалізації єдиної політики та стратегії дій Міністерства оборони, Збройних Сил, інших військових формувань в інформаційному та кіберпросторах, планування, організації та координації заходів щодо, інформаційної та кібер- безпеки і кібероборони, захисту критичної інфраструктури держави; управління силами інформаційної та КБ і кібероборони за єдиним замислом і планом під час кризових ситуацій, в умовах особливого періоду та правового режиму воєнного стану; стан інформаційних та кібертехнологій у сфері оборони, забезпечення розвитку і безпеки власної інформаційної та управлінської інфраструктури і ресурсів, захисту них від інформаційних та кіберзагроз; наявність та стан військового наукового потенціалу, наукових шкіл в галузі інформаційної та кібер- безпеки; стан кадрового забезпечення фахівцями з питань інформаційної та КБ і кібероборони, наявність та стан системи підготовки військових фахівців всіх рівнів з питань інформаційної та КБ і кібероборони тощо.

УДК 623.4

Щерба А. А., Петлюк І. В.

РОЗВИТОК СИСТЕМ НАВІГАЦІЇ КОМАНДИРСЬКИХ МАШИН УПРАВЛІННЯ РАКЕТНИХ ВІЙСЬК І АРТИЛЕРІЇ

Аналіз досвіду ведення бойових дій під час проведення Антитерористичної операції та операції Об'єднаних сил на сході нашої держави показує, що підвищення

ефективності дій артилерійських підрозділів неможливо досягнути без покращення їх мобільності. Для успішного бойового застосування підрозділів артилерії, машини управління командирів артилерійських підрозділів оснащені навігаційною системою, на яку покладені завдання щодо визначення місцеположення та орієнтації об'єкта у просторі.

В залежності від призначення, об'єму отримуваної інформації та методів навігації, які застосовуються при цьому, розрізняють: інерціальні навігаційні системи, одометричні системи обчислення шляху, радіонавігаційні та супутникові радіонавігаційні системи. Комплекси командирських машин управління, які дісталися українській армії у спадок від радянської, сьогодні вже є морально та фізично застарілими, і не відповідають сучасним вимогам щодо оперативності підготовки їх до роботи, точності визначення поточних координат об'єкта під час руху, а також часу та точності безперервної роботи. Разом з тим, беззаперечною перевагою інерціальної навігаційної системи є автономність її роботи, оскільки для свого функціонування не потребує ніяких додаткових джерел інформації, окрім вихідних даних про місцезнаходження у заданій системі координат, та, як наслідок, завадозахищеність. Суттєвим недоліком таких систем є зростання похибки визначення координат та курсу з часом.

Широкого застосування останнім часом набули супутникові радіонавігаційні системи, принцип роботи яких оснований на обробці сигналів від супутників. Разом з тим, їм притаманно: нестійкий сигнал у лісистій та гірській місцевості, можливе пропадання сигналу або некоректна робота внаслідок впливу засобів радіоелектронної боротьби противника. За таких умов більш надійне визначення координат рухомих об'єктів забезпечать радіонавігаційні системи та системи обчислення одометричного типу.

Отже, перспективна навігаційна система машини управління артилерійського командира повинна мати у своєму складі комплексовану навігаційну систему. Таким чином, для забезпечення необхідної точності вирішення навігаційних задач, будуть збережені переваги кожної із підсистем, компенсуються недоліки одного виду навігаційної підсистеми та доповняться переваги інших. Також, до складу сучасної навігаційної системи повинна входити геоінформаційна система, або іншими словами, цифрова карта місцевості.

УДК 378.147

Безугла Г. Є.

ГЕЙМІФІКАЦІЯ ЯК ІНСТРУМЕНТАЛЬНИЙ ЗАСІБ В ДИСТАНЦІЙНОМУ НАВЧАННІ

Вимоги до сучасного навчання складаються не тільки з вимог до навчального матеріалу, а також з вміння використовувати сучасні інформаційні технології викладання на базі поширених платформ дистанційного навчання. Особливості дистанційної і змішаної форм навчання перш за все вимагають враховувати відсутність можливості контролювати увагу студентів під час самого процесу навчання. Тому найголовнішим критерієм успіху є формування зацікавленості студентів до навчального матеріалу.

Формування мотивації вивчення навчальної дисципліни починається з розуміння студентами актуальності, можливості застосовування отриманих знань в практичної діяльності, бачення перспектив розвитку та наявність творчої складової навчальної дисципліни. Головним аспектом формування дистанційних курсів є забезпечення необхідними ресурсами самостійної роботи студентів, отримання постійного зворо-

тного зв'язку для з'ясування ступені засвоювання учбового матеріалу студентами. Розробка інтерфейсу дистанційного курсу також має важливу роль для кращого сприйняття навчального контенту. Гейміфікація як інструментальний засіб знаходить своє застосовування в дистанційному навчанні з метою формування дружнього інтерфейсу, що сприяє більш швидкому ознайомленню з навчальним матеріалом.

Елементами будь якої гри є конкуренція, наявність мотиваційних призів, можливість бачити свій рейтинг і його динаміку у порівнянні з іншими гравцями. Неявно всі ці елементи вже існують в системі отримання знань під час освітнього процесу: отримання балів и рейтингова шкала за дисципліну, формування стипендіального рейтингу, формування творчих завдань на практичні або курсові роботи.

Найбільш поширена система дистанційного навчання Moodle дозволяє використовувати ігрові елементи, а саме: можливості нагороджувати значками за категоріями, що визначені викладачем; розділ доступу для послідовного освоювання матеріалу, що відповідає проходженню різних рівнів ігри; отримання балів за виконання завдань, участь во взаємному оцінюванні за допомогою організації семінарських занять, використання широкого спектру занять та завдань, розробки різноманітних тестових завдань. Графічна візуалізація процесу навчання в системі Moodle представлена у вигляді посилань на зовнішні ресурси або завантаження статичних графічних об'єктів, але система дозволяє відстежувати рівень виконання завдань і, відповідно, ступінь проходження курсу.

У якості додаткового інструмента для більш швидкого освоювання базових понять навчальної дисципліни, методів розв'язку завдань певного типу, застосування формул або алгоритмів в різних умовах завдання можуть використовуватися гіперказуальні ігри (ГКІ) у вигляді окремого додатка. Відмінностями ГКІ є дуже коротка ігрова сесія, просте управління, застосування різноманітних механік та інтерфейсів, відсутність складної стратегії та обмежень до ігрових пристроїв, що забезпечує певні переваги для застосування цього типу ігри, формуванню зацікавленості студентів в процесі навчання.

УДК 528

Кравець Т. М., Кравець М. О.

ОРГАНІЗАЦІЯ СТВОРЕННЯ АРТИЛЕРІЙСЬКОЇ ТОПОГЕОДЕЗИЧНОЇ МЕРЕЖІ В УМОВАХ АКТИВНОЇ ПРОТИДІЇ РЕБ ПРОТИВНИКА

В результаті виконання топогеодезичної прив'язки отримують координати і дирекційні кути орієнтирних напрямків. Однак є ряд особливостей виконання завдань командиром підрозділу топогеодезичного взводу. До основних вимог топогеодезичної прив'язки можна віднести: своєчасність, точність, надійність і прихованість.

Провівши аналіз вимог керівних документів, що до організації та створення артилерійської топогеодезичної мережі (АТГМ) показує, що виконання робіт мають чітко визначені терміни. І якщо час підготовки мережі змінити практично неможливо, то час на здійснення обсяг робіт доцільно зменшити. Зменшення часових показників можливе за допомогою методу сіткового планування.

Аналіз досвіду бойових дій в АТО (ООС) показав, що найпоширенішого застосування набув спосіб застосування СНС. Маючи переваги в мобільності, швидкості застосування, але не в момент застосування радіоелектронної боротьби.

На всій території Донбасу та частині Луганську знаходиться велика кількість та широка номенклатура засобів РЕБ (від древніх, до зразків, які ще не стали на озброєння і проходять там випробування), що неодмінно потребує врахуванню як під час

створення АТГМ так і під час використання радіонавігаційних приладів, оскільки застосування радіонавігаційних апаратів таких як: СН-3003М “Базальт”, СН-3210 “Базальт-К” для визначення координат стає практично неможливим.

Сіткове планування полягає в моделюванні сіткового графіку, розрахункових методів, що необхідні для контрольних заходів для планування і управління роботою.

В результаті дослідження, було проаналізовано створення мереж різними способами, в наслідок аналізу виявили: 1) при наявності часу на виконання поставленої задачі слід застосовувати на геодезичній основі пряму засічку орієнтованим приладом. 2) при обмежених часових показниках, засічку за виміряними кутами за допомогою ПАБ-2АМ, та для здійснення обчислень програму EXCEL.

Для скорочення заходів щодо створення АТГМ командиру запропоновано застосовувати:

- при обмежених часових показниках: для визначення координат – карту геодезичних даних; засічка за виміряними кутами із застосуванням ПАБ 2АМ; обчислення польвих вимірів за допомогою Excel;
- для здійснення контролю: координати вихідного пункту визначені на геодезичній основі; засічку орієнтованим приладом із застосуванням 1Г17; обчислення польвих вимірів за допомогою Excel.

В результаті удосконалення вдалося скоротити: 1) постановку завдання до 15 хв.; 2) визначення координат (за допомогою карти геодезичних даних) 40 с 3) обчислення результатів вимірів (за допомогою телефону в програмному середовищі Excel). В загальному вдалося скоротити час з 340 хв. 40с до 300 хв.

УДК 528

Левкович П. В.

СУЧАСНІ ПІДХОДИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ ДАНИХ ПРО МІСЦЕВІСТЬ ВИКОРИСТОВУЮЧИ ШВИДКІСНЕ 3D-КАРТОГРАФУВАННЯ

В останні десятиріччя у світі відбувається надзвичайно інтенсивний розвиток нових технологій одержання інформації про просторові характеристики об’єктів на поверхні Землі, в тому числі засоби дистанційного зондування, супутникової навігації, геоінформаційного моделювання, штучного інтелекту тощо.

Але саме трьохвимірне моделювання дозволяє точно та детально описати реальну місцевість і взаємне просторове розміщення об’єктів на ній. Завдання побудови трьохвимірних моделей місцевості для об’ємних територій в оперативному режимі стають все більш актуальними. 3D-картографування можливо широко використовувати для вирішення наступних задач:

- використання у програмному забезпеченні, в тому ж числі симулятори при підготовці дій;
- керування діями будь-якого роду підрозділами;
- керування польотними місіями, різноманітних авіаційних засобів;
- організація пошукових операцій та моделювання надзвичайних ситуацій.

Технологія швидкісного 3D-картографування основана на використанні даних дистанційного зондування землі (ДЗЗ), а саме стереопар космічних зображень надвисокого просторового розширення. При цьому можуть використовуватись не тільки дані спеціальної стереозйомки, але також і одиночні зображення, які утворюють так звану ситуативну стереопару та у результаті – дані стерео аерозйомки.

Для обробки даних використовується автоматична технологія побудови 3D моделей, що суттєво мінімізує ручну працю, часові втрати і кінцеву вартість продукту. Якщо порівняти отримані моделі зі світовими стандартами деталізації LOD (Level of Details), то отримаємо відповідність до 2 рівня (LOD2) – "коробки" будівель з деталізацією дахів. Додатково текстурування отриманої моделі. Також важливою особливістю є те, що об'єкти будівель в моделі будуть відокремлені один від одного, у відмінності від більшості продуктів на ринку, в яких автоматично згенеровані моделі території реалізовані однією суцільною територією, що включають в себе будівлі, дерева та рельєф.

Геометрична точність моделей, отримана використанням технології швидкісного 3D картографування на основі космічних зображень, відповідає 2-3 метрам.

Вже в кінцевому результаті, при об'єднаному використанні вище зазначеного способу картографування та фотореалістичної технології, трьохвимірні сцени перетворюються у віртуальну реальність, яка у свою чергу беззаперечно стане підтримуючим фактором у прийнятті рішення при плануванні будь-якої операції для забезпечення правопорядку.

Бабічева А. К., Васильцова Н. В.

МОБІЛЬНА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВИРІШЕННЯ ЗАДАЧІ ОПТИМІЗАЦІЇ МАРШРУТУ ДО ЗАДАНОГО ОБ'ЄКТА

Проблеми вирішення задач оптимізації маршрутів до заданих об'єктів й на теперішній час розглядаються і вирішуються в багатьох працях дослідників. Але, незважаючи на велику теоретичну базу досліджень, на жаль, представлено не дуже багато програмних додатків, що дозволяють людям, які не є фахівцями в галузі математики і програмування, використовувати існуючі розробки для вирішення практичних задач.

Аналіз існуючих підходів до вирішення розглянутих задач показав, що для визначення оптимального маршруту могли б допомогти деякі програми зі зручним інтерфейсом та простотою знаходження цих маршрутів.

Для розв'язання таких задач пропонується використовувати пристрої мобільного зв'язку, наприклад, смартфони, які актуальні й поширені в нашому поколінні для кожної людини.

Для вирішення цієї задачі були проаналізовані та розглянуті основні алгоритми знаходження оптимального маршруту на графах та обраний алгоритм Дейкстри, який найбільше задовольняє поставленій задачі.

Метою роботи є розробка та інтегрування програмного модуля, який реалізує алгоритм Дейкстри, в Google Maps з використанням смартфонів на базі операційної системи Android.

Запропонована реалізація задачі оптимізації маршруту з використанням мобільних інформаційних технологій дає можливість вирішити цю задачу в режимі, близькому до режиму реального часу. Алгоритм вирішення задачі не завжди є тривіальним, але вимоги до його обчислювальної точності порівняно малі. Це дає можливість практично на будь-якому мобільному пристрої отримати результат вирішення задачі оптимізації маршруту навіть на великих обсягах вхідних даних за долі хвилини.

В роботі пропонується автоматизований інструментарій (програмний модуль), що призначений для реалізації задачі виключно на стороні клієнта. При розробці програмного модуля в роботі були проаналізовані відповідні програмні інструментальні засоби й для розробки мобільного додатку для визначення оптимального маршруту з використанням алгоритму Дейкстри використовувались такі з них: Java, XML,

Android Studio, Goggle Maps. Розроблений додаток успішно протестований на різних вхідних даних задачі пошуку оптимального маршруту до найближчого пункту збирання та утилізації використаних елементів живлення. Було досліджено якість результатів при заданих параметрах алгоритму, в результаті чого обрані ефективні рішення. Перевагами пропонованої розробки є:

– оперативність вирішення задачі оптимізації маршруту до заданого об'єкта з використанням мобільного пристрою на платформі Android з невеликими обчислювальними ресурсами;
– адаптація розробки до будь-якого розміру екрану пристрою;
– можливість аналізувати результати кожного етапу вирішення поставленої задачі.

Кравець Т. М., Полець О. П.

ТОЧНІСТЬ КАРТОГРАФІЧНОГО ЗАБЕЗПЕЧЕННЯ ПАК "МАПА"

У програмно-апаратному комплексі (далі ПАК) "МАПА" використовується геопросторова інформація растрової форми у вигляді топографічних карт та супутникових зображень місцевості, в межах завантаженого масштабу (зуму) на певну територію України (по областях, військових полігонах, зона ООС). Об'єми файлів завантаження супутникових зображень залежать від масштабу і характеризуються в середньому 2-4 ГБ для 16 зуму і зона ООС 18 зуму разом з топографічною картою ГШ – 110,7 ГБ. Дане растрове картографічне забезпечення характеризується точністю растра і точністю координатної прив'язки.

Щоб виконати зазначене дослідження запропоновано використати каталог координат геодезичних пунктів (далі ККГП). Прямокутні координати і висота з ККГП приймаються за істинні значення.

У ПАК "МАПА" за допомогою меню програми "Функції" із спливаючого списку вибирають функцію "Перейти на координати". Після цього вводять значення прямокутних координат геодезичного пункту, взяті з ККГП. Після введення координат вибираємо функцію "Перейти". ПАК "МАПА" переходить зображенням до обраних координат. За дешифрувальними ознаками знаходять на картографічному зображенні "МАПИ" пункт геодезичної мережі і максимально точно за найбільш допустимого масштабу наводять цілик у місцеположення центру пункту геодезичної мережі. Отримані значення координат і висоти цього пункту приймають за визначені у ПАК "МАПА" та порівнюють з значенням координат і висоти, взятих з ККГП. Пункти геодезичної мережі, у надійності розпізнавання центру яких були сумніви, до результатів дослідження не враховувались.

Для дослідження точності картографічного забезпечення ПАК "МАПА" було проаналізовано 38 пунктів державної геодезичної мережі 1-3 класів. Це дозволило виконати оцінку точності координатної прив'язки картографічного забезпечення. Виконана оцінка точності картографічного забезпечення у ПАК "МАПА" обчисленням середніх квадратичних похибок. Відповідно середні квадратичні похибки координатної прив'язки картографічного зображення: δ_X=6,0 м, δ_Y =5,5 м, δ_H=18,0 м.

Отримані в дослідженні результати оцінки точності картографічного забезпечення ПАК "МАПА" свідчать, що картографічне забезпечення задовольняє вимогам щодо точності топогеодезичної вогневих позицій артилерії, стартових позицій тактичних ракет, командно-спостережних пунктів, постів та позицій артилерійської розвідки на оцінку відмінно; визначення прямокутних координат об'єктів (цілей); виконання розрахунків і вимірів за картографічним зображенням. Визначення дирекційних кутів орієнтирних напрямів координатним способом за картографічним зображенням ПАК "МАПА" обмежена. Визначення абсолютних висот об'єктів (цілей) також є обмеженим.

Васильцова Н. В., Кузьма Є. А.

ДОСЛІДЖЕННЯ ПРОЦЕСУ АВТОМАТИЗАЦІЇ ЗАДАЧІ ФОРМУВАННЯ ТА ВЕДЕННЯ ІНДИВІДУАЛЬНОГО ПЛАНУ ВИКЛАДАЧА

Діяльність професорсько-викладацького складу закладів вищої освіти (ЗВО) проводиться у теперішній час в рамках жорстких фінансових, часових та інших обмежень, точне врахування яких дозволяє зробити процес навчання адаптивним на кожному кроці виконання планів різних рівнів, що розробляються ЗВО.

Аналіз діяльності кафедри, як основного структурно-функціонального елемента ЗВО, показав, що діяльність викладачів кафедр є ітераційним процесом, який починається в новому навчальному році з формування індивідуального плану викладача. В процесі обстеження діяльності кафедри задача формування і ведення індивідуального плану викладача виявляється дуже складною і потребує виконання з використанням інформаційних технологій. Актуальність такого виду проектування обумовлена наступними обставинами: високою трудомісткістю і низькою оперативністю заповнення плану в паперовій формі; повторюваністю процесу заповнення індивідуального плану внаслідок сильної залежності від змін; відсутністю електронної бази даних, тобто відсутністю можливості повторного використання даних; необхідністю включення у план усіх видів робіт викладача так, щоб зберегти часові норми; потребою ведення декількох індивідуальних планів для викладачів, що мають більше однієї робочої ставки; створенням можливості подальшої інтеграції розробленого програмного продукту до інформаційної системи університету.

В роботі, що пропонується, проведений аналіз структури процесу формування плану викладача. Розділи індивідуального плану включають види, обсяги робіт викладача та підсумкові результати. За напрямками робіт виділяють наступні види робіт: навчальна; методична; наукова; організаційно-виховна. Ці розділи повинні відображати розподіл робочого часу викладача з зазначенням підсумкового результату та строку виконання за кожним видом робіт. Потрібно враховувати, що є види робіт, що мають обов’язково бути включеними до індивідуального плану. До них відносяться такі, що забезпечують якісне функціонування навчальної роботи, а також, такі, що мають виконуватися відповідно до обсягу робіт кафедри.

У роботі представлена концепція процесу формування та ведення індивідуального плану викладача, розроблена концептуальна схема процесу і проведена її декомпозиція, розроблена діаграма потоків даних задачі та її декомпозиція. Виділені базові функції, які забезпечують функціонування бізнес-процесу: формування переліку посад та довгострокових доручень; розрахунок навантаження другої половини дня викладача; планування виконання методичної, наукової; організаційної та виховної робіт.

Особлива увага приділена аналізу останніх трьох функцій. Окрім того, що вони відображають ітеративність процесу планування (особливо це стосується розділів методичної, організаційної та виховної роботи), вони ще й мають подібну структуру представлення в індивідуальному плані (номер за порядком, зміст кожної роботи, підсумковий результат у вигляді форми звітності та запланованих годин, а також, строк виконання). З цього зроблено висновок, що три базових функції можна реалізувати у вигляді однієї з різними вхідними даними. Окрім цього виділені три службові функції: формування переліку видів робіт, рекомендованих до виконання; формування переліку посад та довготермінових доручень; формування і ведення нормативно-довідкової інформації за ключовими показниками (KPI) діяльності кафедри.

Проведені дослідження дозволяють формувати вимоги до проведення процесу автоматизації задачі формування та ведення індивідуального плану викладача.

Бурцева В. В., Шеховцова І. О.

АСПЕКТИ РОЗРОБЛЕННЯ МЕТОДИК КАЛІБРУВАННЯ РОБОЧИХ ЕТАЛОНІВ

Світова практика в галузі метрології ґрунтується на використанні єдиного підходу в оцінці компетентності та якості роботи калібрувальних лабораторій. Вимогами стандартів п. 7.2.1.1. ISO/IEC 17025:2017 та п. 7.1.2. ISO 10012: 2005 передбачено, що лабораторія для здійснення відповідної діяльності повинна мати методики, за якими проводиться калібрування робочих еталонів (далі – РЕ) з використанням універсального показника якості всіх видів вимірювань – невизначеності.

Отже постає питання: розроблення методик калібрування робочих еталонів у сфері військової метрології – це тільки формальність або ж все-таки необхідність, пов'язана з приведенням системи метрологічного забезпечення ЗС України до міжнародних норм і правил, діючих в галузі метрології. Слід зазначити, що в умовах сьогодення переважна кількість нормативних документів (НД), зокрема праці міжнародних інститутів МИ, міждержавні стандарти ГОСТи були скасовані в Україні. Крім того відповідно до наказів Національного органу стандартизації з 1 січня 2022 року радянські ГОСТи, які діють на теперішній час, втрачають свою чинність.

Таким чином, для вирішення питання гармонізації існуючих застарілих НД, згідно з якими у регіональних метрологічних військових частинах (далі – РМВЧ) проводиться повірка робочих еталонів, що суперечить вимогам статті 27 Закону України №1314-VII (із змінами) "Про метрологію та метрологічну діяльність", відповідно до Програми з військової стандартизації фахівцями військової частини А0785 було розроблено відповідний військовий стандарт (ВСТ) 14.210.031. Розроблений ВСТ установлює вимоги до порядку побудови, змістовності та викладення методик калібрування, з урахуванням вимог до простежуваності еталонів, проведення верифікації (оцінки відповідності) та оформлення відповідного підтверджувального документа відповідно до положень ДСТУ ISO 10012:2005 та вимог ВСТ 03.210.030.

Впровадження стандарту з січня 2021 року обумовлює необхідність планування чіткої координації та прийняття рішень між РМВЧ для визначення термінів та переліку першочергових методик калібрування, що підлягають розробленню.

З іншого боку виникає питання щодо трудоємності, оскільки відповідно до додатку 2 частини 17 Методичних рекомендацій щодо організації наукової та науково-технічної діяльності у ЗС України, в середньому мінімальні орієнтовні витрати часу складають приблизно 70-100 годин на розроблення методики з результатом прикладу проведеного метрологічного підтвердження еталону, що відповідає приблизно 20% від загальних витрат часу на виконання завдань наукового співробітника науково-дослідного відділу військових еталонів. У той же час розподіл календарного фонду робочого часу повірників виробничих підрозділів РМВЧ взагалі не враховує витрат часу на розроблення методик.

Враховуючи вищесказане, заходи якісного розроблення повинні включати в себе як перепідготовку фахівців, які проводять калібрування робочих еталонів, так й корегування процесу професійної підготовки випускників ВВНЗ. Необхідною умовою є не тільки розуміння повної процедури вимірювань, а й наявність теоретичних знань та практичних навичок в статистичній оцінці імовірності досліджень при проведенні процедури метрологічного підтвердження.

Важливим аспектом є недопущення формального підходу під час розроблення методик, оскільки це може призвести до низької якості виконаного завдання та невідповідності вимогам замовника під час верифікації.

Красинський С. В., Ніколенко В. В., Шеховцова І. О.

СТРУКТУРИЗАЦІЯ ПРОБЛЕМИ МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМ КОМПЛЕКСНОЇ БЕЗПЕКИ ОБ`ЄКТІВ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В якості системи комплексної безпеки (СКБ) об’єктів спеціального призначення розглядається складна організаційно-технічна система, яка забезпечує стале протистояння наперед визначеним видам загроз. На теперішній час номенклатура основних вимог до метрологічного забезпечення (МлЗ) СКБ та перелік завдань з його реалізації не унормовані. Авторами здійснено визначення мети, складу, принципів, процесів створення та функціонування системи МлЗ, основні заходи з МлЗ за стадіями життєвого циклу (ЖЦ).

Метою МлЗ СКБ слід вважати створення необхідних умов для отримання достовірної інформації, необхідної і достатньої для оцінювання відповідності СКБ і процесів її функціонування встановленим вимогам, прогнозування та вироблення певних організаційно-технічних рішень щодо можливості подальшого використання. Процеси МлЗ СКБ повинні організовуватися та здійснюватися відповідно до діючих нормативних документів (НД) щодо забезпечення єдності та простежуваності результатів вимірювань, необхідної достовірності їх результатів та НД системи технічного захисту інформації.

До елементів, що складають систему МлЗ СКБ слід відносити: еталони одиниць фізичних величин; засоби вимірювальної техніки, вимірювальні прилади, вимірювальні канали та системи (ЗВТ); програмне забезпечення СКБ, методики (вимірювань, контролю, калібрування, верифікації); виконавців (персонал), які визначають та реалізують метрологічні вимоги до об’єкту вимірювань під час його створення, виконують контроль та вимірювання технічних характеристик (параметрів) процесів та СКБ (складових частин); умови вимірювань, тощо.

Систему МлЗ необхідно розглядати як складову системи матеріально-технічного забезпечення (елементом зінтегрованої логістичної підтримки за термінологією НАТО).

Основний принцип здійснення МлЗ – безперервність протягом ЖЦ СКБ.

Процеси МлЗ СКБ повинні охоплювати: встановлення вимог до показників точності та повноти, достовірності, своєчасності отримання вимірювальної інформації; вибір принципів, методів вимірювань; вибір елементів, які необхідні для реалізації встановлених вимог; валідацію придатності елементів МлЗ СКБ, в тому числі метрологічного підтвердження ЗВТ, метрологічної верифікації методик вимірювань, метрологічної експертизи документації, тощо; підготовчі та допоміжні роботи (дії), які пов’язані з організацією МлЗ СКБ, метрологічного підтвердження придатності елементів МлЗ СКБ і підтримання функціонування СКБ.

Заходи із реалізації процесів МлЗ повинні бути узгоджені за стадіями та етапами з роботами щодо забезпечення надійності СКБ. Узгодженість забезпечують комплексним підходом до розробки програми забезпечення надійності або програми забезпечення якості. Основні завдання з МлЗ на стадіях ЖЦ наведено нижче.

На стадії “Задум” повинно здійснюватися формування концепції МлЗ (визначення варіанта побудови системи контроля технічного стану СКБ (вбудована, зовнішня, комбінована) та загальних вимог до контролепридатності; встановлення загальних вимог до достовірності вимірювальної інформації; техніко-економічне обґрунтування МлЗ; розроблення підрозділу “Вимоги до метрологічного забезпечення” проєкту ТТЗ.

На стадії “Розроблення” повинно здійснюватися визначення переліку параметрів, які підлягають вимірюванню (контролю) під час експлуатування СКБ; обґрунтуван-

ня необхідної точності (достовірності контролю) вимірювання визначених параметрів з урахуванням умов вимірювань (факторів, що впливають); вибір методів та засобів вимірювання (контролю) параметрів з урахуванням вимог до точності (достовірності контролю), можливості їх метрологічного підтверджування, конструктивної та програмної сумісності, ступеня автоматизації, уніфікації та контролепридатності; складання переліків ЗВТ, необхідних для вимірювання (контролю) визначених параметрів під час експлуатування СКБ; обґрунтування необхідності розробки нових методів вимірювань.

В процесі розробки документації на СКБ повинні здійснюватися аналіз прийнятих технічних рішень, їх повнота та достатність для виконання встановлених у ТТЗ метрологічних вимог; остаточне визначення переліку параметрів, які підлягають вимірюванню (контролю) та необхідних ЗВТ; розроблення методик вимірювань параметрів СКБ; встановлення порядку МлЗ СКБ у експлуатаційній документації (ЕД); перевірка виконання вимог щодо МлЗ, які передбачені ТТЗ (ТЗ) на виріб ОВТ.

Під час проведення державних випробувань повинні здійснюватися процеси матеріально-технічного забезпечення випробувань та технічного обслуговування СКБ необхідними ЗВТ; організація проведення метрологічного підтвердження ЗВТ; верифікація, валідація випробувального обладнання, яке відтворює нормовані зовнішні впливаючи фактори; перевірка відповідності одержаних значень параметрів (характеристик) СКБ, які вимірюються (контролюються), визначеним у ТТЗ (ТЗ) та програмі випробувань; проведення метрологічної експертизи документації та її коригування; аналіз виконання організаційно-технічних заходів.

На стадії “Виробництва” повинно здійснюватися проведення організаційних та технічних заходів з МлЗ виробництва СКБ; матеріально-технічне забезпечення процесів контролю, випробувань деталей, вузлів, покупних виробів та матеріалів, виробу в цілому необхідними ЗВТ з урахуванням вимог усталеного виробництва; організація проведення метрологічного підтвердження ЗВТ технологічного процесу; контроль застосування ЗВТ та дотримання встановлених метрологічних норм і правил; формування пропозицій щодо вдосконалення організації МлЗ використання (експлуатування) СКБ.

На стадії “Використання” повинно здійснюватися навчання та допуск персоналу до вимірювань; контроль параметрів СКБ шляхом вимірювань; підтвердження повноти та достатності вимог і положень ЕД щодо методів вимірювань параметрів під час проведення дослідної експлуатації; підготовка пропозицій щодо коригування ЕД, у тому числі щодо необхідності застосування нових ЗВТ та необхідності розробки нових методик вимірювань.

МлЗ СКБ, організоване згідно законодавства України про метрологію та метрологічну діяльність є заставою: забезпечення оперативності, достовірності и повноти контролю параметрів СКБ; формування за результатами контролю параметрів СКБ заходів щодо підтримки СКБ в робочому стані в заданих умовах застосування; визначення показників безпеки методів і засобів вимірювань (технічного діагностування).

Дуболазов Ю. О., Коротій О. О.

ВИКОРИСТАННЯ ІНТЕГРОВАНИХ ПРОГРАМНИХ ЗАСОБІВ ЗАХИСТУ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS ЯК АЛЬТЕРНАТИВА КОМЕРЦІЙНИМ АНТИВІРУСНИМ ПРОДУКТАМ

У сучасних реаліях неможливо уявити користування персональними комп’ютерами (ПЕОМ) без захисту від ураження шкідливими програмами. Існує безліч програмних продуктів (програмного забезпечення), які можуть наносити

шкоду операційній системі та інформації користувача, що зберігається на ПЕОМ. На даний час у силових структурах (наприклад у Міністерстві оборони України) набуло широкого розповсюдження використання програмного забезпечення від ураження ПЕОМ різного виду та модифікацій.

У військових частинах та організаціях Міністерства оборони України переважно використовується операційна система Microsoft Windows 8,10, в базову комплектацію якої входить вбудоване програмне забезпечення для захисту ПЕОМ "Захисник Windows". Тобто, при встановленні та використанні ліцензійних систем Microsoft Windows версій 8,10, користувач отримує базовий рівень захисту інформації на ПЕОМ користувача.

Постає питання достатності базового рівня захисту для виконання функціональних задач користувачами ПЕОМ у силових структурах Міністерства оборони України або одночасного використання вбудованих ("Захисник Windows") та додатково встановлених антивірусних програмних продуктів на одному ПЕОМ.

Цілком зрозуміло що інформація ПЕОМ користувачів, які займають різні посади, піддається загрозам різних рівнів.

Якщо посадова особа використовує під час своєї діяльності мережу інтернет, періодично отримує з мережі файли, то це потенційно підвищує рівень небезпеки, яка загрожує операційній системі "вірусами" та іншим програмним забезпеченням спроможним збирати інформацію про діяльність посадової особи і передавати її зловмисникам. При цьому, якщо ПЕОМ користувачів не мають доступу до глобальної мережі інтернет, а з'єднані локальною мережею, то рівень загроз значно менший і це необхідно усвідомлювати при виборі антивірусної програми.

Особливості, згаданих вище функціональних задач, потребують відповідний рівень захисту. Наприклад, варто відмітити, що для посадових осіб, чия діяльність пов'язана з використанням офісного програмного забезпечення базового рівня захисту повинно бути достатньо, так як вбудований "Захисник" надає захист в "режимі реального часу" тобто постійно ведеться моніторинг підозрілих операцій.

Отже, якщо не порівнювати рівень ефективності захисту від небезпечного програмного забезпечення вбудованого "Захисника" та, наприклад, ESET NOD32, а лише зручність використання, простоту настроювання антивірусної програми, то тут варто виділити інтегрований варіант від Microsoft Windows. Він гармонічно поєднується з операційною системою, не заважає роботі користувача безліччю повідомлень та має зрозумілий інтерфейс. Важливим фактором на користь "Захисника" є незначне використання ресурсів ПЕОМ у порівнянні з антивірусним програмним забезпеченням від інших виробників.

Звичайно будь-який не вбудований антивірус має більші можливості і в цілому надає більш надійний захист операційній системі ПЕОМ. Але, наприклад ESET NOD32 - це комерційний продукт, ліцензія на користування яким потребує окремих фінансових ресурсів. І тут виникає питання - чи потрібен захист комерційного рівня користувачам ПЕОМ, які не мають доступу до глобальної мережі інтернет?

Дзисюк О. В., Бойко В. М., Гаврилов А. Б., Меркулов О. А., Ноженко О. М., Нюкін М. В., Рарог Р. М.

РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ ПІДСИСТЕМИ ЗАБЕЗПЕЧЕННЯ ЄДИНИМ ЧАСОМ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ЗБРОЙНИХ СИЛ УКРАЇНИ

Перехід до мереж зв'язку нового покоління з побудовою єдиного інформаційного простору (формування Єдиної автоматизованої системи управління Збройних Сил

(ЗС) України - C4ISR) та інтеграція до неї автоматизованих систем усіх видів та спеціальних військ, у якому послуги зв'язку доповнюються іншими послугами обробки інформації, такими як: накопичення, зберігання, обробка та пошук необхідної інформації, зумовлює використання асинхронних технологій передачі даних – Ethernet (у збройних силах країн-партнерів це так званий тактичний інтернет).

Однією з найважливіших вимог до автоматизованих систем управління, побудованих на основі сучасних цифрових систем зв'язку, є підтримка в комп'ютерному середовищі єдиного часу, синхронізованого зі шкалою всесвітнього координованого часу. Для реалізації в комп'ютерному середовищі єдиного часу за допомогою програмно-апаратних засобів на практиці створюються сервери часу, що забезпечують часо-частотну синхронізацію із точним зовнішнім еталоном часу UTC.

Як показують останні дослідження, з урахуванням специфіки роботи пакетних мереж, у якості перспективного методу синхронізації у збройних силах країн НАТО застосовуються двосторонні мережеві протоколи – NTP (Network Time Protocol) та PTP (Precision Time Protocol). При цьому, в останні роки переваги набув протокол PTP (стандарт IEEE 1588v2, 2008 року), який забезпечує більш високу точність та в більшій мірі адаптований під завдання, що вирішуються із застосуванням інформаційно-телекомунікаційних мереж. Зрозуміло, що при розбудові військового сегмента Служби єдиного часу та еталонних частот на перший план виходять завдання як побудови системи передавання еталонних сигналів часу та частоти, так і створення відповідної системи контролю точностних характеристик.

У цьому напрямку на базі Метрологічного центру військових еталонів ЗС України та ННЦ "Інститут Метрології" (м. Харків) були проведені експериментальні дослідження та здійснена практична (апаратна та програмна) реалізація (тестування) синхронізації шкали часу між Національним еталоном одиниць часу і частоти (ВЕТУ 07-01-03-10), Вихідним еталоном ЗС України (ВЕЗСУ 07-01-01-09) та військовими споживачами (м. Київ) шляхом передавання еталонних сигналів часу та частоти пакетними мережами за допомогою протоколу PTP IEEE 1588v2. Для транспортування цифрових сигналів синхронізації була побудована оптоволоконна мережа між Харковом та Києвом.

Авторами у доповіді висвітлені основні результати цих досліджень:

- здійснена дослідна експлуатація апаратно-програмних засобів синхронізації (прив'язки шкал часу) військових споживачів та створена перша черга підсистеми забезпечення єдиним часом інформаційно-телекомунікаційних систем ЗС України (із синхронізацією Головного інформаційного телекомунікаційного вузла ЗС України з національним еталоном часу та частоти);
- розроблена модель системи метрологічного контролю та управління еталонними сигналами, що використовуються ЗС України;
- обґрунтовані пропозиції щодо складу технічної складової системи метрологічного контролю та управління еталонними сигналами, що використовуються ЗС України;
- досліджені наявні потреби та розроблені пропозиції щодо складу нормативного забезпечення системи метрологічного контролю та управління еталонними сигналами.

Котова М. А., Каревік О. О.

СПОСІБ АВТОМАТИЗОВАНОЇ ПОВІРКИ ВИСОКООМНИХ МАГАЗИНІВ ЕЛЕКТРИЧНОГО ОПОРУ

На даний час у Збройних Силах (ЗС) України та інших військових формуваннях експлуатується великий парк високоомних магазинів електричного опору (типів

Р4002, Р4047, Р4057, Р4075, Р4076, Р4077, Р4078, Р40105, Р40106, Р40107, Р40108, тощо), за допомогою яких здійснюється метрологічне обслуговування комбінованих електровимірювальних приладів, універсальних аналогових та цифрових вольтметрів, мегомметрів, вимірювачів електричного опору ізоляції різноманітних типів. Зазначені засоби вимірювальної техніки (ЗВТ) широко застосовуються для перевірки дотримання умов техніки безпеки при експлуатації військових електроустановок, силових кабелів та мереж живлення, а також контролю параметрів зразків озброєння та військової техніки (ОВТ) на всіх етапах їх життєвого циклу. Тому рівень метрологічного обслуговування еталонних магазинів великого електричного опору безпосередньо впливає на надійність та якість функціонування багатьох технічних систем у ЗС України.

У теперішній час повірка високоомних магазинів опору у діапазоні номінальних значень від $1 \cdot 10^4$ Ом до $1 \cdot 10^9$ Ом здійснюється методом заміщення з використанням еталонних однозначних мір електричного опору (ОМЕО) 2-го розряду та мостової установки типу У401. Процес повірки характеризується великою трудомісткістю, яка зумовлена технічно застарілою конструкцією установки У401, що не дозволяє здійснити автоматизацію процесу вимірювань, обробки та реєстрації результатів вимірювань. Більш досконалих аналогів на даний час установка У401 не має, в зв'язку з чим, існує необхідність у розробці альтернативних методів повірки високоомних магазинів електричного опору з використанням інших типів сучасних ЗВТ.

У доповіді розглядається спосіб повірки магазинів великого електричного опору, який реалізується за допомогою двох еталонних ОМЕО 2-го розряду (ОМЕО 1 та ОМЕО 2), калібратора постійної напруги та 6½ розрядного цифрового мультиметра (ЦМ) типу Agilent 34401A, з'єднаного за допомогою дистанційного інтерфейсу з персональним комп'ютером (ПК). Процес повірки здійснюється шляхом вимірювання цифровим мультиметром падіння напруги на еталонній ОМЕО 1 при почерговому підключенні до неї спочатку еталонної ОМЕО 2, а потім – ступеня декади магазина опору, дійсне значення якого визначається. Вимірювання падіння напруг проводиться при незмінному значенні вихідної напруги калібратора, до якого почергово підключаються послідовно з'єднані ОМЕО 1 і ОМЕО 2 та ОМЕО 1 і ступінь декади магазина опору, яка перевіряється. На основі одержаних ЦМ результатів вимірюваннь та апріорних даних щодо дійсних значень електричного опору еталонних ОМЕО 1 та ОМЕО 2, ПК, за встановленим алгоритмом, з використанням спеціально розробленого програмного забезпечення, розраховує дійсні значення електричного опору ступенів декад магазина опору та формує протокол повірки. Запропонований спосіб повірки дозволяє підвищити рівень метрологічного обслуговування магазинів великого електричного опору різноманітних типів шляхом зменшення трудомісткості та підвищення оперативності процесу вимірювань і обробки результатів вимірювань.

УДК 331.103.3

Метешкін К. О., Русскін В. М.

МОДЕЛЬ РЕЙТИНГОВОГО ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ РОБОТИ ВИКЛАДАЧІВ ТА ПІДРОЗДІЛІВ ЗАКЛАДУ ВИЩОЇ ОСВІТИ

Запропоновано методику рейтингового оцінювання результатів роботи викладачів закладу вищої освіти, яка сприяє системності й результативності показників діяльності викладачів, підвищенню продуктивності праці й конкурентоспроможності працівників, формуванню конкурентоспроможного середовища у навчальному закладі, підвищенню конкурентоспроможності самого закладу вищої освіти.

Сучасні вимоги цифрової трансформації в освітній сфері держави зумовили ство-

рення рейтингових систем в університетах. Багато вчених і інженери намагаються побудувати всеохоплюючу систему рейтингування, починаючи від інженера лабораторії і закінчуючи деканами та проректорами. На цьому шляху, на жаль, зустрічаються значні труднощі, пов'язані з великою кількістю показників функціонування такого складного механізму, як вищий навчальний заклад. В даний час з'являються роботи, спрямовані на створення "розумних вузів" [1, 2], що використовують концепцію управлінням навчанням і освітою на основі інтегрованого інтелекту [3].

Метою створення моделі системи рейтингування на основі інтегрованого інтелекту є дослідження процесу оцінювання, як суб'єктів (осіб, які беруть педагогічні рішення), так і структурних підрозділів ВНЗ. Крім того, система рейтингування має мотивувати основних учасників навчального процесу і забезпечувати реалізацію таких принципів, як відкритість, достовірність, надійність, гнучкість, своєчасність (в реальному масштабі часу) отримання результатів оцінювання.

У дослідженні зі створення рейтингової системи використовувалися методи як технічних наук, наприклад, теорії прийняття рішень, кібернетичної педагогіки, методи побудови інтелектуальних інформаційних технологій, кластеризації та ін., А також і методи психології - теорії особистості, корисності і ін.

Так як кафедра в Законі про вищу освіту України вважається основним підрозділом, то і її особовий склад вважатимемо ядром, яке піддається оцінюванню. В даному ядрі виділяється три групи суб'єктів А - група асистентів і викладачів, які мають невеликий педагогічний стаж до 2 років, D - група старших викладачів і доцентів і група Р - група професорів, включаючи завідувача кафедрою. Серед суб'єктів виділених груп Закон про вищу освіту передбачає систему переваг. Іншими словами, систему кар'єрного росту.

Для суб'єктів група А краще бачити себе в групі D, а суб'єкти цієї групи вважають за краще знаходитися в групі Р. Тоді можна в формальному вигляді записати функцію корисності де $Q[0, t_4^г] \rightarrow (\mathrm{A} \succ D \succ P \succ P^*), [0, t_4^г]$ повний інтервал часу плідної професійної діяльності науково-педагогічного працівника (НПП), а P^*- завідувач кафедри (див. рис.1). Маючи список показників професійної діяльності НПП і вагові коефіцієнти відповідних дій можна побудувати функції корисності для кожного учасника навчального процесу і порівнювати їх між собою. Організація бінарного порівняння вагових коефіцієнтів дозволяє їх ранжувати і знайти максимальні і мінімальні значення сумарних і інтегральних показників і виявити кращих серед груп А, D і Р.

Пропонується виділити з групи D три НПП, у яких кращі показники і порівнювати їх з кращими трьома з інших кафедр, тим самим виявляти кращого доцента, і за аналогією професора серед безлічі кафедр і факультетів. За аналогією виявляються кращий завідувач кафедри серед кафедр факультету та вузу в цілому.

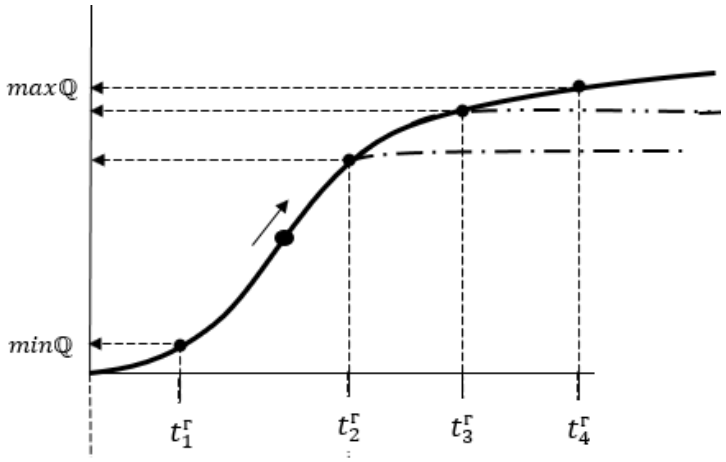


Рисунок 1 - Функція корисності, побудована на основі конкретних даних професора з педагогічним стажем в 30 років

Покажемо фрагмент моделі рейтингування з деякими обмеженнями і припущеннями, а саме, введення в модель для ілюстрації та візуалізації гіпотетичного асистент (ГА) і гіпотетичного доцента (ГД) (див. рис. 2).

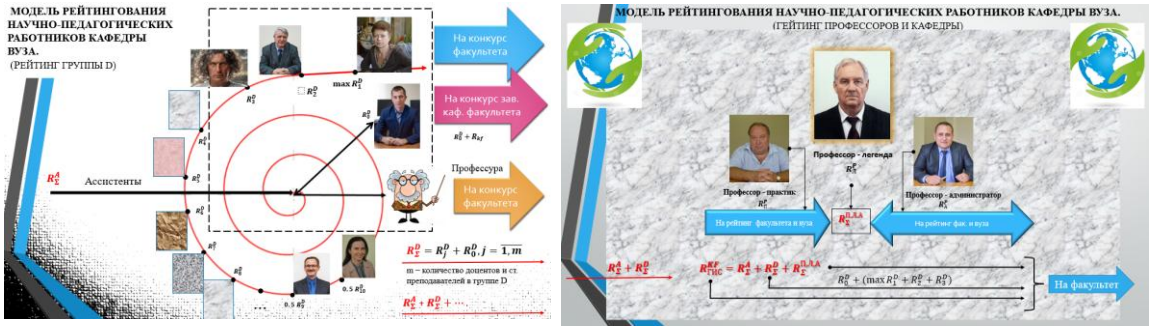


Рисунок 2 - Фрагменти інтерфейсу моделі системи рейтингування НПП

На рисунку 2 не показані фрагменти інтерфейсу з асистентами кафедри.

Таким чином, запропонована модель рейтингування НПП і підрозділів вузу, яка на думку авторів мотивує НПП кафедри до плідної та ефективної професійної діяльності, сприяє формуванню конкурентоспроможного середовища у навчальному закладі, підвищенню конкурентоспроможності самого закладу вищої освіти.

Список літератури

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

2. Метешкін К. О. Концептуальні положення створення геоінформаційної системи “Розумний вищий навчальний заклад” // К.О. Метешкін, Л. О. Маслій. Комунальне господарство міст / науково-технічний збірник, вип.5 (151), 2019. С. 54-59.

3. Метешкин К. А. Кибернетическая педагогика: теоретические основы управления образованием на базе интегрированного интеллекта. Монография. – Харьков: Международный Славянский университет, 2004. – 400 с.

Palamarchuk N., Bondarenko T., Tsymbal I.

APPROACHES TO THE ANALYSIS OF THE RELIABILITY AND SECURITY OF WEBSITES ON THE INTERNET

The Internet has become an integral part of the modern world. In Ukraine, as in other countries, together with the development of communication technologies and their implementation in all areas of activity, security issues related to the use of the Internet (web portals, websites, web pages (base unit) are actively discussed. Internet resource), file servers, social networks, e-mail, etc.).

The current level of computerization of society makes the vast field of information accessible to anyone from anywhere on the planet. Every average Internet user can both receive information from the network and post there almost anything he wants. This is a huge advantage of the resource, but it can be a great danger of its unlimited, illegible, and sometimes unconscious use. Often, users trust the Internet too much, mistakenly believe that the information is valuable and accurate, they have no doubts about the accuracy of the information and the honesty of the authors. In this case, not the least role is played by previous experience of using reliable printed sources of information (textbooks, manuals, official

publications), which is transferred to all other modern sources of information [2, 4].

Knowing and using the basics of evaluating information from the Internet can help you take a more informed approach to using it. There are various tools and services for assessing the reliability of sites. The average user is encouraged to follow this strategy - first learn to distinguish between formal criteria for site reliability, ie signs that do not require careful reading and analysis of the text of the article (feedback from the author; information about the author's qualification; formal signs of URL reliability; dates of site creation, placement of materials and updates; the presence of grammatical and spelling errors, etc.), and then, determining the high probability of reliability of the site on formal grounds, apply critical thinking skills (thinking skills of higher levels according to B. Bloom) for more detailed in-depth analysis (detection of distorted, "curved" logic; violations of logic; detection of facts and their interpretation; detection of articles with advertising, etc.) [3, 4].

Many users sometimes ask for additional verification, using technical tools (there are dozens of free tools and services that have their advantages and disadvantages): built-in security technology to view downloads and check the reputation of websites in Chrome, Firefox, Internet Explorer etc; security services Google Safe Browsing, Web of Trust (WoT), McAfee WebAdvisor, Comodo Web Inspector, etc. [3].

Speaking of connecting corporate information systems to the Internet, there is no doubt about the significant benefits of access to a huge amount of resources contained on web-sites (web-pages) and simplification of the procedure, including international. Maintaining the information resource of web-pages requires appropriate protection, and the user - confidence in the accuracy of information. A successful attack can lead to partial or complete blocking of the web-site, loss of information, violation of its integrity. After large-scale cyberattacks, such as WannaCry and Petya, which caused billions in damage, the importance of protecting information has become paramount.

According to the legislation of Ukraine, protection of information of web-pages is realized by creation and introduction of the complex system of protection of information (with the confirmed conformity) which should provide protection of publicly available information of web-pages (requirements concerning integrity and accessibility) and technological information (requirements concerning confidentiality and integrity). , the protection requirements of which differ. Also, when creating a web-page and determining the operator to connect to the network, you must take into account that to protect against external threats, the connection to the Internet must be made using a secure access node that has a certificate of compliance [1] .

Thus, the average user, along with the need to have modern computer technology, it is advisable to evaluate web resources using formal criteria and critical thinking skills. And the problem of protecting the information of web-pages can be solved by applying an integrated approach, when the protection, in addition to the known subsystems of access delimitation, integrity control can include a subsystem of analysis and detection of intrusions, which will focus further research.

References

1. ND TZI 2.5-010-03 Vymohy do zakhystu informatsii WEB-storinky vid nesanktsionovanoho dostupu, zatverdzheno nakazom DSTSZI SB Ukrainy vid 02.04. 2003 r. № 33 (zi zminamy).

2. Felechko O.S. Veb-sait: vid poniattia do stvorennia ta funktsionuvannia. Materialy druhoi mizhnarodnoi shchorichnoi konferentsii IT pravo: problemy i perspektyvy rozvytku v Ukraini). [Elektronnyi resurs]. – Rezhym dostupu: http://aphd.ua/publication-363/.

3. Yak pereviryty sait na nadiinist. [Elektronnyi resurs]. – Rezhym dostupu: https://naukovistudii.org.ua/7119/.

4. Dementiievska N.P. Formuvannia navychok krytychnoho otsiniuvannia veb-resursiv i

problema bezpeky uchniv v interneti. [Elektronnyi resurs]. – Rezhym dostupu: http://lib.iitta.gov.ua/709804/1/Dementievska_Crit_oc.pdf.

Паламарчук С. А., Овсянніков В. В., Черниш Ю. О.

ЗАДАЧІ З ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Функціонування об'єктів критичної інфраструктури (ОКІ) в такому специфічному середовищі, як кіберпростір, пов'язане з уразливістю і загрозами і вимагає розробки нового інструментарію. Поряд з інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Неодмінною умовою вирішення питань щодо забезпечення інформаційної та кібербезпеки ОКІ є розуміння того, що держава знаходиться в нерозривному зв'язку і взаємодії з іншими структурами і суб'єктами, що відображається законодавчими, організаційними та технічними (технологічними) аспектами/рівнями взаємодії. В межах вказаних аспектів пропонуються наступні задачі з вдосконалення інформаційної та кібернетичної безпеки ОКІ [1, 2]:

1) розробка та прийняття національних нормативних документів:
- Переліку об'єктів критичної інфраструктури держави;
- Плану заходів щодо реалізації Стратегії кібербезпеки України;
- Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) ОКІ під час попередження, виявлення, припинення кібератак та кіберінцидентів.

2) організаційне узгодження діяльності суб'єктів забезпечення інформаційної та кібернетичної безпеки ОКІ, а саме:
- розробка відомчих документів щодо визначення вимог до кіберзахисту ОКІ;
- визначення повноважень посадових осіб (введення підрозділів), відповідальних за забезпечення інформаційної та кібернетичної безпеки;
- визначення порядку ведення та використання державного реєстру кіберінцидентів.

3) технічне забезпечення інформаційної та кібернетичної безпеки ОКІ:
- створення систем забезпечення безпеки ОКІ згідно нормативних (відомчих) документів;
- визначення показників забезпечення інформаційної та кібернетичної безпеки ОКІ;
- адаптація засобів управління інформацією і подіями безпеки відповідним вимогам;
- формалізація підходів керування ОКІ з врахуванням вимог відомчих документів (на прикладі вимог визначених в [3]).

Отже, комплексна реалізація зазначених задач дозволить забезпечити ефективну інформаційну та кібернетичну безпеку ОКІ шляхом виконання низки правових, організаційних, технічних, наукових заходів, всебічного забезпечення на національному та відомчому рівнях. Подальші дослідження доцільно спрямувати на оцінювання організаційних та технічних аспектів функціонування відомчого ОКІ, з метою повноцінного виконання вимог кіберзахисту та кібербезпеки.

Список літератури

1. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 "Про за-

твердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури”.

2. Мартинюк В.В., Паламарчук Н.А., Паламарчук С.А., Сівоха О.М. Задачі вдосконалення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури. Збірник наукових праць ВІТІ, № 2, 2020, стор. 54-63.

3. Постанова Правління Національного банку України від 28.09.2017 року № 95 “Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України” [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0095500-17.

Черниш Ю. О., Мальцева І. Р., Паламарчук С. А., Ткач В. О.

ЕЛЕКТРОННА ВЗАЄМОДІЯ ТА ЕЛЕКТРОННА ІДЕНДИФІКАЦІЯ ЯК ОСНОВА СУЧАСНОЇ ДІЯЛЬНОСТІ

Електронний документообіг та електронні послуги (сервіси) є сталою платформою всіх організацій в сучасному світі як забезпечуючого сервісу громадян так і функціонування органів державної влади, в тому числі, і військових формувань, які мають складні ієрархічно підпорядковані/взаємодіючі структури, та які знаходяться на шляху створення інформаційно-телекомунікаційних систем. Основою таких систем є система електронної взаємодії, яка повинна базуватися на існуючих телекомунікаційних мережах із застосуванням сучасних засобів захисту інформації [1, 2].

Захищена система, має включати механізми автентифікації користувачів та реєстрацію їх дій, розмежування доступу, забезпечення збереженості та достовірності документів, тощо. Актуальність впровадження захищених інформаційно-телекомунікаційних систем безперечна.

Шлях України в питаннях цифрової трансформації досі має ряд гальмівних тенденцій: неузгодженність технічних платформ, “привязка до паперового дублювання”, відсутність механізмів забезпечення належно захищених та інтероперабельних платформ для електронної взаємодії. На фоні створення систем обміну електронними даними одним із не вирішених залишається питання електронної ідентифікації для системної та міжсистемної взаємодії, що має ряд проблемних питань, основні з яких [4]:

- несформованість нормативно-правової бази, що регулює сферу електронної ідентифікації;
- відсутність єдиної нормативної та технічної політики використання та захисту ідентифікаційних даних користувачів;
- відсутність єдиних технічних вимог до застосування альтернативних схем електронної ідентифікації під час надання різних електронних послуг;
- неузгодженість у виборі ідентифікаторів користувачів та брак їх адекватної верифікації;
- використання в інформаційних системах технологічно несумісних засобів та схем електронної ідентифікації та автентифікації.

На сьогодні основним і практично єдиним із запропонованих на ринку механізмом реалізації захисту є електронний підпис, принцип роботи якого заснований на використанні стандартів шифрування за допомогою відкритого ключа.

Закон України “Про електронні довірчі послуги”, що набув чинності 07.11 2018 року більше нагадує технічний норматив, ніж, власне, закон [1, 2]. Одним з найважливіших його положень є взаємне визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів. Законом запровадились такі

механізми, як електронна ідентифікація, електронний підпис, електронна печатка, електронна позначка часу, реєстрована електронна доставка, інтероперабельність тощо. Схема електронної ідентифікації буде встановлювати високий (використання кваліфікованих електронних підписів і печаток), середній (використання вдосконалених електронних підписів і печаток) або низький рівень довіри до використовуваних засобів електронної ідентифікації. Варто зазначити, що Закон загалом інтегрує в собі всі попередні здобутки у сфері застосування електронного цифрового підпису, бо створює базу унікальних цифрових "ключів", які закріплені за кожним суб'єктом відносин.

В цілому, розвиток електронної ідентифікації та довірчих послуг дасть змогу:

- запровадити повноцінну системи електронної взаємодії органів державної влади;
- сприяти розвитку електронної взаємодії базових державних реєстрів і баз даних, центрів надання адміністративних послуг;
- забезпечити зручний та безпечний доступ громадян та суб'єктів господарювання до визначених даних з інформаційних систем органів державної влади, різноманітних електронних послуг та інтерактивних інструментів без необхідності використання декількох облікових записів в різних інформаційних системах;
- сприяти розвитку електронних форм взаємодії громадян та держави та загалом, встановить рівень довіри до електронних послуг "сервісної" держави.

Список літератури

1. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 р. (зі змінами).
2. Закон України "Про електронні довірчі послуги" від 05 жовтня 2017 р.
3. Регламент ЄС №910/2014 Європейського Парламенту та Ради від 23.07.14 "Про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку і скасування Директиви 1999/93/ЄС".
4. Розпорядження Кабінету Міністрів України від 20.09.17 р. № 649-р. "Про схвалення Концепції розвитку електронного урядування в Україні".

Овсянніков В. В., Паламарчук С. А., Паламарчук Н. А., Побережець Т. В.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В БЕЗПРОВОДОВИХ МЕРЕЖАХ

При побудові бездротових мереж однією з найбільш гострих проблем є забезпечення їх безпеки. Принцип передачі інформації в безпроводових мережах зумовлює складність забезпечення захисту інформації та кібербезпеки в них: незахищений характер та відкритість бездротового середовища передачі; вразливості, пов'язані з мобільністю пристроїв користувачів, мобільністю сервісів та застосувань; розподіленістю, змінами у топології; недоліками або помилками під час проектування протоколів (наприклад WEP); принциповою неможливістю реалізації деяких механізмів безпеки через структурні особливості безпроводових мереж; наявністю специфічних технічних обмежень [2].

Безпека кожної безпроводової мережі в значній мірі залежить від того, наскільки кожен компонент безпроводової мережі, включаючи клієнтські пристрої, точки доступу та безпроводові комутатори захищений протягом усього життєвого циклу мережі, починаючи від первинного проектування, розгортання, технічного обслуговування та моніторингу. Головна відмінність між провідними і бездротовими мережа-

ми пов’язана з наявністю неконтрольованої області між кінцевими точками бездротової мережі. Це дозволяє атакуючим, що знаходяться в безпосередній близькості від бездротових структур, виробляти цілий ряд нападів, які неможливі в дротовому світі та реалізовувати відповідні загрози безпеці інформації [1, 3].

Загалом, безпроводова мережа, як об’єкт захисту являє собою організаційно-технічну систему, що об’єднує фізичне середовище, програмне забезпечення (обчислювальну систему), середовище користувачів (персонал), оброблювану інформацію і технологію її обробки в мережі (середовища функціонування). Принцип дії бездротової мережі призводить до виникнення великої кількості можливих вразливостей для атак і проникнень. Атаки, спрямовані на порушення безпеки, в тому числі і бездротових мереж, діляться на активні (підміна адреси, повтор, модифікація повідомлення і відмова в обслуговуванні) і пасивні (перехоплення даних, застосування аналізатора трафіку) [1]. Для адміністратора неможливо встановити факт пасивної атаки.

Виходячи з призначення безпроводових мереж та завдань, які покладаються на них, загрози безпеці становлять загрози доступності, конфіденційності, цілісності та автентичності даних. Забезпечення безпеки інформації в безпроводових мережах повинне виконуватись за допомогою реалізації наступних послуг безпеки:

- конфіденційності, цілісності, доступності та автентичності інформаційних ресурсів, які циркулюють в безпроводових мережах;
- причетності до відправлення або прийняття інформаційних ресурсів, які циркулюють у мережах.

Ступінь надійності реалізації цих послуг визначається рівнем безпеки протоколів, які реалізують вказані вище послуги. Вимоги до функціонального складу комплексу захисту інформації залежать від характеристик оброблюваної інформації, програмного забезпечення, фізичного середовища, персоналу, технології обробки і організаційної підсистеми. Вимоги до гарантій визначаються характером (важливістю) оброблюваної інформації і призначенням безпроводової мережі.

Слід визнати, що для визначення вимог до захисту інформації в безпроводових мережах, які найповніше відповідають характеристикам і вимогам конкретної мережі, необхідне проведення якісного обстеження середовищ функціонування мережі з метою підготовки вихідних даних для формування вимог до захисту інформації та розробки функціонального профілю захищеності. Функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинна реалізовувати система захисту інформації в безпроводових мережах щоб задовольняти певні вимоги щодо захищеності інформації, яка циркулює в даній мережі. Перелік функціональних послуг безпеки та рівнів гарантій, їх структура і семантичне позначення наведені у нормативних документах щодо захисту інформації: НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99; НД ТЗІ 3.7-003-05; МСЭ-Т X.501; МСЭ-Т “Обзор технологий в области безопасности сетей”; МСЭ-R F.2058, МСЭ Т X.509; T-REC-X.1154; МСЭ -Т Y.2705; МСЭ Т Y.2720; ИСО/МЭК 9594-8-98; ИСО МЭК 27001 тощо.

Список літератури

1. NIST 800-153. Вказівки щодо захисту локальної бездротової мережі. Рекомендації Національного інституту стандартів і технології, Міністерство торгівлі США, Гейтерсбург, 2012 р.

2. Сергій Гладиш. Превентивні та реактивні механізми безпеки в бездротових традиційних та Ad-Hoc мережах. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 1(18) вип., 2009 р. стор. 109-116.

3. Панська А.В., Резніченко В.А. Загрози та вразливості бездротових мереж. Матеріали Всеукраїнської науково-практичної конференції. “Актуальні задачі та досягнення у галузі кібербезпеки”, 23-25 листопада 2016 року, м. Кропивницький, стор. 146-147.

Каук В. І., Павлов С. П.

СИСТЕМА УПРАВЛІННЯ ОСВІТНІМ ПРОЦЕСОМ ТА КОНТРОЛЮ ЯКОСТІ НАВЧАННЯ НА ОСНОВІ LMS MOODLE

Добре відома безкоштовна система управління освітнім процесом LMS Moodle, містить досить велику кількість можливостей для побудови сучасного освітнього процесу не тільки як в електронній або змішаній формах навчання, а і для підтримки звичайного денного навчання.

На основні такої системи створюється повноцінний інформаційний простір, у якому кожен із учасників освітнього процесу має постійний доступ до інформаційних матеріалів і може захищено спілкуватися між собою. Система також передбачає можливості повного адміністрування користувачів з наданням їм відповідних функцій та ролей від адміністратора та викладача до асистента та студента. В системі також присутня роль "куратора категорій", користувачі якої можуть здійснювати постійний моніторинг всіх дистанційних курсів певної категорії.

Такими категоріями можуть бути: факультет, кафедра, семестр, форма навчання та інше. Слід враховувати що якщо куратор категорії підписаний тільки до категорії і не підписаний до певного дистанційного курсу, то викладачі та студенти дистанційного курсу навіть не бачать хто може моніторити їх діяльність.

Таким чином можливо налагодити процес простого моніторингу діяльності за кожним курсом або категорією.

Крім цього в системі є можливість вводити навчальні плани, для того щоб формувати певні програми навчання. До кожного дистанційного курсу можна також додавати перелік компетентностей, які студент має отримати на цьому дистанційному курсі (назва із загально введеної бази даних, відсоток оволодіння певною компетентністю). Викладач на власному дистанційному курсі може керувати компетентностями за допомогою будь-якого оцінюємого елементу курсу. Тобто, якщо студент виконав завдання на певну кількість балів, то це дає йому можливість оволодіння компетентністю на певний відсоток.

Таким чином можна повністю контролювати наступні питання: чи покриті всі компетентності у навчальному плані, чи дублюються та перекриваються компетентності у різних навчальних дисциплінах (дистанційних курсах), чи може студент набрати 100 % компетентності, вивчивши певну кількість навчальних дисциплін. Адміністратор або куратор категорії завжди може бачити зведений план навчання та той відсоток компетентностей що набрав студент під час навчання. Це дуже цікаві дані для подальшої освітньої аналітики.

В системі є можливість вести студентів у глобальних та локальних академічних групах. Є можливість формування потоків. Крім цього кожен викладач може на власному курсі формувати будь-які групи. Це дуже доречно, коли мова йде про так звані альтернативні навчальні дисципліни. Гнучка система формування груп та потоків дозволяє у повній мірі формувати індивідуальні освітні траєкторії для кожного студента. В системі також є можливість самостійного дозаписування студентів на курс, що стає могутнім інструментом для дійсно вільного вибору тих навчальних дисциплін, які по справжньому цікавлять студента.

Вбудованим функціоналом є наявність сучасного журналу відвідувань та журналу оцінок. При дуже легкому налаштуванні журнал відвідувань дозволяє студентам самостійно (або за допомогою викладача) відмічатися у журналі. Вбудовані механізми захисту (автентифікація за корпоративною адресою, пароль, певний QR-код, доступ тільки з певних адрес wifi мережі) дозволяють уникнути моментів, коли за студента

відмічається інший студент. Для додаткової мотивації викладач може оцінити присутність студента, як окрему активність (і вона автоматично додається до журналу оцінок). Потім при аналізі можна дуже легко вивантажити журнал відвідувань у форматі MS Excel. Передбачені всі можливі види фільтрації (за прізвищем, за групою).

Крім цього у системі є дуже потужна статистика за кожним користувачем, яка дозоляє проаналізувати коли був користувач, що він робив у системі, скільки часу він провів виконуючи ту чи іншу активність, що він надав у якості виконаного завдання, коли це завдання було перевірено та інше.

Таким чином можна повністю перейти до електронного журналу відвідувань з подальшим аналізом того, які види занять найбільш затребувані, які види навчальних матеріалів викликають більшу цікавість, як саме викладач проводить навчання.

Дуже потужним інструментом є журнал оцінювання. Його можливості налаштувань дозволяють зводити у категорії оцінок певні групи оцінок. Це може бути такі категорії: контрольна точка, практичні заняття, тести, змістовні модулі та інші. Налаштування також дозволяють за різними алгоритмами обчислення завжди приводити реальну оцінку до 100-бальної та літерної шкал оцінювання. Студенти завжди можуть бачити як саму модель оцінювання (з чого складається оцінка), яка має відповідати силабусу навчальної дисципліни, так і власну поточну оцінку (в тому числі власний прогрес навчання, тобто скільки у відсотках набрано балів або пройдено елементів дистанційного курсу).

Вбудовані можливості анкетування та опитування дають змогу постійно проводити опитування серед студентів щодо якості освітнього процесу. В системі є вбудовані анкетні опитування, а також можливість гнучко створювати будь-які (анонімні та персональні) опитування. Це дуже зручних механізм для того щоб системно (незалежно від викладача) збирати думки всіх учасників освітнього процесу.

Таким чином LMS Moodle є сучасною інформаційною системою, яка дозволяє організувати, моніторити та контролювати освітній процес, який повністю або частково відбувається у Інтернет. Оволодіння такою системою є дуже простим і не потребує багато часу та коштів.

УДК 378.14

Каук В. І., Гребенюк В. О.

ІНТЕГРАЦІЯ СЕРВІСІВ GOOGLE ТА LMS MOODLE

Майже всі ЗВО України використовують LMS Moodle у якості платформи для організації електронного або змішаного навчання. Ця система постійно розвивається та містить у собі потужні механізми інтеграції з іншими веб-сервісами. Деяка інтеграція можлива за рахунок вбудованої функціональності (наприклад H5P) або за рахунок встановлення додаткових модулів(плагінів) (наприклад сервіс віддаленої автоматичної перевірки програмних кодів). Також можна проводити інтеграцію на системному рівні (загальна система аутентифікації, сховища. вбудованих посилань та інше).

Компанія Google пропонує для освітніх організацій безкоштовну підписку Google Workspace for Education Fundamentals (попередня назва G Suite for Education). Більш детальну інформацію можна отримати за посиланням:

https://edu.google.com/products/workspace-for-education/education-fundamentals/.

Така підписка містить суттєві переваги: можливість проводити з відео-записом зустрічі в Google Meet до 100 учасників без обмеження часу, необмежений Google Drive для кожного співробітника та студента освітньої організації та інші.

В ХНУРЕ реалізована інтеграція сервісів Google та LMS Moodle на повному системному рівні. Це означає що кожен співробітник та студент ХНУРЕ має власний корпоративний аккаунт в домені *@nure.ua, за допомогою якого він авторизується на платформі електронного навчання. Інтегрована також автоматична розсилка електронних листів для всіх учасників освітнього процесу. При відповідних налаштування студенти та викладачі отримують повідомлення щодо занять, отриманих завдань, виконаних тестів, отримання оцінки та коментарів. Є шлях інтеграції до внутрішньої системи розкладу, коли кожен викладач має можливість власних розклад спочатку додати до Google Calendar, а потім синхронізувати такий календар із календарем власного дистанційного курсу у системі.

Є також взаємна інтеграція щодо демонстрації на платформі Moodle різноманітних електронних матеріалів (Google Slides, Youtube video та інше). Викладач має змогу гнучко розміщувати необхідну інформацію на Google Drive, а потім використовувати у системі лише посилання на ці файли.

Нещодавно до системи електронного навчання була додана можливість використання функціональності Google Assignments. Це дає можливість зберігати завдання отримані від студентів на необмеженому Google Drive викладача.

Таким чином інтеграція таких могутніх та безкоштовних веб-сервісів дає викладачеві нові можливості зі створення та використання сучасних електронних засобів навчання.

УДК 378.14

Каук В. І., Пуголовок К. М.

ЗАБЕЗПЕЧЕННЯ ТЕХНОЛОГІЙ ЕЛЕКТРОННОГО НАВЧАННЯ У ПОЛЬОВИХ УМОВАХ

Як правило немає проблем при використанні LMS Moodle, якщо є повноцінна інформаційна інфраструктура: комп'ютери, мережа, надійний доступ до Інтернет та веб-сервісів. При забезпечення діяльності силових структур іноді виникають завдання щодо забезпечення якісного електронного навчання в умовах з суттєвими обмеженнями можливостей (наприклад польові умови тренувальних таборів). Якщо розглядати таки обмеження, то можна їх поділити на різні за обмеженностями рівні:

- немає стабільного Інтернет, але є локальна мережа та комп'ютери;
- немає комп'ютерів;
- обмежена можливість навіть щодо електроживлення.

Для кожного з цих рівнів можуть бути окремі рішення. Далі будемо розглядати єдине мобільне рішення, яке може обійти всі ці обмеження. Система електронного навчання (на основі LMS Moodle) розгорнута на пристрої Raspberry Pi 4 (https://www.raspberrypi.org/products/raspberry-pi-4-model-b). Такий пристрій має наступну специфікацію:

- Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz;
- 2GB, 4GB or 8GB LPDDR4-3200 SDRAM (depending on model);
- 2.4 GHz and 5.0 GHz IEEE 802.11ac wireless, Bluetooth 5.0, BLE;
- Gigabit Ethernet;
- Operating temperature: 0 – 50 degrees C ambient;
- A good quality 2.5A power supply can be used if downstream USB peripherals consume less than 500mA in total.

Вартість такого пристрою в Україні від 2 500 грн. Він може працювати від мобільного акумулятору та містить в собі точку підключення wifi, яка підтримує від 10

до 20 підключень одночасно.

Замінити комп'ютери можливо на сучасні смартфони, на які можливо встановити відповідний мобільний додаток Moodle:

https://play.google.com/store/apps/details?id=com.moodle.moodlemobile.

У підсумку ми отримуємо мобільну інформаційну систему, яка майже не залежить від електроживлення та може бути розгорнута будь-де, якщо є акумулятори та смартфони, а температура від 0 до 50 градусів. Використання такої системи дозволяє швидко та ефективно проводити якісне навчання у польових умовах. Це може також бути використано для швидкого збору даних або тестування співробітників силових структур у реальних умовах. Така побудова системи дозволяє повністю синхронізувати всі процеси із повноцінною системою на базі LMS Moodle (створювати дистанційні курси, тести, аналізувати дані та інше).

Безкоровайний В. В., Судік А. О.

СИСТЕМОЛОГІЧНИЙ АНАЛІЗ ПРОБЛЕМИ ОПТИМІЗАЦІЇ ЛОГІСТИЧНИХ МЕРЕЖ

Задачі системної оптимізації логістичних мереж (ЛМ) є обов'язковою складовою технологій проектування, планування розвитку, адаптації чи реінжинірингу систем транспорту, збуту продукції, технічного обслуговування та ремонту озброєння і військової техніки [1] тощо. У таких системах врахування територіальної розосередженості функціональних підсистем і елементів призводить до проблеми, яка не може бути розв'язана традиційними методами системної оптимізації. Для розв'язання проблеми здійснюється її декомпозиція на ієрархічні рівні й аспекти, а процесу оптимізації – на групи процедур, пов'язаних з отриманням і перетворенням описів (рішень) щодо виділених рівнів і аспектів з подальшим їх об'єднанням (агрегацією) для отримання на відповідному рівні рішень по системі в цілому [2].

Пропонується подавати проблему оптимізації ЛМ як метазадачу, яка складається з множини задач, що відносяться до різних рівнів декомпозиції, з їх взаємозв'язками за вхідними даними і результатами розв'язання:

$$Problem = \{Task^l\},\ Task^l = \{Task_i^l\},\ l = \overline{1, n_l},\ i = \overline{1, i_l}, \qquad (1)$$

де $Task^l$ – множина задач *l*-го рівня; n_l – кількість рівнів декомпозиції; $Task_i^l$ – *i*-та задача *l*-го рівня; i_l - кількість задач, які необхідно розв'язати на *l*-му рівні.

На метарівні проблема (1) розглядається в цілому, аналізується її місце серед інших проблем управління відповідного масштабу. Комплекс виділених задач метарівня охоплює весь спектр питань оптимізації ЛМ, що виникають на стадіях передпроектних досліджень, проектування, створення і експлуатації, що вирішуються в системах їх проектування і управління ними. За своєю суттю є задачами системної оптимізації і відрізняються обмеженнями, які відображають специфіку основних етапів життєвого циклу мережі: $Task_1^1$ – формування вимог до ЛМ і розробка технічного завдання на її проектування; $Task_2^1$ – системне проектування мережі; $Task_3^1$ – планування розвитку мережі; $Task_4^1$ – модернізація мережі; $Task_5^1$ – реінжиніринг мережі.

Виділені задачі мікрорівня пов'язані з вирішенням питань системного проектування ЛМ: $Task_1^2$ – вибір принципів побудови мережі; $Task_2^2$ – вибір структури мережі; $Task_3^2$ – визначення топології елементів і зв'язків; $Task_4^2$ – вибір технології функціонування мережі; $Task_5^2$ – визначення параметрів елементів і зв'язків; $Task_6^2$ – оцінка ефективності варіантів побудови мережі та прийняття рішення.

У рамках системологічного підходу кожна з задач $Task_i^l$ проблеми (1) розглядається як перетворювач її вхідних даних In_i^l у вихідні Out_i^l:

$$Task_i^l: In_i^l \to Out_i^l,\ l = \overline{1,n_l},\ i = \overline{1,i_l}. \quad (2)$$

Розв'язання задач оптимізації ЛМ здійснюється за множиною показників (часткових критеріїв $k_i(s),\ i = \overline{1,m}$), які дозволяють отримувати кількісні оцінки ступеня досягнення мети її створення. Серед найбільш загальних вимог, що пред'являються до ЛМ, виділяються оперативність, надійність, живучість, економічність. У процесі розв'язання задач оптимізації мереж прагнуть до інтегральності часткових критеріїв $k_i(s),\ i = \overline{1,m}$.

Оцінку варіантів побудови мережі $s \in S$ (де S – множина допустимих варіантів) пропонується здійснювати з використанням методології функціонально-вартісного аналізу [2]. Метою створення ЛМ є максимізація їхньої ефективності. Вона може бути подана як отримання максимального співвідношення розміру ефекту від її функціонування Q і витрачених на це ресурсів C. При цьому функціональний ефект від використання мережі $\overline{Q}$ є неубутною функцією від витрачених на його досягнення ресурсів (вартості) $\overline{C}$: $\overline{Q} = F(\overline{C})$ (де F – оператор, що відображає стратегію використання ресурсів, яка визначається вибором варіанта побудови мережі $s \in S$.

За умови встановлених обмежень на наведені показники ефекту від використання мережі $\overline{Q} \geq \overline{Q}^*$ і витрат на його досягнення $\overline{C} \leq \overline{C}^*$ задача її системної оптимізації формально може бути подана у такому вигляді:

$$s^o = arg\ max\{\overline{Q}(s)/\overline{C}(s):\ s \in S,\ \overline{Q} \geq \overline{Q}^*,\ \overline{C} \leq \overline{C}^*\}. \quad (3)$$

Для побудови ефективної технології оптимізації ЛМ необхідна розробка комплексу моделей всіх задач (1) з урахуванням наборів їхніх вхідних і вихідних даних (2).

На основі формалізації мети створення мережі (3) і декомпозиції проблеми на комплекси взаємопов'язаних задач (1) запропоновано мережеву модель завдання її системної оптимізації [3, 4]. Мережева модель дозволяє побудувати логічну схему системної оптимізації, що визначає раціональну послідовність вирішення комплексу задач (1).

Для створення схеми системної оптимізації ЛМ необхідно визначити п'ятірку множин:

$$SysOptS = <Tasks, InDat, Res, DesDec, ProcDec>, \quad (4)$$

де *Tasks* – упорядкована множина задач (1); *InDat* – множина вхідних даних задач (1); *Res* – множина обмежень задач (1); *DesDec* – множина проектних оптимізаційних рішень; *ProcDec* – вирішальна процедура, що ставить кожній парі $< InDat_i^2,\ Res_i^2 >$ непорожню підмножину $DesDec_i^2,\ i = \overline{1,6}$.

Аналіз вхідних і вихідних даних моделей задач системної оптимізації (1) показав, що всі вони залежні між собою за внутрішніми вхідними і вихідними даними, а технологію її розв'язання доцільно будувати на основі послідовної ітераційної схеми [3]. Практична реалізація схеми (4) в технології системної оптимізації ЛМ передбачає вибір найбільш ефективних чи розробку нових математичних моделей і методів розв'язання часткових задач *Tasks* комплексу (1).

Список літератури

1. Морозов О.О. Методика синтезу системи технічного обслуговування та ремонту озброєння і військової техніки // Військово-технічний збірник. 2015. №12. С. 87-90.

2. Бескоровайный В.В. Системологический анализ проблемы структурного синтеза территориально распределенных систем // Автоматизированные системы управления и приборы автоматики. 2002. Вып. 120. С. 29-37.

3. Beskorovainyi V., Imanhulova Z. Technology of large-scale objects system optimization // ECONTECHMOD. 2017. Vol. 06. №4. P. 3-8.

4. Системологічний аналіз проблеми оптимізації мережі об'єктів головного центру спеціального контролю / В.В. Безкоровайний, Ю.О. Гордієнко, А.В. Кошель [та ін.] // Проблеми створення, випробування, застосування та експлуатації складних

інформаційних систем. 2019. Вип. 16. С. 50-62.

Єльчанінов О. Д.

ЕНТРОПІЙНИЙ ПІДХІД ДО СИНТЕЗУ ІНТЕГРАЛЬНОГО ПОКАЗНИКА ЯКОСТІ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНОЇ СИСТЕМИ

Інформаційно-вимірювальна система (ІВС) є невід'ємною структурною складовою будь-якого робототехнічного комплексу (РК). У загальному випадку така система являє собою сукупність функціонально об'єднаних апаратно-програмних засобів, призначених для отримання поточної інформації про власний стан робототехнічного комплексу та стан зовнішнього середовища з подальшим перетворенням цієї інформації у сигнали керування. Ефективність функціонування робототехнічного комплексу (РК) у цілому в значної мірі залежить від якості його інформаційно-вимірювальної системи.

Мета дослідження полягає в застосуванні ентропійного підходу до синтезу інтегрального показника якості ІВС робототехнічного комплексу та оцінювання її стану в умовах ситуаційної невизначеності.

В широкому сенсі, інформаційна модель стану інформаційно-вимірювальної системи РК в умовах зовнішніх та внутрішньосистемних збурень характеризується величинами апріорної та апостеріорної ентропії Шеннона до та після оцінювання N-мірного процесу $\mathbf{U}^T = [u_1(t),...u(t),...u_N(t)]$, який містить доступну інформацію про стан системи. Їхня різниця показує середню кількість інформації на виході досліджуваної системи. Представляючи узагальнений критерій невизначеності стану будь-якої технічної системи, ентропія являє собою дійсну функцію, яка залежить від щільності ймовірності $p(\mathbf{U})$. Серед сукупності відомих функцій розподілу $p(\mathbf{U})$ з однаковою дисперсію σ^2, максимальною ентропію має розподіл Гаусса.

За цією логікою глобальним показником якості ІВС може бути модифікована ентропійна метрика Шеннона, за якої середня кількість отриманої інформації про стан системи, що досліджується, фактично визначається величиною знятої невизначеності.

Дослідження інформаційних можливостей за умови розширення спектра внутрішньосистемних збурень пропонується здійснювати варіаційно-параметричним методом. Відхилення параметрів показника якості стану системи з елементами адаптивного управління від його оптимального значення пов'язано, перш за все, з випадковими варіаціями $\Delta\mathbf{W}$ параметричного вектора $\mathbf{W}$. Такі варіації найбільш адекватно відображають внутрісистемну невизначеність стану будь-якої технічної системи незалежно від особливостей конкретної фізичної проблеми. Аналітичним узагальненням внутрісистемної невизначеності стану інформаційно-вимірювальної системи РК є збурений параметричний вектор.

УДК 658.3

Вечерский М. В.

ОПРЕДЕЛЕНИЕ НЕОБХОДИМЫХ КОМПЕТЕНЦИЙ И НАВЫКОВ ПЕРСОНАЛА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

В настоящее время, в связи с развитием цифровой экономики, меняется набор требований к сотрудникам всех сфер деятельности. Человеческий капитал играет

огромную роль в повышении конкурентоспособности организации. Так, среди основных преимуществ цифровизации, является существенное снижение количества барьеров для выхода на рынок как крупных организаций, так и мелких. В связи с увеличением количества конкурентов на различных рынках, организациям необходимо задействовать все свои преимущества для достижения успеха. Так, одним из способов повышения конкурентоспособности является снижение себестоимости предлагаемых товаров и услуг. Основными направлениями снижения затрат организации являются уменьшение расходов на материальные составляющие продукции (материалы, сырье, комплектующие, услуги других организаций) и внутренние расходы организации (фонд заработной платы, общехозяйственные расходы).

Сокращение материальной части продукции является наиболее эффективным способом снижения ее себестоимости, так как может иметь долгосрочный эффект и оставлять задел для дальнейшего совершенствования продукта. Однако, влияние на материальную составляющую продукции зачастую требует первоначальных вложений: покупка экономичного оборудования, изменение технологического процесса, поиск нового поставщика. Кроме финансовых вложений, данные способы могут потребовать и значительных временных ресурсов, в течение которого организация не будет получать прибыль.

Сокращение внутренних расходов организации могут помочь получить быстрый и заметный результат, однако, его действие не является продолжительным, поэтому руководству, через некоторое время, придется снова искать способы снижения себестоимости. Цифровизация может продлить действие данных результатов. Так, в настоящее время, организациям не обязательно арендовать дорогие помещения в центре городов, они могут арендовать помещения на окраинах, тем самым сокращая ежемесячные расходы на аренду, компенсировать данное расстояние можно использованием информационно-коммуникационных технологий. Также, распространенным способом снижения себестоимости, является сокращение фонда заработной платы. Данное сокращение достигается не путем уменьшения заработной платы сотрудников, а за счет сокращения штата сотрудников и распределения обязанностей между оставшимися сотрудниками. Развитие цифровых технологий и новых методов обучения позволяет изучать смежные профессии, что является преимуществом для работодателей, ведь они смогут нанимать меньше сотрудников с большим кругом обязанностей. В связи с этим, в настоящее время требования к квалификации сотрудников постоянно меняются и усложняются.

Базовым при формировании требований к квалификации сотрудника является определение его компетентности в конкретной сфере. Так, согласно Европейской рамке квалификаций (EQF), компетенция складывается из:

- знаний – сведения, информация, факты, теория усвоенная человеком в процессе обучения;
- навыков – способность применять полученные знания на практике. Причем выделяются как инструментальные (умение пользоваться инструментом, оборудованием, программой для работы), так и когнитивные (творческое мышление, логика, умение решать практические задачи на основании изученной теории);
- отношения – мотивация сотрудника заниматься определенным видом деятельности и брать на себя ответственность за ее реализацию [1].

Таким образом, компетенции можно понимать как способность и желание применять полученные и усвоенные знания на практике, и брать за это ответственность.

Согласно исследованиям аналитиков Всемирного Экономического форума наиболее важными навыками, необходимыми работникам в условиях цифровизации экономики являются: способность комплексно решать проблемы, аналитическое и критическое мышление, умение управлять людьми, творчески мыслить, работать с большими объемами данных, взаимодействовать и работать с людьми [2].

В свою очередь, модель фундаментальных навыков цифровой экономики, разработанная компанией Burning Glass, выделяет 3 уровня компетенций:

- базовые – набор основных знаний и навыков, необходимых для работы по определенной профессии. Данные компетенции позволяют человеку получить работу в конкретной сфере и служат платформой для получения опыта и дальнейшего совершенствования своих способностей;
- ключевые – набор навыков, которые формируются у человека в процессе длительной работы или дополнительного обучения. Данные компетенции помогают человеку выделиться среди большого количества кандидатов, а значит, способствуют получению высокооплачиваемой работы. Данные навыки нуждаются в постоянной доработке, в связи с развитием рынка;
- специальные – узкий набор способностей человека, которые необходимы для работы в конкретной предметной области профессии. Данные компетенции не формируются самостоятельно и требуют непрерывного обучения. Компетенции такого уровня являются очень востребованными на рынке из-за малого предложения [3].

Таким образом, можно сделать вывод, что в условиях цифровой трансформации человеческий капитал имеет огромное значение. Работодателю необходимо правильно определить набор компетенций и навыков для повышения конкурентоспособности организации.

Список испрользованных источников

1. Ala-Mutka K. Mapping Digital Competence: Towards a Conceptual Under standing [Электронный ресурс]. – Электронные данные. – Режим доступа: http://jrc.es/pub/EURdoc/JRC67075_TN.pdf.
2. The 10 Skills You Need in the FourthIndustrial Revolution [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.weforum.org/agenda/2016/01/the-10-skills-you-need-to-thrive-in-the-fourth-industrial-revolu-tion.
3. The New Foundational Skills of theDigital Economy. Developing the Professionalsof the Future [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.burn-ing-glass.com/wp-ontent/uploads/New_Foundational_Skills.pdf.

УДК 623.55.02

Іохов О. Ю., Малюк В. Г., Ткаченко К. М.

ВИЗНАЧЕННЯ МЕЖ ЗОНИ ЕЛЕКТРОМАГНІТНОЇ ДОСТУПНОСТІ ДЖЕРЕЛА РАДІОВИПРОМІНЮВАННЯ З НАПРАВЛЕНОЮ АНТЕНОЮ

Працездатність системи радіозв’язку військового призначення та її розвідувальна доступність залежить в першу чергу від електромагнітної доступності (ЕМД) радіозасобів, що входять у склад такої системи.

Під зоною ЕМД будемо розуміти сукупність точок простору, перебуваючи в яких джерело радіовипромінювання (ДРВ) забезпечує на вході приймача рівень потужності сигналу необхідний для виявлення радіовипромінювання, пеленгування та вимірювання його технічних параметрів. Форма та розміри зони ЕМД залежать від ряду факторів:

- рельєфу місцевості, характеру підстильної поверхні, забудови і рослинності;
- чутливості приймачів радіопеленгаторів;
- висоти підйому антенних пристроїв над поверхнею землі;
- характеристик джерел випромінювань.

У найпростішому випадку розповсюдження корисного сигналу у вільному просторі при ідеальних умовах потужність сигналу на вході приймача визначається виразом:

$$P_R = P_T + G_T(\theta_{TR}, \varphi_{TR}) + G_R(\theta_{RT}, \varphi_{RT}) - L_{TR}(d) - K_п - \alpha_R - \alpha_T - FDR(\Delta f), \quad (1)$$

де P_R - потужність, що приймається антеною на відстані d;

P_T - потужність передавача сигналу;

$G_T(\theta_{TR}, \varphi_{TR})$ та $G_R(\theta_{RT}, \varphi_{RT})$ - коефіцієнти підсилення антен передавача радіосигналу у напрямку на приймач та приймальної антени у напрямку на радіопередавач відповідно;

$\theta_{TR}, \varphi_{TR}$ - азимут та кут місця з точки розташування передавача на приймач;

$\theta_{RT}, \varphi_{RT}$ - азимут та кут місця з точки розташування приймача на передавач;

α_T і α_R - втрати в антено-фідерних трактах відповідно;

$L_{TR}(d)$ - втрати сигналу на трасі поширення радіохвиль;

$K_п$ - коефіцієнт, що враховує втрати за рахунок розбіжності поляризації антен передавача і приймача;

$FDR(\Delta f)$ - коефіцієнт, що враховує втрати за рахунок розбіжності смуг і робочих частот випромінювання передавача і приймача.

У подальших розрахунках використовуються функції коефіцієнтів підсилення антен передавача G_T та приймача G_R, одержані у відповідності до методики, викладеної у роботі [1].

Критерієм прийняття рішення про ЕМД є виконання умови:

$$P_R \geq P_{min}, \quad (2)$$

де P_{min} - чутливість приймача.

Отже зоною ЕМД можна вважати сукупність точок простору

$$\Omega_{ЕМД} = \{(x, y) \mid P_R \geq P_{min}\}. \quad (3)$$

Для визначення меж зони ЕМД (3) використаємо хвильовий алгоритм [1], для якого координати ДРВ задаються у якості стартової точки. Критерієм зупинки хвилі є невиконання співвідношення (3) для усіх точок-кандидатів до наступного фронту хвилі. Приклад розрахунку зони ЕМД для передавача/приймача Mototrbo™ DP4000 [2] потужністю 1 Вт з направленою антеною відповідно до масштабу карти наведено на рис.1.

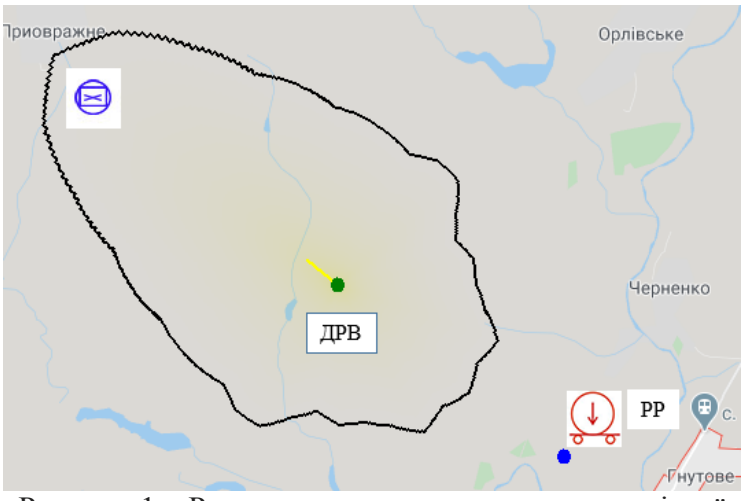


Рисунок 1 – Розрахунок меж зони електромагнітної доступності ДРВ з направленою антеною

Як видно з розрахунків, для зазначених параметрів радіозасобів та обраної орієнтації антени ДРВ забезпечуються вимоги щодо виконання умов працездатності радіоканалу, оскільки точка розміщення пункту управління належить області ЕМД. Відповідним чином забезпечуються умови розвідзахищеності радіоканалу, оскільки точка розміщення засобу радіорозвідки (РР) противника не входить у область ЕМД.

Напрямком подальших досліджень є проведення більш точних розрахунків за рахунок використання електронних цифрових карт, інформації про підстильну поверхню, забудову і рослинність.

Список літератури

1. Iohov O., Maliuk V., Horielyshev S., Tkachenko K., Herasimov S. Development of a Method for Boundary Determination of the Noise-resistant Area of the UHF/VHF Band. Advances in Military Technology, 2020, vol. 15, no. 2, pp. 231-246. DOI 10.3849/aimt.01376

2. Портативные цифровые радиостанции Mototrbo™ серии DP4000 DP4800 [Електронний ресурс]. Режим доступу: https://cutt.ly/lhGaH7A (Дата звернення 15.12.2020).

Безкоровайний В. В.

ВИДІЛЕННЯ ПІДМНОЖИН ЕФЕКТИВНИХ ВАРІАНТІВ ДЛЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Ефективність переважної більшості проектних і управлінських рішень оцінюється сукупністю частинних критеріїв [1]. За результатами декомпозиції проблеми прийняття багатокритеріальних рішень у загальному випадку виділяють множину задач [2]: формалізації мети; визначення універсальної множини рішень; визначення множини допустимих рішень; виділення підмножини ефективних (Парето-оптимальних) рішень; ранжирування рішень; вибору найкращого рішення. При цьому в умовах багатокритеріальності, ранжирування і вибір найкращого варіанта здійснюється особою, що приймає рішення (ОПР), на множинах ефективних (таких, що не можуть бути покращені, Парето-оптимальних, компромісних) рішень [1-2], які можуть бути досить потужними [3]:

$$X = X^S \bigcup X^E,\ X^S \bigcap X^E = \varnothing, \qquad (1)$$

де X – множина допустимих рішень; X^S – підмножина згоди (неефективних рішень), будь-яке рішення з якої може бути покращене хоча б за одним із частинних критеріїв $k_i(x)$, $i = \overline{1,m}$ без погіршення якості за іншими; X^E – підмножина компромісів, жодне з рішень з якої не може бути покращене одночасно за всіма критеріями $k_i(x)$, $i = \overline{1,m}$.

Це обумовлює актуальність завдань дослідження методів формування, виділення та скорочення підмножин рішень для остаточного вибору ОПР.

Формально задача прийняття рішень полягає у виборі альтернативи з множини допустимих $x \in X$, що призводить до деякого результату $z \in Z$. Ефективність кожної альтернативи $x \in X$ визначається ступенем відповідності отриманого результату $z \in Z$ поставленій меті. Для оцінювання альтернатив $x \in X$ в рамках як ординалістичної (порядкової), так і кардиналістичної (кількісної) теорії корисності використовуються функції корисності $P(x)$, за значенням яких вибирається найкраще рішення:

$$x^O = \arg\max_{x \in X} P(x). \quad (2)$$

Значення корисності (цінності) пар рішень $P(x)\ \forall x, y \in X$ дозволяє визначити їхній порядок: $x \sqsupset y \leftrightarrow P(x) = P(y);\ x \succ y \leftrightarrow P(x) > P(y);\ x \geq y \leftrightarrow P(x) \geq P(y)$.

Точне визначення підмножини $X^E \subset X$ є досить складною задачею, що розв'язується методами дискретного вибору, парних порівнянь, на основі методів Карліна (для опуклих множин) і Гермейєра (для неопуклих множин) [3].

Підмножина ефективних X^E на опуклій множині допустимих рішень X на основі теореми Карліна знаходиться шляхом об'єднання варіантів $x_i^o,\ i = \overline{1,m}$, що оптимізують кожен з частинних критеріїв $k_i(x),\ i = \overline{1,m}$, з розв'язками задачі параметричного програмування відносно параметрів [4]:

$$\lambda_i \in \Lambda = \{\lambda_i : \lambda_i > 0\ \ \forall i = \overline{1,m},\ \ \sum_{i=1}^{m} \lambda_i = 1\}, \quad (3)$$

$$x_i^o = arg\ \max_{x \in X} \{P(x) = \sum_{i=1}^{m} \lambda_i \xi_i(x)\}, \quad (4)$$

де $\xi_i(x),\ i = \overline{1,m}$ – нормоване значення або значення функції корисності i-го частинного критерію, що подається як значення функції належності розмитій множині «краще рішення».

Підмножина ефективних варіантів $X^E \subset X$ на основі теореми Гермейєра знаходиться шляхом об'єднання варіантів $x_i^o,\ i = \overline{1,m}$, що оптимізують кожен з частинних критеріїв $k_i(x),\ i = \overline{1,m}$ з розв'язками задачі параметричного програмування відносно параметрів [4]:

$$\lambda_i \in \Lambda = \{\lambda_i : \lambda_i > 0\ \ \forall i = \overline{1,m},\ \ \sum_{i=1}^{m} \lambda_i = 1\}, \quad (5)$$

$$x_i^o = arg\ \max_{x \in X} \{P(x) = \min_i \lambda_i \xi_i(x)\}. \quad (6)$$

Методи дискретного вибору і парних порівнянь дозволяють коректно виділяти підмножини ефективних рішень. Однак, зважаючи на високу часову складність ці методи можна застосовувати лише на відносно невеликих множинах альтернатив. Вагові методи, включаючи методи на основі теорем Карліна і Гермейєра, мають меншу регульовану часову складність, ніж точні методи. Однак вони дозволяють виділяти неповні підмножини. Ефективним способом спрощення задачі є попереднє визначення наближеної множини компромісів X^P. Умовами коректності процедури визначення наближеної підмножини компромісів є вимога, щоб вона містила в собі підмножину компромісів $X^E \subseteq X^P$ та простота її визначення.

Для остаточного вибору ОПР пропонується надавати лише підмножину ефективних рішень $X^o \subset X^K$, що містить субоптимальні рішення, які відповідають встановленим перевагам між частинними критеріями $k_i(x),\ i = \overline{1,m}$. Скорочення підмножини ефективних до підмножини субоптимальних рішень $X^o \subset X^E$ запропоновано здійснювати з використанням оцінок на основі поліному Колмогорова-Габора [3]

$$P(x) = \sum_{i=1}^{m} \lambda_i \xi_i(x) + \sum_{i=1}^{m} \sum_{j=i}^{m} \lambda_{ij} \xi_i(x) \xi_j(x) + \ldots, \quad (7)$$

де λ_i, λ_{ij} – вагові коефіцієнти частинних критеріїв і їхніх добутків; $\xi_i(x), \xi_j(x)$ –

функції корисності частинних критеріїв $k_i(x), k_j(x),\ i, j = \overline{1,m}$.

Запропонований двоетапний метод для підтримки прийняття багатокритеріальних рішень дозволяє автоматизувати функції визначення та скорочення підмножини ефективних варіантів, а також вибору найкращого серед заданих значеннями частинних критеріїв.

Список літератури

1. Greco S., Ehrgott M., Figueira J.R. Multiple Criteria Decision Analysis – State of the Art Surveys. New York: Springer, 2016. 1346 p.

2. Маляр М.М. Моделі і методи багатокритеріального обмежено-раціонального вибору: Монографія. Ужгород: РА «АУТДОР-ШАРК», 2016. 222 с.

3. Vladimir V. Beskorovainyi, Lubomyr B. Petryshyn, Olha Yu. Shevchenko. Specific subset effective option in technology design decisions // Applied Aspects of Information Technology, 2020. Vol.3 No.1, pp. 443-455.

4. Михалевич В.С., Волкович В.Л. Вычислительные методы исследования и проектирования сложных систем. М.: Наука, 1982. 288 с.

Шаповалов Б. Б., Завістовський О. Д.

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ФОРМУВАННЯ ГОТОВНОСТІ ПРАВООХОРОНЦІВ ДО ДІЙ В ЕКСТРЕМАЛЬНИХ СИТУАЦІЯХ (НА ПРИКЛАДІ ПОЛІЦЕЙСЬКОГО ХОРТИНГУ)

Діяльність працівників правоохоронних органів нерідко відбувається в екстремальних ситуаціях, які характеризуються небезпекою для життя та здоров'я. Формування їх готовності до зазначених дій є складним педагогічним процесом, від ефективності якого залежить не лише безпека правоохоронців, але й успішність діяльності держави у сфері забезпечення громадського порядку, боротьби зі злочинністю, захисту громадян від небезпечних факторів.

Прискорений розвиток суспільства вимагає нових підходів до формування готовності працівників ризиконебезпечних професій до ефективної діяльності в складних, небезпечних, критичних ситуаціях. З цією метою фахівцями Поліцейського центру бойових мистецтв «Закон і порядок» та Міжнародної федерації поліцейського хортингу були розроблені сучасні психолого-педагогічні технології формування готовності до дій в екстремальних ситуаціях, а саме:

- систему підготовки людини до екстремальних ситуацій Бориса Шаповалова;
- систему самозахисту та виживання (ССВ);
- поліцейську систему самозахисту і контролю (ПССК).

Зазначені системи, в свою чергу, разом з українським національним професійно-прикладним видом спорту, системами військово-патріотичного виховання, оздоровчими та реабілітаційними системами, входять до системи Поліцейського хортингу.

У широкому розумінні, поліцейський хортинг можна визначити як синергетичну сукупність прийомів, методів, засобів, знань, навичок та умінь, спрямованих на виживання особистості в типових та екстремальних ситуаціях, пов'язаних з необхідністю захисту загальнолюдських цінностей.

Створення поліцейського хортингу в цілому як і кожної його підсистеми було б неможливим без якісного інформаційно-аналітичного забезпечення, тобто процесу створення оптимальних умов задля задоволення інформаційних потреб та реалізації посадових обов'язків органів державної влади і волонтерської роботи представників громадських організацій на основі формування та використання інформаційних ресурсів.

Процес створення поліцейського хортингу відбувався в два етапи. Суть першого етапу, який умовно можна назвати інформаційним – відносно самостійна діяльність автора та інших фахівців, занятих пошуком, відбором, накопиченням, класифікацією, обробкою, узагальненням та збереженням необхідної інформації. На цьому етапі:

- вивчалися посібники, навчальні програми, відеоматеріали змагань та тренувального процесу значної кількості бойових мистецтв та спортивних єдиноборств;
- було проаналізовано організацію навчального процесу військових, правоохоронців, рятувальників різних країн світу;
- ретельно вивчалися правові норми, що регулюють діяльність в екстремальних ситуаціях;
- проводилося узагальнення результатів наукових досліджень з анатомії, фізіології, біомеханіки, конституційного права, кримінального права, адміністративного права, криміналістики, кримінології, теорії і методики фізичної культури і спорту, психології, філософії, тактики і стратегії в частині, що стосується закономірностей і регламентації дій в екстремальних ситуаціях.

Значну роль у створенні поліцейського хортингу зіграв особистий багаторічний досвід служби автора у рятувальних, правоохоронних, миротворчих підрозділах, а також його 40-річний стаж занять бойовими мистецтвами.

Під час другого етапу (умовна назва – аналітичний) автор на підставі наявних інформаційних одиниць і складних розумових процесів розробив нове знання щодо закономірностей поведінки правоохоронців в екстремальних ситуаціях та особливостях формування готовності до дій в зазначених умовах. Зокрема:

- були сформульовані принципи ефективності технічних дій самозахисту;
- були сконструйовані нові технічні дії захисту від нападу неозброєного та озброєного правопорушника, звільнення від захватів та обхватів, затримання нападників, їх конвоювання;
- були розроблені алгоритми поведінки в різних екстремальних ситуаціях;
- були сформульовані теоретичні засади українського національного професійно-прикладного спорту правоохоронців – поліцейського хортингу тощо.

Психолого-педагогічні системи формування готовності до дій в екстремальних ситуаціях, як і вся система поліцейського хортинга знаходяться у динамічному розвитку і постійно модернізуються відповідно до змін в соціальному житті, тенденцій (негативних чи позитивних) криміногенної обстановки тощо. А це означає, що інформаційно-аналітичне забезпечення зазначених систем є однією з головних умов їх розвитку.

УДК 656.7.072.6

Яновський П. О., Ткаченко В. А., Целіщев І. О.,
Кульбашевський В. А., Гайченя Д. В.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ОБСЛУГОВУВАННЯ ВІЙСЬКОВИХ ПЕРЕВЕЗЕНЬ У ВАНТАЖНОМУ КОМПЛЕКСІ АЕРОПОРТУ

Практика розвитку економічних відносин в Україні свідчить, що використання новітніх результатів науково-технічного прогресу здійснюється швидкими темпами не лише у виробництві, а і в транспортній сфері. Прискорення науково-технічного прогресу в даний час слід використовувати, як один із важливих напрямків удосконалення технології переробки військових вантажів в аеропортах. В зв’язку з цим в транспортному обслуговуванні вантажовласників, в т.ч. і військових, особливе місце посідає інформатизація технологічних процесів на всіх видах транспорту.

Традиційно конкурентною перевагою повітряного транспорту є швидкість перевезення. Але посилення заходів безпеки, тривалі процедури оформлення перевезень знижують позитивний ефект від технічних і технологічних нововведень. Істотна частина вантажів, що перевозяться авіакомпаніями країн СНД, належить великим транснаціональним компаніям і урядам іноземних держав. Тобто такі вантажопотоки не пов'язані з ринком нашої держави тому, що аеропорти відправлення і призначення знаходяться в інших країнах. По іншому склалася ситуація з організацією військових перевезень в нашій державі, де здійснюється практично весь комплекс технологічних операцій при використанні повітряного транспорту.

Тому для українського ринку вантажних повітряних перевезень задача модернізації технології обробки вантажів, в т.ч. і військових, в вантажних терміналах аеропортів є актуальною. Це пояснюється, не лише необхідністю скорочення терміну доставки вантажів з поліпшенням якості їх обслуговування і прискоренням перебування у вантажних комплексах, а і тим, що частка вітчизняних підприємств на світовому авіаринку невелика, що відповідає нашому економічному потенціалу, обумовленого рівнем розвитку економіки, географічним положенням держави та інш. Оптимізувати процес доставки вантажів в сучасних умовах, задовольняти потреби клієнтів якісними послугами можна реалізацією в структурах повітряного транспорту інноваційних заходів та сучасних досягнень у сфері інформаційних технологій (ІТ).

Для поліпшення якості обслуговування вантажовласників і функціонування вантажних терміналів в аеропортах при переробці військових вантажів важливо впровадити комплекс інформаційного забезпечення (КІЗ) транспортно-логістичних процесів (ТЛП), який охоплював би не лише внутрішні бізнес-процеси, а і надавали би точну інформацію про результати роботи зовнішніх суміжних об'єктів (як приватних, так і державних структур) з надання транспортних послуг. Виконання цієї умови є важливою для прийняття обґрунтованих управлінських рішень. Тому слід з використанням електронного документообігу в транспортному процесі проводити оцінку ефективності впровадження ІТ для вирішення практичних задач з обслуговування військових перевезень в аеропортах.

УДК 656.7.072.6

Яновський П. О., Ткаченко В. А., Яременко В. В.,
Марценюк С. О., Міщук В.П.

ІНТЕГРОВАНІ ТЕХНОЛОГІЇ В СИСТЕМІ ПЕРЕВЕЗЕНЬ ВІЙСЬКОВОСЛУЖБОВЦІВ ЗБРОЙНИХ СИЛ УКРАЇНИ

Однією з важливих ознак сучасного розвитку України є спрямованість економіки на підвищення конкурентоспроможності продукції усіх працюючих підприємств завдяки модернізації виробництв, впровадження нових технологій та сучасного обладнання. Провідна роль у цих процесах належить використанню інформаційних технологій (ІТ), які здійснюють знімання з виробничих об'єктів, обробку і представлення інформації з наданням рекомендацій щодо підтримки прийняття рішень (ППР). З використанням отриманих даних на багатьох підприємствах якісно здійснюється регулювання виробничих процесів, успішно працюють автоматичні та автоматизовані системи управління окремими структурними підрозділами і підприємствами в цілому. За рівнем наукомісткості цей напрям повинен залишатися провідним у вітчизняному виробництві, що вимагає постійного його розвитку і удосконалення. Це стосується системи перевезень особового складу ЗС України на повітряному транспорті.

Система перевезень особового складу ЗС України відноситься до сфери діяльнос-

ті оборонного сектору держави. Причому такі перевезення здійснюються повітряним транспортом не часто і в невеликих обсягах, що перешкоджає широкому впровадженню інновацій, науково-технічних ідей, досвіду, накопиченого практиками і вченими в сфері інформатизації транспортних операцій. Внутрішньогалузева таємність і монополізм в їх організації обмежують плідність співробітництва, виключають конкуренцію галузевої науки з представниками академічних і вузівських секторів.

В умовах глобалізації світових процесів набуває особливого значення інформатизація виробничих процесів, своєчасне одержання даних з якої, сприяє якісному вирішенню проблем у суспільстві кожної держави. Це, перш за все, пов'язано із економічними процесами, які постійно супроводжуються кризами в будь-якій сфері людської діяльності. Не є виключенням і транспортна сфера, в якій теж проявляється суперництво, що при певних обставинах може призвести до значних людських і фінансових втрат суспільства, в т.ч. і в оборонному секторі. Для усунення можливих втрат при перевезеннях для ЗС України необхідне створення сучасних інформаційних систем (ІС), які будуть забезпечувати накопичення необхідної для практичної діяльності інформації, її оброблення, зберігання і поширення, а також проведення техніко-економічних розрахунків для підтримки прийняття оперативних рішень (ППР).

Вибір складу, структури ІС, а також принципів її функціонування залежить від конкретизації мети створення системи, ступеня використання накопиченого досвіду при здійсненні реальних перевезень, а також від функціонального призначення системи (обслуговування цивільних пасажирів, перевезення особового складу ЗС України). В техніко-економічних обґрунтуваннях вибору раціональної системи ІТ слід враховувати вартість обладнання, його встановлення, залучення висококваліфікованого персоналу. Використання ІТ сприятиме автоматизації перевізного процесу військовослужбовців.

УДК 656.7.072.6

Яновський П. О., Ткаченко В. А., Яременко В. В.,
Кульбашевський В. А., Грозан О. С.

ІНФОРМАТИЗАЦІЯ УПРАВЛІННЯ ЕКСПЛУАТАЦІЄЮ АВІАЦІЙНОЇ ТЕХНІКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Процес обслуговування повітряних суден (ПС) здійснюється в аеропарках відправлення, призначення, транзиту і включає операції з технічного та комерційного обслуговування. До технічного обслуговування належать операції із заправки повітряного судна паливом, водою, спеціальними рідинами, перевірка роботи обладнання тощо. До операцій з комерційного обслуговування належать операції з оформлення прильоту літака, розрахунку і комплектування комерційного завантаження; реєстрація квитків і оформлення багажу; посадка та висадка пасажирів, розвантаження літака; завантаження літака і кріплення вантажу, багажу і пошти; оформлення супровідної документації тощо.

Стоянка повітряного судна в аеропортах обмежена за часом; перевищення часу перебування літака, затримки рейсу через несвоєчасне виконання обслуговування рейсу можуть призвести до додаткових витрат та штрафів, у деяких випадках – втрати слотів. Тому відмінною рисою процесів обслуговування на повітряному транспорті є короткий термін виконання всіх операцій. Процеси підготовки повітряних суден до вильоту, обслуговування пасажирів, оброблення вантажів, багажу та пошти в аеропортах відправлення, призначення, транзиту виконуються дуже швидко, починаються та закінчуються в точно визначений термін. У практиці авіакомпаній вико-

ристовуються технологічні графіки підготовки повітряних суден до вильоту за типами літаків.

Інформаційні технології (ІТ) виконують збирання та обробку інформації про транспортний процес на повітряному транспорті, здійснюють його діагностику, аналіз та синтез, а також дають оцінку наслідків прийняття різних варіантів рішень. Для таких складних і важливих процесів, як транспортний, інформаційні технології (ІТ), які здійснюють аналітичне забезпечення прийняття рішень втрачають другорядність, не залишаються допоміжними, а стають першочерговими для досліджуваного процесу. В результаті застосування ІТ значно підвищується якість прийняття рішень. Для цього створення ІТ в процесах технології обслуговування повітряних суден (ПС), спираючись на автоматизований документообіг з поглибленою аналітичною обробкою даних, надасть управлінням підтримку прийняття оптимальних рішень для оцінки технічного стану ПС.

Незважаючи на складність технології обслуговування ПС по вильоту, прильоту і трансферних рейсів інформаційна технологія (ІТ) своєчасно забезпечить управлінський персонал на високому рівні якісною інформацією завдяки високій оперативності функціонування ІТ щодо збирання, накопичення, систематизації та обробки даних про стан ПС та їх окремих вузлів. Завдяки цьому персонал отримуватиме своєчасно якісну інформацію і матиме змогу приймати ефективні рішення щодо можливостей подальшої експлуатації ПС.

УДК 656.7.072.6

Яновська В. П., Яновський П. О., Маліновський А. В., Яновська Т. Г.

КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ РОЗВИТКУ ТРАНСПОРТНОГО ОБСЛУГОВУВАННЯ ОБОРОННОЇ СФЕРИ УКРАЇНИ

У процесі еволюції галузей економіки в суспільстві широке розповсюдження в багатьох державах світу отримали комп'ютерно-інтегровані технології (КІТ) для вирішення питань розвитку виробничих процесів, в тому числі і транспортних. Можливість визначення за допомогою таких систем найкращого шляху зменшення витрат, в т.ч. і в організації перевезень у Збройних Силах України завдяки широкого обліку в діяльності підприємств всієї системи діючих факторів дуже важлива в сучасних ринкових умовах через наявність значного дефіциту фінансових ресурсів.

Впровадження КІТ в нашому суспільстві сприяє зменшенню витрат на утримання працівників апарата управління, в першу чергу на таких операціях, як розрахункові процеси і оперативний контроль за ходом транспортного обслуговування ЗС України.

Робота КІТ надає можливість встановити шляхи удосконалення і покращення використання власної технічної бази і транспорту. Забезпечення інформацією для підтримки на всіх рівнях прийняття управлінських рішень є нагальною задачею сучасного розвитку України.

Сучасні КІТ допомагають здійснювати спостереження за зовнішніми і внутрішніми інформаційними потоками, які з часом постійно збільшуються. Крім того, вони проводять їх аналіз, на підставі чого здійснюють прогнозування розвитку подій і напрацювання рекомендацій щодо підтримки прийняття рішень. Також використання інформаційних технологій (ІТ) спрямовується на забезпечення координації діяльності усіх зовнішніх і внутрішніх структур в сфері переміщень матеріальних цінностей і військовослужбовців, що підвищить ефективність використання бюджетних коштів.

На процес прийняття управлінських рішень впливають різноманітні фактори:

завжди існує ймовірність прийняття неправильного рішення, дефіцит часу для прийняття рішення, підтримка або не підтримка колективом рішення, особисті якості управлінців, престиж організації.

Кінцевим результатом прийняття рішення є саме управлінське рішення щодо варіанту організації перевезень матеріальних цінностей ЗС України, на яке інтегровано впливають різні фактори.

При розробці комп'ютерної системи підтримки прийняття рішень (КСППР) важливо враховувати складність і багатоетапність реалізації раціональної технології прийняття рішень: діагноз проблеми, накопичення інформації про проблему, розробка альтернативних варіантів, їх оцінка і саме прийняття рішення.

Широке застосування СППР у сфері транспортного обслуговування оборонної сфери держави дозволяє підвищити ефективність міжвідомчої взаємодії, покращити надання послуг оборонним структурам, роботи підрозділів і штату працівників.

Пріоритети у використанні СППР в транспортному обслуговуванні ЗС України встановлюються в загальній системі діючих законів в державі щодо основних засад розвитку інформаційного суспільства в Україні.

УДК 351.741:[621.397.4+004]

Мордвинцев М. В., Хлєстков О. В., Ницюк С. П.

АНАЛІЗ ВИКОРИСТАННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

Національна поліція України (далі – НП України) для збору доказів злочину, пошуку і затримання злочинців, забезпечення публічної безпеки, охорони власності, контролю за дотриманням правил дорожнього руху широко впроваджує системи відеоспостереження [1]. Розглядаються основні тактичні прийоми їх використання НП України.

Управління силами та засобами патрульної поліції здійснюється за допомогою системи централізованого управління нарядами патрульної служби «ЦУНАМІ». До складу цієї системи входить система стаціонарного відеоспостереження, яка забезпечує оперативний візуальний контроль за основними криміногенними місцями, вулицями, майданами, транспортними потоками, об'єктами що охороняються. НП Україні використовує інформацію з понад ніж 24 тис. відеокамер, з яких майже 2,8 тис. це так звані «розумні».

Патрульна поліція України використовує нагрудні відеокамери (відеореєстратори), системи відеоспостереження, встановлені на службових транспортних засобах, і стаціонарні системи відеоспостереження. Основною метою використання відеореєстраторів є забезпечення об'єктивної оцінки дій патрульного під час виконання ним своїх обов'язків, ретельний збір доказів правопорушення.

За допомогою систем відеоспостереження, встановлені на службових транспортних засобах функціонує інформаційна підсистема «Гарпун». Система «Гарпун» використовує спеціалізоване аналітичне програмне забезпечення створене для розшуку викрадених транспортних засобів та номерних знаків, виявлення одночасного перебування номерних знаків на різних транспортних засобах, фактів використання знищених номерних знаків, а також для автоматизованого інформування про такі факти чергових диспетчерів патрульної служби. «Гарпун» є підсистемою інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».

До Єдиного аналітичного сервісного центру Головного управління Національної поліції в Донецькій області належить система UASC, в якій використовують інтелек-

туальні відеокамери. Система проводить ідентифікацію автомобіля, на який встановлений державний номер і виявляє відповідність номера автомобіля згідно з реєстрацією, розпізнає тип і марку автомобіля та його колір, перевіряє чи знаходиться автомобіль у розшуку, чи відповідає державний номер автомобіля, ідентифікує осіб, які знаходяться на передньому сидінні. Система виявляє скупчення людей, може фіксувати їх неадекватну поведінку, розпізнає заборонений або нетиповий рух автотранспорту т.і.

В структурі апарату НП України створено Управління організації діяльності підрозділів поліції на воді та повітряної підтримки (УПВП). Його запроваджено для організації, координації й контролю службової діяльності підрозділів поліції на воді та забезпечення повітряної підтримки підрозділів НП України. Підрозділи поліції застосовують БпЛА для: висотного спостереження під час проведення масових святкувань, політичних демонстрацій, спортивних заходів, а також під час припинення масових заворушень; висотного спостереження при загрозі нападу на стратегічні об’єкти та об’єкти, які знаходяться під охороною; виявлення злочинів та адміністративних правопорушень; організації відео документування; забезпечення зв’язку й управління наземними нарядами поліції; організації взаємодії підрозділів поліції з іншими силовими структурами; забезпечення та контролю безпеки дорожнього руху; проведення спостереження при здійсненні оперативних заходів, відстеження оперативної обстановки під час виконання службових завдань; пошуку підозрюваних, які намагаються сховатись; пошуку зниклих людей.

КАСКАД – комплексна система контролю автомобільних доріг (Київ). Єдиний повнофункціональний пристрій що впроваджений в експлуатацію, та розроблений під особливості національного технічного регулювання, законодавчу базу. Встановлені комплекси фіксують події з ознаками порушень ПДР: швидкісний режим; проїзд на забороняючий сигнал світлофора; порушення розмітки, перетин суцільної смуги; порушення правил паркування; рух смугою громадського транспорту. Дані передають до системи збору та обробки даних.

Система безпеки Vezha буде введена в експлуатацію у Вінницькій області. В основі системи лежить використання штучного інтелекту для аналізу відеопотоку з камер відеоспостереження. Штучний інтелект дає змогу пришвидшити в сотні разів процес розпізнавання та зберігання потрібних даних, обробляти великі масиви зображень та даних за лічені секунди. Система постійно самонавчається, що дає смогу збільшити перелік завдань, які можна вирішувати на основі Vezha. Система може проводити розпізнавання облич, що передбачає визначення та розпізнавання людських облич в потоці, порівняння їх зі списком моніторингу та отримання сповіщення про збіг. Є можливість розпізнавання обличчя з фотографії та пошук по фото, фіксацію місцезнаходження та руху людини, визначення статі та віку, керування тривогою під час роботи. Система може проводити розумний пошук людини, що дозволяє шукати людину за кольором одягу, допомагає ідентифікувати попереднє місцезнаходження людини, поєднати події з декількох відеоресурсів, дає можливість отримувати звіти по годинах, днях, тижнях або місяцях. Система визначає людей, транспортні засоби та тварини у визначеній області, зберігає зібрані дані виявлених об'єктів, транспортних засобів, людей в базі даних, контролює час та тип об’єкта, вид тварини, транспортного засобу, що перебувають у зоні, виявляє порушення певних правил парковки, проводить фіксацію об’єктів за допомогою фотографій, та сповіщення, про паркування. Визначає номер, марку, колір та маршрут транспортних засобів у потоці руху. Визначайте інтенсивність, кількість та склад трафіку транспортних засобів чи людей. Виявляйте появу натовпу людей на відкритих майданчиках чи всередині конкретного приміщення. Система дозволяє проводити швидкий пошук дітей.

Список літератури

1. Коршенко В.А., Чумак В.В., Мордвинцев М.В., Пашнев Д.В. Стан систем безпеки з використанням технічних засобів відеозапису та відеоспостереження: зарубіжний досвід, перспективи впровадження в діяльність Національної поліції України / В.А. Коршенко, В.В. Чумак, М.В. Мордвинцев, Д.В. Пашнев // Право і безпека. – 2020. – № 2(77) – С. 86-92.

УДК 358.119.1+007 + 357.3 + 355.692.32

Козубцов І. М., Хлапонін Ю. І., Козубцова Л. М.

ІДЕЯ ВПРОВАДЖЕННЯ ЗВОРОТНОГО ЗВ'ЯЗКУ ЯК ВДОСКОНАЛЕННЯ ФУНКЦІОНАЛЬНОЇ ЗАЛЕЖНОСТІ РЕАЛІЗАЦІЇ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Постановка завдання. Здійснити пошук механізму удосконалення механізму забезпечення кібербезпеки ґрунтуючись на онтологію кібербезпеки ISO/IEC 15408-1.

Мета доповіді. Апробувати ідею зворотного зв'язку у загальні функціональні залежності реалізації кібернетичної безпеки.

Результат дослідження. Пошук рішення науково-технічної проблеми забезпечення кібербезпеки в нашому дослідженні зорієнтуємо на (алгоритм) онтологію кібербезпеки поданого на рис 1, який представляє собою адаптацію відповідної схеми із ISO/IEC 15408-1. Як можна побачити з наведеного рисунка ключовим блоком є активи. Очевидно агенти загроз націлені на знищення активів зацікавлених сторін, а ті їх зберегти. З наведеного рисунку цієї очевидності не переглядається зі сторони зацікавлених сторін, оскільки на схемі відсутній принциповий зворотній зв'язок від активів до зацікавлених сторін.

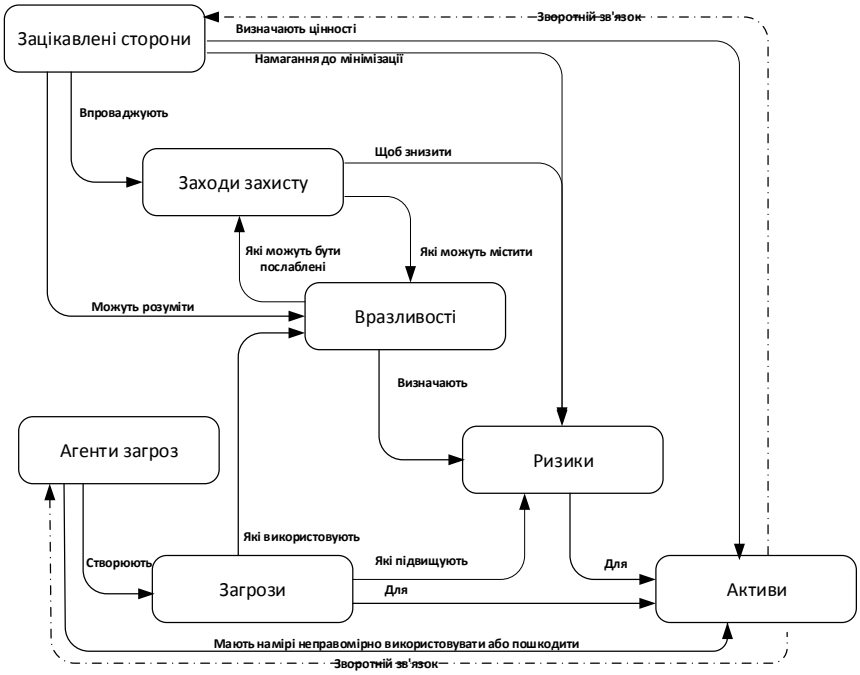


Рисунок 1 – Онтологія кібербезпеки ISO/IEC 15408-1

В подальших роботах пропонується привести схему наведену на рис. 1 у відповідність логікі протікання процесів та мети.

Висновки. Таким чином, ідея застосування зворотного зв'язку у загальні функціональні залежності реалізації кібернетичної безпеки на нашу думку є необхідною,

оскільки через неї буде протікати інформація про процес оцінки рівня досягнення заходів з кібербезпеки заданій меті як результуючий процес впливу та захисту.

УДК 004.852

Канашевич Д. В., Шубін І. Ю.

МЕТОДИ ВІЗУАЛЬНОЇ ІНТЕРПРЕТАЦІЇ ВЕЛИКИХ ДАНИХ

Розвиток сфер діяльності людини, що засновані на застосуванні цифрових технологій, робить актуальним створення засобів обробки, передачі й зберігання великих обсягів даних. Існуючі підходи до дослідження емпіричних даних мають ряд недоліків, до яких слід віднести їхню значну ресурсоємність і високі вимоги до підготовки фахівців, що приймають участь у дослідженні [1]. Потенційні можливості візуалізації сформували умови для її залучення до вирішення актуальних завдань у багатьох сферах людської діяльності: медицина, техніка, економіка, юриспруденція і т.ін. Одним із прикладних напрямків у розвитку візуалізації, що має зростаючу актуальність, стає розробка технології когнітивної інтерпретації, що застосовується для дослідження великих обсягів гетерогенних даних. На сучасному етапі розвитку засобів інформаційної комунікації візуализація розглядається як домінуюча форма інформаційної взаємодії [2]. Однак, на цей момент не сформований єдиний підхід до вивчення й використання можливостей візуалізації як інструмента наукового дослідження. Одним з утруднень у цьому напрямку є необхідність проведення об'ємних міждисциплінарних досліджень, для яких характерними перешкодами є формування загального визначення об'єкта досліджень і використання спеціалізованих методів, що відповідають вузьким предметним областям.

Термін «розуміння» значною мірою збігається з поняттям «інсайт» (*insight*), для якого визначені властивості, на підставі яких можливий перехід до кількісних характеристик розуміння. Глибина інсайту відображає обсяг нових знань, отриманих дослідником при осмисленні питання або інтерпретації візуально сприйнятого об'єкта, а також комплексність – кількість зв'язків з іншими поняттями або областями знання.

Дана робота спрямована на обґрунтування залучення когнітивного потенціалу візуалізації до одержання нових знань при обробці великих обсягів гетерогенних даних. Існуючі приклади використання засобів візуалізації дозволяють припустити, що їхня результативність може бути суттєво поліпшена завдяки активному використанню власного потенціалу дослідника, у тому числі, інформативного, когнітивного, емоційного. Крім того, систематизація зусиль, прикладених до розробки й застосування засобів візуалізації, є необхідною умовою для досягнення високої інтерпретуємості досліджуваних даних, забезпечуючи одержання нових знань. Створення засобів візуального дослідження, що мають передбачувану і керовану результативність дозволить розширити їхнє практичне застосування як прикладного інструментарію у наукових дослідженнях. У наш час, залучення й активне використання когнітивного потенціалу дослідника є пасивними резервами існуючих засобів досліджень. Цілеспрямоване використання цих резервів при розробці засобів візуалізації здатне збільшити їхню практичну значимість як інструмент для дослідження більших обсягів гетерогенних даних.

Розроблений оригінальний алгоритм побудови засобів візуалізації, що відрізняється адаптацією створюваних інструментів до умов завдання дослідження гетерогенних даних і до когнітивних можливостей користувача. Природнім наслідком стає існування підходу до розробки засобів візуалізації, що відрізняється способами подання і інтерпретації даних: створення універсальних систем, орієнтованих на широ-

ке практичне застосування, які характеризуються наявністю типового набору інформаційних об'єктів і відповідних йому способів візуального представлення. Завданням розробника засобів візуалізації є створення алгоритму перекладу досліджуваних даних у подання, що спирається на бібліотеку типових об’єктів.

У візуалізації даних на модель накладається обмеження на її обов'язкове використання як об'єкт зорового сприйняття. Надано визначення «*візуальної моделі даних*» – модель M даних D, об'єкт зорового сприйняття, зпівставлений цими данимі по визначенному контрольному правилу *V*, тобто *M = V(D)*. Також визначається *«функція візуального подання»* – правило зпівставлення *V*, що управляє побудовою візуального образа *I*. Функція візуального представлення – множина впорядкованих пар *(D, I)*, що задане на множині вихідних даних *D* і множини припустимих візуальних образів *I*.

Основним завданням візуалізації слід вважати знаходження функції візуального представлення *V*, що забезпечує візуальну модель *M* властивостями, достатніми для досягнення користувачем мети дослідження.

Другим напрямом моделювання є розробка вузькоспеціалізованих систем, що орієнтованих на використання в обмеженій предметній області, для яких характерне створення й розвиток способів візуалізації, що враховують особливості обмеженої предметної галузі, традиційні способи подання інформації й існуючі методи досліджень. Природнім недоліком спеціалізованих систем є недостатня застосовність для рішення завдань, що мають міждисциплінарний характер або пов'язаних з дослідженням об'єктів, що не мають певного типу. Неминучим ефектом використання візуалізації є вплив на свідомість спостерігача через формування нової інформаційної дійсності, пов'язаної з ілюзією об'єктивності візуалізації в процесі її інтерпретації. Для існуючих систем візуалізації використання зазначеного ефекту є резервом, залучення якого утруднено відсутністю систематизованого підходу до використання когнітивних аспектів візуалізації.

Таким чином, одним з актуальних питань слід вважати дослідження співвідношення в інтерпретації інформативного образа об'єктивної й суб’єктивної складових. У цьому випадку є необхідність обліку як властивостей образа, що піддано інтерпретації, так і умов його створення, специфіки сприйняття й інших аспектів. Сформульований підхід до візуалізації й когнітивної інтерпретації гетерогенних даних та запропонована система визначень, що включає наступні елементи: структурна одиниця візуалізації, класифікація завдань візуального дослідження, загальна результативність візуалізації. Також розроблений алгоритм побудови засобів візуалізації гетерогенних даних, відповідних до вимоги досягнення високої результативності візуального дослідження. Підставою запропонованого алгоритму є комплексний підхід до візуального аналізу даних. Розроблений алгоритм створює засіб візуального дослідження – адекватну візуальну модель гетерогенних даних, необхідну для досягнення мети дослідження. Спільне використання візуалізації й методів машинного навчання в завданнях дослідження гетерогенних даних дозволяє зробити доступним для вирішення за допомогою методів машинного навчання множини слабко формалізованих завдань.

Список літератури

1. Tory M., Moller T. Evaluating Visualizations: Do Expert Reviews Work // IEEE Computer Graphics and Applications. 2005. № 5 (25). p. 8–11.

2. Соломоник А. Очерк общей семиотики / А. Соломоник, Минск: МЕТ, 2009. 191 с.

Ляшик В. А., Шубін І. Ю.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДОСЛІДЖЕННЯ АДАПТИВНОГО ТЕСТУВАННЯ ЗНАНЬ В ДИСТАНЦІЙНІЙ ОСВІТІ

Контроль знань або тестування – це процес, що проводиться з метою визначення рівня знань і це є найбільш стандартизований і об'єктивний метод контролю й оцінювання знань, умінь і навичок випробуваного, який позбавлений таких традиційних недоліків інших методів контролю знань, як неоднорідність вимог, суб'єктивність екзаменаторів, невизначеність системи оцінок і т.п. Рівні знань зазвичай дискретизуються. При такому підході, тестування може розглядатися як деякий діагностичний процес, а стани, що характеризують оцінки знань випробуваного, – як діагностичні стани. Тести є ефективним засобом перевірки якості знань, одержуваних студентами, і оперативного контролю ходу навчання [1]. Розглядаються інформаційні освітні ресурси що містять, тестові матеріали, що використовують системи комп'ютерного тестування (СКС) з відповідним наповненням тестовими матеріалами.

Переваги тестових адаптивних ресурсів очевидні – вони дозволяють звільнити викладача від рутинної роботи при проведенні іспитів і проміжній оцінці знань у традиційному навчальному процесі, а при навчанні з використанням дистанційних технологій стають основним засобом контролю, надають можливість автоматизації обробки результатів, об'єктивність контролю й швидкість перевірки якості підготовки великого числа суб’єктів тестування по широкому колу питань. Це дозволяє визначити розділи, які представляють найбільшу складність у вивченні, і, можливо, коректувати процес навчання залежно від результатів тестування. Також інформаційні ресурси надають можливість реалізації навчальної функції та дозволяють зробити індивідуалізацію процесу засвоєння знань учнями.

Для забезпечення гнучкості в прийнятті рішень, простоти створення питань і правил, що визначають прийняття рішень для конкретного питання, доцільним є об'єднання питання й процедури ухвалення рішення, пов'язаної з ним. Такий підхід спрощує як процедуру тестування, так і саму систему тестування з погляду задоволення вимогам мінімальної складності застосовуваних алгоритмів.

Прийняття загальних для всього процесу тестування рішень, вимагає загальних підходів в одному сеансі тестування. Ці підходи визначаються застосуванням загального методу (або методів), що визначає той крок у процесі тестування, коли додаткова інформація про знання суб’єкта тестування буде надлишковою, процедурою початку роботи системи тестування (вибір першого питання) і стратегією переходу від одного питання до наступного також наданням докладних результатів тестування, як у природній, так і обробленої тими або іншими методами формі.

Це вимагає використання протоколу тестування й застосування:

- алгоритмів операційного й статистичного аналізу результатів тестування з погляду надмірності або недостатності інформації;
- алгоритмів, що визначають, рівень підготовки суб’єкта тестування;
- алгоритмів, що забезпечують стохастичні переходи по мережах тестових завдань.

Фактично, модель студента в окремій сесії визначається протоколом опитування та результатами оцінки знань.

Таким чином, даний підхід формує те, що є природнім для викладача, має аналог у класичнім розумінні іспиту й визначається як модель випробуваного.

У класичному розумінні мереж Маркова перехід з одного стану мережі в інше являє собою нескінченний процес. Існує також деякий початковий стан (у цьому випадку це випадково обраний питання заданого рівня складності), що є стартовою крапкою цих переходів. Вибираючи початковий рівень складності на початку тестування, і переходячи до іншого рівня складності, здійснюється перехід у підсистему,

певну для обраного рівня складності для якої слушні правила описані вище. Слід зазначити, що принцип залучення додаткових питань, що мають інший рівень складності, ніж обраний трохи ускладнює поведінку мережі. У випадку, коли додаткові питання, що належать основному питанню, утворюють фрагмент деревоподібної мережі, то при використанні якого-небудь додаткового питання із усього безлічі цих питань певного для тесту взагалі, гілка деревоподібної мережі (графа) знищується повністю. Такий же результат має місце тоді, коли це додаткове питання задане безпосередньо в контексті конкретного основного питання тесту, але в цьому випадку цей результат має місце після закінчення відповіді на додаткові питання, що належать його гілці.

Метою розробки прототипу програмного забезпечення є обґрунтування переваг застосування запропонованого методу формування тесту на основі мережі Маркова з елементами мереж Петрі, що включає в себе додаткові питання як частина основних питань і статистичну обробку, певну для малих вибірок даних при невідомому виді функції розподілу ймовірностей правильної відповіді з її наступної безпосередньою апроксимацією. Наведений алгоритм із ваговими коефіцієнтами для тем і основних питань є доречним, а результат у двох випадках практично однаковий незважаючи на різницю в шкалах оцінки (нормальну й логарифмічну).

При тестуванні й верифікації набору тестових завдань як продукту інформаційна технологія дозволить оцінити різницю витрат часу при автоматизованому тестуванні й з іншої сторони може бути використана для прогнозування традиційного іспиту як частини моделі, що визначає час, який затрачується на вибір додаткових питань.

Однак, при невеликій різниці між зазначеними передбачуваними й дійсними властивостями групи випробуваних застосування зазначеної методики дає позитивний ефект, із чого можна зробити висновок, що застосування запропонованого методу є ефективним для будь-яких обсягів і інших властивостей, що визначають тестування як процес.

Збільшення складності алгоритму тестування не приведе до яких або істотним витрат ресурсів ПК.

Список літератури

1. Бейкер, Р. Educational data mining and learning analytics/Р. Бейкер, Г. Сіменс – The Cambridge handbook of the learning sciences, 2019. – 274 с.

2. Дашкевич О. Аналіз можливостей Apache Kafka в рамках забезпечення стримінгу Big Data // Информационные системы и технологии: Материалы 7-й Международ. науч.-техн. конф. 2018. № 12. С. 34-35.

УДК 004.852

Мустафаєв Є. О., Шубін І. Ю.

МОДЕЛІ АВТОМАТИЧНОГО ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ІНФОРМАЦІЙНОГО ПОШУКУ

Тематичні моделі – це сімейство імовірнісних генеративних моделей, використовуваних для визначення тематики документів на основі їх умісту. У загальному випадку під темою розуміється імовірнісний розподіл над «словами» документа. У якості ілюстрації можна привести природній приклад текстових документів наприклад, новини.

Інший випадок – тематичне моделювання зображень, де під «словами» розуміються невеликі фрагменти, що відображують різні візуальні елементи, які зустрічаються на зображеннях. Темами тут можуть бути, наприклад, смужки, особи людей або текстура

тла. У тематичних моделях зазвичай передбачається, що кожний документ колекції містить у собі суміш різних тем, представлених з певною ймовірністю. Однієї з перших тематичних моделей вважається модель імовірнісного латентно-семантичного аналізу (Probabilistic Latent Semantic Analysis, PLSA), запропонована [1].

Усі покажчики якості, інформаційного пошуку визначені в припущенні, що покажчик релевантності є індикаторною функцією, значення якої рівно 1, якщо документ релевантний, і 0, якщо інакше. Однак часто розробка нових методів вимагає оцінювати ступінь релевантності документа по деякій шкалі (наприклад, від 1 до 5). Щоб урахувати шкалу релевантності в оцінці, сучасні дослідження часто використовують нормовану дисконтовану сукупну вигоду[2].

Важливим етапом у розробці будь-якого методу оцінки якості контенту є визначення й фіксація поняття якості. Різні джерела описують даний термін по-різному. Або сприймають якість відповіді як щось зовнішнє стосовно авторів питання й відповіді – «об'єктивне» знання, або напроти, виходять із того, як сприймається якість автором питання, тобто, наскільки відповідь суб'єктивно задовольняє його інформаційну потребу. Базовим сценарієм персоналізації інформаційного пошуку є використання історії минулих дій користувача в пошуковій системі для поліпшення якості результатів його поточного запиту. Наприклад, можна використовувати попередні запити користувача, дані відвіданих їм веб-сторінок і переглянутих документів для побудови моделі інтересів користувача, на основі якої й відбувається подальша персоналізація пошукової видачі.

Використання соціальних зв'язків користувача для персоналізації пошуку в соціальній мережі: модель інтересів у цьому випадку будується на основі пошукових стратегій «близьких» користувачів (тобто тих, з ким шуканий спілкується найбільше) або користувачів, ведучих себе в соціальній мережі схожим образом. Використовується порівняння ефективності персоналізації пошуку в різних умовах. Зокрема затверджується, що методи, засновані на моделях інтересів користувачів, показують нестабільне поліпшення в порівнянні із простим аналізом кліків користувача.

Загалом, користувацький контекст може бути розглянутий під різними кутами. Слід розрізняти контекст обладнання (дані, отримані з обладнання користувача), просторово-часовий, а також особистісний контекст, під яким розуміються характеристики конкретного користувача. Особистісний контекст поєднує поняття персонального і соціального контексту. У такий спосіб методи одержання, обробки й аналізу контекстної інформації залежать від типу використовуваного контексту.

Існуючі методи персоналізації інформаційного пошуку спираються, в основному, на класичні підходи до витягу релевантної інформації. Часто стадія персоналізації вбудовується у звичайний цикл обробки запиту й видачі результатів. Використовано методи вбудовування на етапі обробки запиту (наприклад, модифікація запиту), під час ранжирування (модифікація функції ранжирування) або після ранжирування (переранжування пошукової видачі).

У роботі запропонований метод, що домішує до видачі по початковому запиту кілька видач по запитах, розширених полями користувача. Запит, розширений одночасно більшим числом полів з історії пошукових запитів користувача, може вийти досить довгим. Дослідження показують, що збільшення довжини запиту в середньому поліпшує якість пошуку. Поряд із цим, при обробці подібних запитів виникає ряд проблем. Середня довжина запиту в пошукових системах мережі Інтернет становить за різними оцінками 2-3 слова, що змушує розробників сучасних систем оптимізувати метрики якості пошуку для коротких запитів. У випадку з довгими запитами пошукові системи можуть поводитися по-різному: у процесі обробки обрізати запит, намагатися шукати всі терміни в одному документі (що спричиняє падіння повноти пошуку) тощо. Крім того, у пошукових системах часто використовується модель «мішка слів» (bag of words), згідно з якою в документах і запиті не враховується по-

рядок слів. Ця обставина може стати причиною падіння точності пошуку у випадку витягу документів по підмножині слів запиту. Така ситуація можлива через те, що довгий запит породжує велику кількість підмножин, багато з яких не є релевантними. В запропонованому методі моделювання користувача пошукової системи на основі даних його історії пошуку інформації. Реалізований відповідний алгоритм персоналізації пошуку по колекції веб-сторінок обраної тематики. Зокрема, реалізовані відповідні комплекси проблемно-орієнтованих програм. Зокрема, реалізований ефективний алгоритм виправлення орфографічних помилок і друкарських помилок. Розроблений новий метод автоматичної оцінки компетентності користувача соціальних сервісів питань-відповідей, дослідження торкається питань якості інформації в подібних сервісах і універсальних пошукових системах. У якості однієї зі складових методу запропонована модель тематичного фокуса користувача.

Отже, в якості рішення вищеописаної проблеми в роботі пропонується замість одного запиту, розширеного більшим числом полів, робити кілька запитів, розширених малим числом полів. Отримані пошукові видачі документів пропонується змішувати й упорядковувати за допомогою додаткової функції ранжирування, у загальному випадку відмінної від тієї, що використовується усередині основної пошукової системи. Тоді в кожному випадку пошукова система буде виконувати більш конкретне завдання, а у фінальній видачі буде врахований не тільки основний запит користувача, але й персональні дані його організму.

Список літератури

1. Маннинг К., Рагхаван С., Шютце Х. Введение в информационный поиск. : Пер. с англ. - М. : ООО "И.Д. Вильяме", 2011. - 528 с.
2. Teevan J., Dumais S., Horvitz E. Personalizing Search via Automated Analysis of Interests and Activities // Proceedings of SIGIR’05 Conference. — 2005. — P. 449-456.

УДК 004.852

Циблієва Н. О., Шубін І. Ю.

ДОСЛІДЖЕННЯ МЕТОДІВ АНАЛІЗУ БЕЗПЕКИ СЕМАНТИЧНИХ БАЗ ДАНИХ

Слова «семантичні технології» часто зустрічаються в описах концепції «Семантична Павутина» (Semantic Web), запропонованої в [1]. Ціль Семантичної Павутини полягає в додаванні структурованої метаінформації до існуючих в WEB-мережі документів і даним для явного опису їх семантики, що дозволяє програмам виконувати більш якісну роботу із цими даними. В подальшому в даній роботі під семантичними технологіями будуть розумітися семантичні технології концепції Semantic Web. Семантичні технології складаються з багаторівневого набору різних стандартів і технологій, в яких кожний рівень використовує можливості нижчих рівнів.

Сучасні інформаційні системи установ і організацій створюються на основі реляційних БД. При проектуванні структур реляційних БД враховується семантика даних, під якою розуміється зміст, що лежить у їхній основі, що може бути описаний за допомогою взаємозв'язків між різними поняттями і їх властивостями. Після створення БД використовуються отримані схеми БД (таблиці й зв'язки між ними), а робота із семантикою даних вже не виконується. Однак у наш час в інформаційних системах усе більше потрібно працювати не тільки із синтаксисом даних, але й з їхньою семантикою, що дозволяє підвищити якість роботи інформаційних систем за рахунок більш якісного опису ресурсів з використанням семантичних метаданих і

виконання логічних висновків. Уся ця інформація зберігається в спеціальних БД, які називаються семантичними БД. Семантичні моделі й дані семантичних інформаційних систем описуються з використанням спеціальних мов, які входять до складу семантичних технологій Semantic Web. Для роботи із семантикою даних вже розроблені й продовжують розроблятися спеціальні семантичні технології, під якими розуміється набір стандартів і методів, що дозволяють описувати зміст даних (їх семантику) і виконувати роботу з ними [2].

Онтології почали використовуватися в області інформатики з 1980-х років дослідниками, що працюють в галузі штучного інтелекту. Спочатку вони використовувалися для обробки природної мови, а потім і для представлення знань. В 1990-х роках почалося дослідження можливості використовувати онтології для інтеграції й пошуку інформації в БД і мережі Інтернет. Пізніше онтології стають основними ключовими елементами, використовуваними для реалізації концепції семантичної мережі.

В роботі використовується визначення онтології, як формального, точного опису (специфікації) погодженої концептуалізації». У даному визначенні термін «формальна» означає, що онтологія є машиночитною структурою. Під терміном «погоджена концептуалізація» мається на увазі, що даний концептуальний опис не є чиєюсь приватною думкою, а думкою, з якою згодна деяка група людей. А під терміном «концептуалізація» розуміється структура реальності, розглянута незалежно від словника предметної області й конкретної ситуації. Онтологія включає модель (схему), що представляє собою опис множини понять і відносин між ними (онтологічна модель) і екземпляри понять. Опис онтологій ґрунтується на формальних логіках. У якості таких логік використовується описова логіка.

В роботі використовуються три способи класифікації онтологій: за ступенем формальності, за метою створення (призначення) і за змістом. У свою чергу ці типи онтологій містять у собі подальшу класифікацію. Ступінь формальності онтології відображає, як описується зміст онтології.

За допомогою прямих запитів користувачі U можуть переглянути окремі елементи СБД, кожний триплет або набір RDF-триплетів. За допомогою використання логічних запитів вони можуть отримувати результати логічних висновків. У зв'язку із цим для забезпечення безпеки СБД необхідно контролювати виконання кожного виду запитів користувачів і гарантувати, що вони отримують відповіді на відправлені запити відповідно до їхніх рівнів доступу. Завдання дослідження полягає в контролі результатів, отриманих користувачами при виконанні запитів.

Метод виявлення порушень результатів логічних висновків – множина триплетів може бути презентованою у вигляді RDF-графа, де кожний триплет відповідає одному спрямованому ребру, що зв'язує дві вершини. З урахуванням цього, набір онтологій і множина семантичних метаданих можуть розглядатися як RDF-граф Q. Користувачеві U, відповідно до його рівня доступу sl_U, дозволяється бачити тільки деякі вершини (суб'єкт, об'єкт триплетів) і ребра (предикат триплетів) графа Q. Однак користувач шляхом застосування логічних правил R до вершин, що є видимими і ребрам може спробувати отримати зв'язки до інших вершин і ребер (отримати результати логічних висновків R_L). Для рішення задачі контролю результатів логічних висновків необхідно визначати можливості за результатом логічних висновків між двома вершинами й контролювати нові отримані вершини й ребра. З обліком цієї задачі виявлення порушень результатів логічних висновків може бути розділена на такі підзадачі, як представлення семантичних БД у вигляді RDF-графів, визначення можливості отримання результатів логічних висновків між двома вершинами та контроль отриманих результатів логічних висновків. Процес контролю доступу користувачів до елементів БД виконується в такий спосіб: при кожному вході користувача в систему за допомогою модуля «перевірка облікового запису користувачів» виконується перевірка наявності його облікового запису, рівня доступу й прав доступу, інформа-

ція про які зберігається в СБД, а при відправленні користувачем запитів, система виконує їхню перевірку за допомогою модуля «перевірка запиту». Система визначає рівні безпеки всіх елементів онтологій і триплетів у СБД. Дана програма гарантує, що користувачі виконають операції над даними семантичних БД і отримають результати відповідно до їхніх рівнів і прав доступу.

Отже, в рамках виконання даного дослідження сформовані теоретичні основи для вирішення завдання підтримки безпеки роботи з семантичними БД. Створено метод виявлення порушень результатів логічних висновків в семантичних БД, що виявляє всі можливі порушення безпеки результатів логічних висновків та розроблено алгоритм контролю отриманих результатів при виконанні запитів до семантичним БД, що гарантує отримання відповідей на запити користувачів відповідно до їх рівнів безпеки. Запропоновано оригінальну архітектуру забезпечення безпеки семантичних БД, що дозволяє з допустимими затримками забезпечити підтримку безпеки СБД при інтенсивному навантаженні.

Список літератури

1. Kienast R. Semantic Data Integration on Biomedical Data using Semantic Web Technology / R. Kienast, C. Baumgartner // Trends and Methodologies. – 2011. – P. 57–76.
2. Hendler A. J. Handbook of Semantic Web Technologies. – Springer, 2011. – 479 p.

Швець К. В., Шубін І. Ю.

ДОСЛІДЖЕННЯ МОДЕЛЕЙ ЕВОЛЮЦІЇ КЛАСТЕРІВ В ЗАДАЧАХ РОЗПІЗНАВАННЯ

Розширення функціональних можливостей, ускладнення й збільшення числа завдань, розв'язуваних сучасними мережевими інформаційно-керуючими системами (ІКС), що забезпечують автоматизоване керування, контроль, інформаційну підтримку прийняття рішень в умовах реального часу в складних технічних системах, вимагають розвитку й удосконалення методів їх комп'ютерного моделювання, що передують етапам проектування, розробки й експлуатації. У сучасних умовах ускладнення мережевих ІКС найбільш гостро відчувається недолік методів і інструментів оцінки продуктивності й надійності, особливо для мережевого програмного забезпечення (ПЗ) в умовах виникнення граничних інформаційних навантажень, які суттєво впливають як на діяльність, так і на надійність. Такі інформаційні навантаження часто мають нетривалий, «сплесковий» характер, тому в контексті роботи називаються піковими інформаційними навантаженнями [1].

Основною метою роботи є розгляд ряду випадкових процесів і алгоритмів їх моделювання, застосованих у якості базової складової методів оцінки надійності ПЗ, які використовують опис процесів виявлення програмних помилок на етапах його розробки й тестування.

Для мережевих ІКС, як багатокористувацьких, мультизадачних, багатомашинних і багатопроцесорних систем, характерним є ще один аспект подійності – конкуренція за мережеві розподілені обчислювальні ресурси з метою збільшення продуктивності, мінімізації простоїв і таке інше. Обидва цих аспекта – синхронізація й конкуренція – роблять мережеві комп'ютерні системи значно більш нелінійними, що ускладнює їхнє аналітичне й імітаційне моделювання, а запропоновані в роботи методи й чисельні алгоритми можна розглядати як можливу лінеаризацію з метою спрощення моделювання таких систем. Кінцевим інструментом дискретно-подійного моделювання є розроблене в роботи спеціалізоване ПЗ, що реалізоване на функціональних та імперативних мовах програмування.

В основу дискретно-подійного моделювання, що розвивається появи відомої системи GPSS [2] і мереж Петрі [3] покладена інша концепція: стану системи змінюються під впливом деяких подій, у загальному випадку безвідносно їх точної прив'язки до тимчасової шкали. Істотними є лише факти наявності виникнення цих подій і взаємодія їх між собою, тобто синхронізація (деяка подія передує іншому, деяка подія викликає виникнення іншого, або інших подій і так далі). Прикладом таких інформаційних систем є мережеві комп'ютерні системи. Для мережевих комп'ютерних систем, як багатокористувацьких багатозадачних, багатомашинних, багато процесорних систем, характерним є ще один аспект подійності – конкуренція за мережеві розподілені обчислювальні ресурси, з метою збільшення продуктивності, мінімізації простоїв і таке інше. Обоє ці аспекти – синхронізація й конкуренція роблять мережеві комп'ютерні системи суттєво нелінійними, що ускладнює їхнє аналітичне й імітаційне моделювання, а розглянутий далі в роботі підхід можна розглядати як можливу лінеаризацію таких систем. Подійно-орієнтоване моделювання в дискретно-подійній системі, проілюстроване на рис.1.

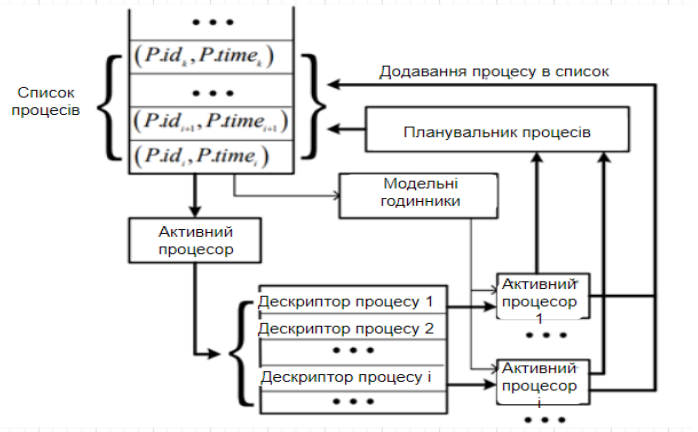


Рисунок 1 – Подійно-орієнтоване моделювання

Більшість систем, застосовуваних у якості засобів автоматизації технологічних процесів на виробництві, у промисловості, на транспорті й в інших галузях є програмно-керованими. Якість функціонування таких систем залежить не тільки від якості апаратних засобів, застосовуваних у їхньому складі, але й від якості ПЗ, найважливішою характеристикою якого є надійність.

Отже, розроблено модель аналізу продуктивності мережевої системи з встановленням граничних значень показників продуктивності для рішення завдань моделювання систем з гарантованим обслуговуванням. Це підтверджується виконанням алгоритму чисельного розрахунку функціонала оцінки пікового інформаційного навантаження на основі апроксимації випадкових точкових процесів експонентними процесами відновлення. Дискретно-подійний підхід для оцінки надійності програмного забезпечення, що використовує покомпонентно технологію моделювання подій виникнення помилок на вході й виході програмного компонента. Процеси виявлення й усунення помилок моделюються випадковими точковими процесами, а час виявлення помилок зпівставляється з подіями, при виникненні яких потрібно розрахувати ймовірнісні оцінки надійності програмних компонентів, які залежно від реалізованих ними алгоритмічних структур мають різні формули для розрахунку.

Такі класи алгоритмів призначено для моделювання випадкових точкових процесів і відповідних їм, що вважаються випадковими процесами з безперервним часом: на основі одномірних неоднорідних випадкових процесів з одним датчиком; на основі одномірних неоднорідних випадкових процесів із двома датчиками; двовимірних неоднорідних випадкових процесів на колі й в області, обмеженою деякою функцією.

Список літератури

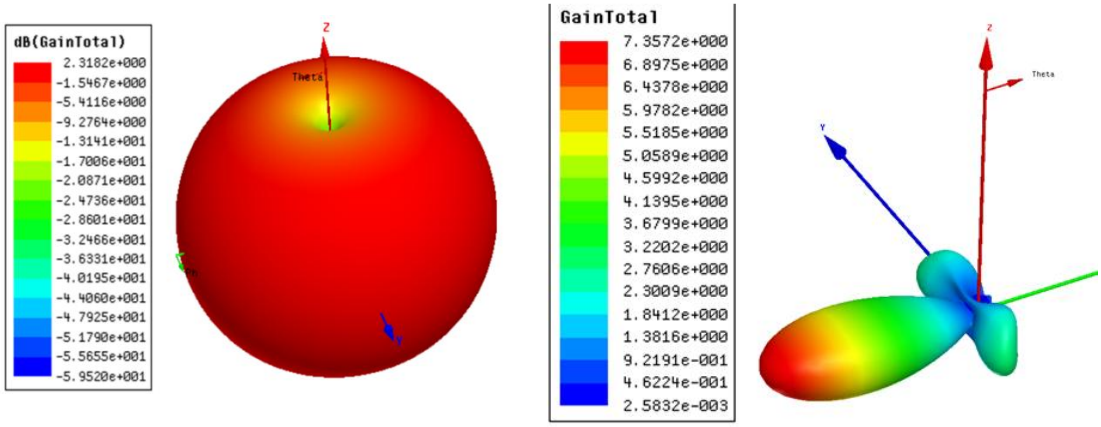
1. Baccelli F. Synchronization and linearity: An algebra for discrete event systems / Baccelli F., Cohen G., Quadrat J.-P. – Chichester: Wiley. – 1992. – 514 p.
2. Бражник А. Н. Имитационное моделирование: возможности GPSS WORLD. — СПб.: Реноме, 2006. – 439 с.
3. Котов В.Е. Сети Петри.- М.: Наука, 1984. – 160 с.

УДК 623.55.02

Малюк В. Г., Казіміров О. О., Борзенков Б. І.

СПОСІБ ШВИДКОГО ОБЧИСЛЕННЯ ЗНАЧЕНЬ ТРИВИМІРНОЇ ДІАГРАМИ СПРЯМОВАНОСТІ АНТЕННОГО ПРИСТРОЮ У ПРОГРАМАХ КОМП'ЮТЕРНОГО МОДЕЛЮВАННЯ РАДІООБМІНУ

Для комп'ютерного моделювання засобів радіозв'язку UHF/VHF діапазону необхідно розрахувати тривимірну просторову функцію напруженості поля антенного пристрою в полярних координатах $G(\theta,\varphi)$, де θ - кут азимута, а φ - кут місця. Форму діаграми спрямованості (ДС) антенної системи при наявності відповідних креслень можна обчислити за допомогою програмних засобів моделювання тривимірних електромагнітних полів, наприклад, таких як HFSS Ansoft [1, 2]. На рис. 1а наведено взятий з [3] приклад розрахунку неспрямованої ДС дипольної антени, виконаний в програмі HFSS Ansoft. На рис. 1б наведено приклад розрахунку спрямованого антенного пристрою, що складається з дипольної антени і металевого екрану.



а) дипольна антена б) спрямований антенний пристрій

Рисунок 1 – Приклади розрахунків ДС для антен різних типів

Результатом розрахунку ДС є її нормовані перетини $D_g(\theta), \theta \in [0^0, 360^0]$ і $D_v(\varphi)$, $\varphi \in [-90^0, 90^0]$, табульовані з кроком у 10^0 в горизонтальній і вертикальній площині відповідно. Тривимірну функцію ДС антенного пристрою можна отримати наступним чином:

$$G(\theta,\varphi) = D_g(\theta) * D_v(\varphi). \quad (1)$$

Одним з варіантів обчислення значень функції $G(\theta,\varphi)$ у програмах комп'ютерного моделювання радіообміну є використання окремої обчислювальної процедури, яка для заданих кутів азимуту θ та куту місця φ використовує операцію

кусочно-лінійної інтерполяції на основі табульованих значень $D_g(\theta)$ та $D_v(\varphi)$. Однак використання такої процедури, виправданої для одиночних обчислень, суттєво уповільнює роботу програми моделювання радіообміну у трудомістких задачах обчислення меж зони електромагнітної сумісності [3] або задачах розміщення засобів активного радіомаскування направленої дії [4].

Для прискореного обчислення значень функції (1) у програмах комп'ютерного моделювання радіообміну пропонується виконати попереднє табулювання функції $G(\theta,\varphi)$ з кроком у 1^0, використовуючи за необхідності операцію кусочно-лінійної інтерполяції. Результати розрахунків розміщуються у двовимірній матриці $MG[0..360][-90..90]$, діапазон індексів якої відповідає діапазону значень аргументів функції (1): $\theta \in [0^0, 360^0]$ та $\varphi \in [-90^0, 90^0]$. Таким чином, використання окремої обчислювальної процедури замінюється звертанням до елементу матриці, що суттєво прискорює роботу програми комп'ютерного моделювання радіообміну.

Список літератури

1. ANSYS HFSS. 3D Electromagnetic Field Simulator for RF and Wireless Design. URL: https://cutt.ly/wdugp1J (дата звернення 01.08.2020).

2. Банков С.Е., Курушин А.А. Расчет антенн и СВЧ структур с помощью HFSS Ansoft. М.: ЗАО «НПП «РОДНИК», 2009. 256 с.

3. Iohov O., Maliuk V., Horielyshev S., Tkachenko K., Herasimov S. Development of a Method for Boundary Determination of the Noise-resistant Area of the UHF/VHF Band. *Advances in Military Technology*, 2020, vol. 15, no. 2, pp. 231-246. DOI 10.3849/aimt.01376

4. Іохов О.Ю., Малюк В.Г., Ткаченко К.М. Програма обчислення зони розміщення засобів активного радіомаскування засобів радіозв'язку військових підрозділів на ділянці фронту. *Application of information technologies in the preparation and operation of law enforcement forces*: зб. тез доп. міжнар. наук.-практ. конф. м. Харків, 15 бер. 2019 р. Харків: НАНГУ, 2019. С.144

УДК 37.022

Шамшин О. П.

ВИКОРИСТАННЯ ГРАФОВОГО МЕТОДУ ПРИ РОЗВ'ЯЗАННІ ЗАДАЧ З ФІЗИКИ В ЗВО

Бурхливе впровадження інновацій у вищих технічних закладах освіти приводить до кардинальної перебудови змістової і технологічної складових підготовки майбутніх фахівців, визначає перебудову і модернізацію класичної системи вивчення фундаментальних курсів, розробку і впровадження нових методичних засобів навчання фізико-математичних дисциплін.

Інформаційно-комунікаційні технології (ІКТ) суттєво змінюють систему викладання фундаментальних дисциплін, і фізики, зокрема, що склалася в докомп'ютерну еру. Активне впровадження сучасних ІКТ в освіті сьогодні є не тільки необхідною умовою подальшого розвитку сучасного суспільства, але і нагальною вимогою для успішного функціонування навчального закладу будь-якого рівня. У закладах вищої освіти впровадження ІКТ здійснюється за багатьма напрямками, однин з яких – використання комп'ютерних засобів для розв'язку фізичних задач.

Одною з сучасних вимог до підготовки з фізики студентів ЗВО є формування ін-

формаційного середовища навчання фундаментальним дисциплінам. Завдяки інноваційному підходу для студентів створюється можливість приймати активну участь в освітньому процесі, опановувати новий досвід креативного мислення та використання сучасного інструментарію навчальної, наукової та дослідницької діяльності.

Як правило, фізична задача представляється у вигляді текстової задачі – word problem (WP). У зв'язку зі швидким розвитком методів NLP штучного інтелекту (AI) розв'язок WP активно вивчається, розглядається в багатьох роботах, але навіть у найпростіших WP з арифметичними діями, знаходження рішення за допомогою AI є нетривіальним, виконаним для певного кола задач. Перехід до нового класу задач вимагає зміни алгоритму дій. Процес пошуку відповіді на WP у психології розглядається як перекодування, переформулювання інформації, що міститься в тексті, так званої задачної ситуації, викладеної природньою мовою вербальним образом за допомогою графічних і знакове-символьних елементів, на мову математичних символів, функцій, рівнянь.

Уніфікація розв’язування фізичних задач може бути досягнута при використанні теорії графів, зокрема обчислювальних графів, які дають наочне уявлення про покроковий «шлях», «маршрут» рішення задачі, дозволяють автоматизувати цей процес завдяки його діджиталізації в контексті віртуалізації освітнього середовища предметної області фізики [1].

Моделювання графами, як один з напрямків математичного моделювання, використовується при дослідженні структурованих об'єктів. При цьому виконується умова взаємне однозначної відповідності між елементами моделі й об'єкта. На сьогоднішній день у фізиці є області, де графи з успіхом застосовуються десятиліттями – електротехніка: матриця Кірхгофа при записі законів Кірхгофа, у методі контурних струмів, вузлових потенціалів, еквівалентного генератора. Квантова теорія поля: діаграми й правила Фейнмана, які зіставляють кожному елементу діаграми Фейнмана певні математичні об'єкти (величини й операції), так що по діаграмі Фейнмана можна однозначно побудувати аналітичне вираження, що дає внесок в амплітуду розсіювання квантованих полів. У системах із взаємодією може бути побудована відповідна діаграмна техніка у вигляді графів для температурних функцій Гріна. Ця техніка широко використовується при вивченні фазових переходів у надпровідниках, надтекучості, температурі Кюрі в різних системах. У фізиці конденсованого стану можна описати просторові стани деяких моделей шляхами у відносинах граф – суміжність. Статична модель кристалічної структури у вигляді точкове-штрихової (граф) *r*'-моделі. Графи Келі кристалографічних груп.

Разом з тим недостатньо вивчене використовування графів при розв'язку WP по фізиці в технічному вузі. Таке застосування обмежується побудовою дерева задачі, по якому в одних випадках знаходиться кількість рівнянь необхідних для розв'язку, а в інших - по дереву задачі визначається рівень її складності [2]. У роботі розглядається побудова обчислювального графа задачі, який складається із двох видів циклів, що описують функціональні зв'язки фізичних величин і співвідношення між ними. Додавання або видалення циклів дозволяє масштабувати розв'язок задачі у випадку зміни умови. Застосування запропонованого графового методу дозволяє підвищити ефективність навчання за рахунок удосконалення змістовної частини структури розв'язку, у якій чітко видні методи розв'язку, завдяки використанню єдиної матриці суміжності графа для функціональних і реляційних зв'язків фізичних величин і побудові шляху графа, який, по суті, є послідовним записом рівнянь, необхідних для знаходження шуканої величини.

Список літератури

1. Шамшин О.П. Віртуалізація фізики та психолого-педагогічні аспекти / О.П. Шамшин // Фізико-математична освіта. - 2020. - №4 (26). - С. 134–140.

2. Быкова Н.П. Графовое моделирование структур решений задач как средство их систематизации / Н.П. Быкова, Н.Г. Рыженко // Математические структуры и моделирование. - 2004. - Вып. 14. - С. 128-139.

УДК 681.5.015

Дядюн С. В.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОЦЕСІ ВИРОБЛЕННЯ І ПРИЙНЯТТЯ РІШЕНЬ

Основою управління є рішення. Помилки від невірно прийнятих рішень осіб, які приймають рішення (ОПР), можуть призвести не тільки до економічної катастрофи для окремого підприємця або галузі, а й до глобальної катастрофи для людства. Дієвим способом підвищення ефективності та якості управління є оволодіння топменеджерами методологією системного аналізу і прийняття рішень на основі математичних методів. При цьому в ролі інтелектуального помічника людини виступає комп'ютер. При вирішенні задач управління, зокрема, задач теорії прийняття рішень (ТПР), ОПР постійно використовує аналіз і синтез, системний підхід і конкретно-формальні методи.

Проблема прийняття рішень – одна з найпоширеніших в будь-якій предметній області. Її рішення зводиться до вибору однієї або декількох кращих альтернатив з деякої їх безлічі. Для того, щоб зробити такий вибір, необхідно чітко визначити мету і критерії (показники якості), за якими буде проводитися оцінка деякого набору альтернативних варіантів. Вибір методу вирішення такої задачі залежить від обраних цілі, альтернатив, критеріїв вибору, кількості і якості доступної інформації.

Дані, необхідні для здійснення обгрунтованого вибору, можна розділити на такі категорії: інформація про альтернативні варіанти, інформація про критерії вибору, інформація про переваги, інформація про оточення задач.

До класу задач прийняття рішень в умовах визначеності належать задачі, для вирішення яких є достатня і достовірна кількісна інформація. У цьому випадку застосовуються методи математичного програмування.

Задачі прийняття рішень в умовах ризику мають місце, коли існує можливість описати настання того чи іншого результату з певною ймовірністю. Для побудови розподілу ймовірності настання результатів необхідно мати представницьку статистику результатів спостережень або знання експертів. Зазвичай для їх вирішення застосовуються методи одновимірної або багатовимірної корисності. Ці задачі займають проміжне положення між задачами в умовах визначеності та невизначеності.

Задачі прийняття рішень в умовах невизначеності мають місце, коли інформація, необхідна для прийняття рішень, є неточною, неповною, некількісною, багатокритеріальною, недостовірною, а формальні моделі досліджуваної системи дуже складні, або відсутні. В цьому випадку використовуються знання експертів, виражених кількісно, які називаються *уподобаннями*.

Задачі прийняття рішень в умовах конфлікту - найбільш складний і мало розроблений із практичної точки зору аналіз. На практиці ця і попередня ситуації зустрічаються досить часто. У таких випадках їх намагаються звести до однієї з перших двох ситуацій або використовують для ухвалення рішення неформалізовані методи.

В залежності від масштабу проблеми, прийняті рішення можуть бути *стратегічними, тактичними і оперативними*. Методи ТПР найбільш широко застосовуються на стратегічному рівні, рідше на тактичному, і дуже рідко на оперативному та при прийнятті особистих рішень. У ТПР центральне місце займають багатокритеріальні

задачі вибору. Облік багатьох критеріїв наближає постановку задачі до реального життя. Слід виділити такі основні задачі прийняття рішень:

1. Впорядкування альтернатив;
2. Розподіл альтернатив за класами рішень;
3. Виділення кращої альтернативи.

Основні ознаки, які використовуються для побудови класифікації рішень:

1) ступінь розробки (запрограмовані і незапрограмовані рішення);
2) ступінь обґрунтування (інтуїтивні, логічні, раціональні рішення);
3) можливість реалізації (допустимі, неприпустимі рішення);
4) ступінь досягнення мети (нерозумні, задовільні, оптимальні рішення);
5) рівень творчого вкладу (рутинні, селективні, адаптивні та інноваційні рішення).

В даний час у зв'язку зі збільшеними можливостями сучасних комп'ютерів розроблені програмні інформаційні системи, що забезпечують підтримку процесу вироблення та прийняття рішень на всіх його фазах.

Натурний експеримент завжди обмежений за часом і ресурсами. У всіх ситуаціях він призводить до зниження невизначеності. Натурний експеримент часто неможливий, проте володіє максимальною достовірністю, будучи критерієм фактичного вирішення проблемної ситуації.

Експертне дослідження проблемної ситуації характеризується тим, що загальна інформація про ситуацію обмежується особистісним знанням експерта. Однак експертне знання має найважливішу властивість концентрованості на найважливіших групах альтернатив. Модельні дослідження ситуації пов'язані з формалізацією опису ситуації, вибором належного критерію адекватності моделей і модельованих ситуацій. Безпосереднє дослідження ситуації на моделі завершується інтерпретацією результатів моделювання для перерозподілу переваги альтернатив. Властивості всіх трьох класів натурних, модельних, експертних операцій над альтернативами ситуацій змушують для досягнення максимальної ефективності системного аналізу здійснювати раціональне комбінування експертних, модельних і натурних досліджень при виборі альтернатив. Кінцевим результатом операцій натурного, модельного та експертного дослідження альтернатив є або виграш у часі, або економія ресурсів, необхідних для досягнення заданого рівня визначеності проблемної ситуації. Засоби вирішення проблемної ситуації включають комп'ютерні технології та спеціальні організаційні структури, наприклад, групи системного аналізу. Комп'ютерні технології підтримують всі види експериментів і методів отримання інформації про переваги альтернатив. Існують різні комп'ютерні технології планування та управління ситуаційним експериментом.

До комп'ютерних технологій відносяться і технології експертних систем. Комп'ютерні технології моделювання ситуації найчастіше реалізують технологію ділових ігор, що проводяться групами системного аналізу. Натурні дослідження ситуації включають вибір факторів, які повинні впливати на вибір кожної групи альтернатив. Необхідно вибрати також критерій ефективності натурного дослідження, який залежить від значень факторів. Поєднання всіх можливих факторів і їх рівнів утворює безліч допустимих станів проблемної ситуації. Експертні дослідження ситуації часто здійснюються за допомогою експертних систем. Експертні системи розширюють діапазон достовірного дослідження проблемної ситуації і виділяють з даних інформацію, суттєву для перерозподілу альтернатив проблемної ситуації. Комплекс системного інформаційного забезпечення ситуаційного аналізу включає раціональні методи поєднання модельного, натурного і експертного дослідження проблемної ситуації.

У доповіді розглядаються інформаційні технології вироблення та прийняття рішень. При цьому приділяється увага розробленим автором 6 тестам для навчання студентів з дисципліни ”Теорія прийняття рішень” для студентів спеціальності

122 - Комп'ютерні науки. Навчальні тести використовуються в Moodle, причому підсумковий тест містить 180 питань, по 30 з яких кожен студент отримує випадковим чином для оцінювання набутих знань, після чого одразу з'являється оцінка його відповіді. Тести охоплюють широкий спектр матеріалу з даної тематики, і можуть бути використані не тільки для навчання студентів університетів та курсантів військових закладів освіти, а й для підготовки і тренінгу керівного складу та працівників різних організацій і підприємств, комп'ютерних та будь-яких інших фірм.

UDK 681.3.07

Novykova O., Glushchenko M.

COMPUTER TECHNOLOGIES OF LEARNING IN TRAINING OF MILITARY SPECIALISTS IN COMMUNICATION ORGANIZATION FOR NGU UNITS

The most difficult tasks of the National Guard of Ukraine (NGU) in the law enforcement forces are to eliminate the possible consequences of emergencies and to stop mass riots in the state region. Their solution requires a comprehensive situational approach, taking into account the scale and complexity of the problem. Therefore, there is a question of improving the quality of training of military specialists to ensure the management of the actions of NGU units by means of communication to quickly solve professional problems.

The traditional way of forming a sufficient level of professional training of servicemen and its further improvement (command and staff exercises, training, military games, etc.) is often economically inefficient. In addition, when working with a standard group of cadets of 25 people, even a highly qualified teacher is faced with different levels of initial training and motivation of cadets and their psychophysiological characteristics. Also, in traditional mass learning, the teacher can not individualize the pace of learning, quickly control the level of learning material, assesses the knowledge of cadets subjectively, even in the presence of assessment criteria. Because a person's short-term memory is limited (Miller's number), the teacher cannot track each cadet's acquisition of the necessary knowledge and skills.

In the world practice of training military specialists of various profiles, there are positive results of the introduction into the educational process a means of technical training (computer training programs and stands), military simulators of varying complexity and military computer games. This eliminates the above disadvantages of traditional learning.

With regard to NGU units, joint exercises and trainings with the use of simulation systems are offered. Another application of computer technology in the training of military specialists is the creation and implementation of intelligent computer learning systems (ICLS), which can adapt to the level of knowledge, skills and abilities of the cadet and provide direct feedback through intellectual analysis and answers support. Such systems are performed with an advanced interface, means of recording the knowledge and skills of cadets and diagnosing their mistakes. The core of ICLS is the unit for solving stadying tasks. In this case, it is important not only the correctness of the answer, but also the process of obtaining it, because it forms the necessary components of competence. According to the concept of a universal environment for graphical creation of ICLS, the process of their creation is to develop a set of tasks, determine the properties of each of them, combine them into a project and develop an algorithm for calling tasks in the form of a pedagogical scenario [1]. An individual approach to each cadet is carried out in the external management cycle of ICLS, the pedagogical scenario of tasks and the internal cycle of each of them. The external cycle is designed to select the next task of a certain

level of complexity on a topic of the discipline. The pedagogical scenario allows to divide the learning material into such parts at mastering of which the cadet acquires certain knowledge and skills. The internal cycle is designed to decompose a single task into steps and decide to provide the next step for cadets. The task must be solved in the minimum number of steps.

Thus, on the basis of computer technology, it is possible to develop competency models of military specialists in the organization of communications for NGU units and algorithms that would provide decision support.

References

1. A.G. Chukhrai, S.I. Pedan. Ob odnom podkhode k razrabotke intsllectualnyh komp'uternyh sredstv obucheniya [Elektronnii resurs]. - www.nbuv.gov.ua/portal/natural/vcpi/NRvST/2011_9/89_94.pdf.

Єрошенко О. А., Прасол І. В., Новікова К. А.

ПРОГРАМНА РЕАЛІЗАЦІЯ СПОСОБУ ОЦІНКИ СТАНУ ЛЮДИНИ

Сьогодні проблема загрози здоров'ю розглядається світовою спільнотою як загроза планетарного масштабу. Тому необхідно стежити за фізичним станом людини, а особливо у наш час за фізичним станом курсантів та військовослужбовців.

Сфера медичних технологій є одною з найпередовіших галузей у нашому столітті. Такий швидкий розвиток технологій обумовлено тим, що нові технології спрощують життя у багатьох сферах життєдіяльності.

Сьогодні без винятку всі люди занурені в роботу, проблеми, вирішення повсякденних питань, і тому часу для моніторингу здоров'я зовсім не залишається. В такому випадку під рукою завжди є мобільний телефон як пристрій для підтримування корисних лікарських програм [1-3]. Тому пропонується мобільний застосунок, який реалізує контроль за станом людини.

Мобільний застосунок реалізує швидке і зручне рішення одного з найбільш витратних і довгих процесів в розробці, а саме кроссплатформенність. Цей застосунок написано на мові Dart, що в свою чергу є унікальною для свого часу мовою, яка дозволяє написати адаптивні застосунки під всі мобільні платформи. Зазвичай для адаптивних застосунків під ту чи іншу платформу використовувалася "власна мова": для Android – Kotlin, для iOS – Swift. Dart ж пропонує можливість написати код один раз, а його бібліотеки зроблять застосунок доступним для всіх мобільних платформ. Саме на такій технології написано цю програму для стеження здоров'я.

У застосунку достатньо одноразово ввести дані для подальших обчислень. З нього можна дізнатися такі параметри (рис. 1, а): необхідна кількість випитої води за день; ідеальний індекс маси тіла; необхідні кілокалорії на добу; "ідеальний" артеріальний тиск; співвідношення талія – стегна.

Для розрахунку цих даних додатком знадобляться такі параметри тіла людини (рис1, б): вага, зріст, стать, вік, обхват зап'ястя, обхват стегон, обхват талії.

Додаток «Health Balance» обробляє введені дані для розрахунку параметрів в єдиному комфортному інтерфейсі.

а) категорії розрахункових параметрів

б) форма для введення параметрів тіла

Рисунок 1 – Скріни застосунку

Список літератури

1. Никитин П.В. Мобильное здравоохранение: возможности, проблемы, перспективы / П.В. Никитин, А.А. Мурадянц, Н.А. Шостак // Клиницист. – 2015. – Т. 9. №4. – С. 13-21.

2. Yeroshenko O. OrganizationofaWireless System for Individual Biomedical Data Collection / O. Yeroshenko, I. Prasol, O. Trubitsyn, L. Rebezyuk // International Journal of Innovative Technology and Exploring Engineering. – 2020. – Vol. 9. No. 4. – Pp. 2418-2421. DOI: https://doi.org/10.35940/ijitee.D1870.029420

3. 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.

УДК 621.3, 621.32

Орлов М. М., Ткаченко К.М.

ПРО СПОСОБИ УПРАВЛІННЯ РУХОМИМИ ОБ'ЄКТАМИ В РАЙОНІ БОЙОВИХ ДІЙ НА ДОНБАСІ

Аналіз варіантів звільнення тимчасово окупованих окремих районів Донецької і Луганської областей підтвердив, що:

1) реалізація варіанта № 1 – мирним шляхом (шляхом домовленості України з Російською Федерацією), неможливо;

2) реалізація варіанту № 2 – воєнним шляхом, неможливо. Без детального опису зазначених варіантів № 1 і № 2, автори цієї праці пропонують розглянути варіант № 3 – поступовий вихід спеціально сформованих мобільних груп від України на українсько-російський кордон Луганської і Донецької області з метою ізоляції тимчасово окупованих районів і з подальшим «очищенням» зазначених районів від незаконних збройних формувань.

Для централізованого управління мобільними групами пропонується розглянути два варіанти управління (рис.1).

Перший спосіб управління мобільними групами пов'язаний з використанням ра-

діорелейних станцій. Позитивним такого способу є:

1) можна передавати (приймати) усі види інформації;

2) можна забезпечити прихованість змісту інформації, що циркулює в контурі управління.

Недоліками зазначеного способу є: значні ресурсні затрати щодо засобів зв'язку, бойової обслуги і особового складу охорони радіорелейних станцій.

Другий спосіб управління мобільними групами пов'язаний з використанням радіостанцій, безпілотного літального апарату (БПЛА), як автоматичного ретранслятора електричних сигналів. В межах зазначеного способу застосовується обмін інформації з використанням рознесеного маркерно-кодового зв'язку.

Рисунок 1 – Пояснення до варіантів управління рухомими групами на державному кордоні України

Позитивним такого способу є:

1) обмежені ресурсні затрати щодо наземних засобів зв'язку, бойової обслуги і особового складу охорони радіостанцій;

2) забезпечення відносної скритності обміну інформації.

Недоліками зазначеного способу є:

1) обмеженість щодо передавання (приймання) усіх видів інформації (телекодова інформація потребує значної швидкості оброблення електричних сигналів);

2) велика вірогідність збиття БПЛА військами противника;

3) обмежена дальність зв'язку в УКХ діапазоні.

Напрями подальшого дослідження:

1) структура і можливості БПЛА як автоматичного ретранслятора електричних сигналів;

2) вибір безпечного району баражування БПЛА;

3) визначення рівня компетенцій бойової обслуги і посадових осіб органів системи управління;

4) обґрунтування складу і завдань мобільних груп системи, поданої на рис.1.

УДК 621.396

Романюк В. А.

ЛАЗЕРНІ ТЕХНОЛОГІЇ В СУЧАСНИХ СИСТЕМАХ ОЗБРОЄННЯ: ПЕРЕВАГИ І НЕДОЛІКИ

Лазерні технології знаходять широке застосування у військовій сфері. При цьому в перспективі їх використання буде розширюватися за рахунок створення систем лазерного озброєння. Удосконалення технологій сприятиме масовому застосуванню лазерів як засобів ураження. Напрямки використання лазерів у військовій сфері, включаючи перспективні, можна розділити на чотири категорії:

1) супровід бойових дій,

2) наведення і використання як допоміжний елемент для засобів ураження,

3) придушення цілі,

4) безпосереднє ураження (руйнування) цілі.

У чому переваги бойових лазерів в порівнянні з традиційними системами озброєння?

Висока швидкість і точність ураження. Промінь рухається зі швидкістю світла і досягає цілі практично миттєво. Її знищення відбувається за лічені секунди, для перенесення вогню на іншу ціль необхідний мінімум часу. Випромінювання вражає саме ту область, на яку було направлено, не впливаючи на навколишні предмети.

Лазерний промінь здатний перехоплювати цілі, які маневрують, що вигідно відрізняє його від протиракет і зенітних ракет. Його швидкість така, що відхилитися від нього практично неможливо.

Лазер можна використовувати не тільки для знищення, а й для засліплення цілі, а також її виявлення.

Промінь лазера не має маси, тому при пострілі не потрібно вносити балістичні поправки, враховувати напрям і силу вітру.

Відсутня віддача.

Постріл з лазерної установки не супроводжується такими демаскирующими факторами, як дим, вогонь або сильний звук.

Боєкомплект лазера визначається тільки потужністю джерела енергії. Поки лазер підключений до нього, його «патрони» ніколи не закінчаться.

Відносно низька вартість одного пострілу.

Однак є у лазерів і серйозні недоліки, які і є причиною того, що поки вони не стоять на озброєнні жодної армії.

Розсіювання. Через рефракцію лазерний промінь розширюється в атмосфері і втрачає фокусування. На відстані в 250 км пляма лазерного променя має діаметр 0,3-0,5 м, що, відповідно, різко зменшує його температуру, роблячи лазер безпечним для цілі. Ще гірше впливають на промінь дим, дощ або туман. Саме з цієї причини створення далекобійних лазерів поки неможливо.

Неможливість вести загоризонтний обстріл. Промінь лазера – це ідеально пряма лінія, ним можна стріляти тільки по видимій цілі.

Випаровування металу цілі затінює її і робить лазер менш ефективним.

Високий рівень енергоспоживання. ККД лазерних систем малий, тому для створення зброї, здатної вразити ціль, потрібно дуже багато енергії. Цей недолік можна назвати ключовим. Тільки в останні роки з'явилася можливість створення лазерних установок більш-менш прийнятного розміру і потужності.

Від лазера легко захиститися. З лазерним променем досить просто впоратися за допомогою дзеркальної поверхні. Будь-яке дзеркало відображає його, незалежно від рівня потужності.

Kirichenko L., Kobziev V., Fedorenko Y.

DATA MINING METHODS FOR DETECTION OF COLLECTIVE ANOMALIES IN TIME SERIES

Data Mining [1] is a set of methods for identifying previously unknown, non-trivial, practically useful and accessible interpretations of knowledge needed for decision-making in various areas of human activity. One of the tasks of intellectual analysis is to detect anomalies - to identify rare and unusual elements, events or observations that cause suspicion, because they differ significantly from most data.

A time series is a time-ordered sequence of values of some process (for example, the value of a sensor). The need to detect unusual observations (emissions, or anomalies) in time series often arises in situations such as monitoring the condition of equipment, number of participants in certain events, accounting for patient health indicators, etc. [2]. There are three main types of anomalies in time series: point, contextual, and collective anomalies. In this paper, we will review collective anomalies, as they are the most common for time series. Collective anomalies occur when a sequence of related instances of data (e.g., a time series section) is anomalous with respect to an entire data set. A single instance of data in such a sequence may be random deviation, but the co-occurrence of such instances is a collective anomaly [3].

The basic idea of collective anomalies is that such grouped points cannot be anomalies alone. There are many methods for identifying such anomalies, including clustering methods, which allow you to select set of anomalous values as a separate cluster [4].

For a large number of observations, it would be rational to use the method of k-means. This method is one of the simplest and most popular clustering methods for separate a set of elements of a vector space into a predetermined number of clusters k for a certain number of iterations. The general concept of this method is: at each iteration recalculate the center of mass for each cluster obtained in the previous step, then the vectors are divided into clusters again according to which of the new centers was closer in selected metric. The algorithm ends when there is no change intra-cluster distance on any iterations. This occurs for a finite number of iterations, since the number of possible partitions of the finite set is finite, and at each step the total quadratic deviation decreases, so the loop is impossible.

The paper considers the approach to the detection of collective anomalies in time series, based on the use of clustering methods, in particular the method of k-means, as well as the effectiveness of their application.

References

1. Han, Jiawei. Data mining: concepts and techniques / Jiawei Han, Micheline Kamber, Jian Pei. – 3rd ed. - Morgan Kaufmann Publishers is an imprint of Elsevier. 2012. – 740p.

2. Mohammad Braei, Dr.-Ing. Sebastian Wagner. Anomaly detection in univariate time-series: a survey on the state -of-the-art, 2020: https://arxiv.org/pdf/2004.00433.pdf

3. Y. Jiang, C. Zeng, J. Xu and T. Li. Real time contextual collective anomaly detection over multiple data streams, 2014: https://api.semanticscholar.org/CorpusID:18868065

4. F. Anguilli and F. Fassetti. Detecting distance-based outliers in streams of data. CIKM '07: Proceedings of the sixteenth ACM conference on information and knowledge management. 2007. P. 811–820.

Оленченко В. Т., Майборода І. М.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ ОСВІТИ

Важливим елементом визначення якості освіти є процес оцінювання знань. З цією метою експерти – науково-педагогічні працівники – за певними ознаками виставляють бали, які, на думку експертів, відповідають рівню знань опитуваного здобувача освіти.

У переважній більшості країн склалися власні системи оцінювання знань і використовуються шкали, які отримали статус національних – чотирибальна (2, 3, 4, 5), семибальна (A, B, C, D, E, F, N), дванадцятибальна та інші шкали.

Світова глобалізація та необхідність отримати можливість переходу між вузами, навіть інших країни, призвела до появи європейської кредитно-трансферної системи – ECTS з її семибальною шкалою.

Також широкого застосування набула стобальна шкала, яка при своїй перевазі у розмірності має ряд недоліків, основним з яких є відсутність чітких критеріїв приписування балів.

Важливим моментом у забезпеченні єдиної міждержавної процедури виміру й порівняння між закладами освіти результатів навчання здобувачів освіти та забезпечення їх мобільності є технологія переходу (рис. 1) між різними шкалами оцінювання.

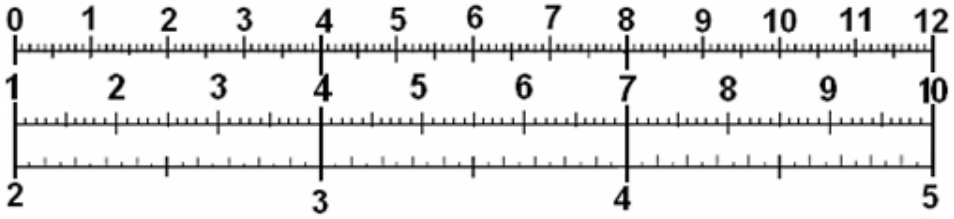


Рисунок 1 – Номограма зв’язку оцінок за удосконаленою чотирибальною, десятибальною та дванадцятибальною шкалами

Проте це важливо лише на фінальній стадії вивчення певної дисципліни. В інших випадках доцільно використовувати національну чотирибальну шкалу.

УДК 621.384.6

Фик О. І., Флорін О. П.

ПОБУДОВА ФРАКТАЛІЗОВАНОГО ЗАХИСТУ РАДІОЕЛЕКТРОНОЇ АПАРАТУРИ ВІД УРАЖЕННЯ ПОТУЖНИМИ ЕЛЕКТРОМАГНИТНИМИ ЗАВАДАМИ

Фрактальний сигнал має високу ступінь захищенності інформації завдяки великій надлишковості, яка визначається ієрархічною, “самовкладенною” спектральною структурою. І тому, для вирішення проблеми побудови системи захисту РЕА від збоїв або електромагнітного ураження необхідно визначитись або з фракталізованою геометричною структурою елементів фазованної решітки , або з параметрами корисного фракталізованного широкосмугового сигналу, який буде збуджувати ці елементи та формувати випромінювання з самоподібною спектральною структурою. Можливо також використовувати одночасно фракталізацію, як елементів рещітки та і форми токів, які їх збуджують. Існують два рішення побудови такого пристрою:

1. Режим співпадіння частоти робочого сигналу та частоти, на якій зосереджена основна потужність завади;

2. Режим, коли частота робочого сигналу перевищує частоту, на якій зосереджена основна потужність завади.

Розглянуто спосіб побудови захисту радіотехнічних систем від потужних імпульсних завад на основі фазованної фрактальной антенної решітки, яка може працювати у режимах 1 або 2. Фрактальна антена, що випромінює, являє собою фрактальную фазовану решітку, яка відрізняється від традиційної меншою кількістю елементів та законом їх розподілу на поверхні решітки, а також конфігурацією елементарного випромінювача. Фрактальність спектру елементарних випромінювачем антенної решітки дозволяє використовувати систему прийомно-передавальних антен у якості захисних пристроїв не тільки від електромагнітного ураження, а і від інформаційних сбоїв елементів РЕА приймача радіоелектронних засобів.

Запропонована фрактальна захисна система від потужних завад має наступні переваги:

- малий час спрацьовування;
- висока електрична стійкість;
- захищеність від зовнішніх впливів (бо треба впливати потужними фракталізованними за спеціальним законом сигналами).

Отже, запропонований принцип побудови фрактальної антени може бути використаний для захисту високочутливих радіотехнічних систем від ураження потужними імпульсними сигналами складної структури.

УДК 621.396.6

Кучер Д. Б., Фик О. І.

ОЦІНКА РЕЗУЛЬТАТІВ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ НАДПРОВІДНОГО ЗАХИСТУ РАДІОЕЛЕКТРОНОЇ АПАРАТУРИ ВІД УРАЖЕННЯ ПОТУЖНИМИ ЕЛЕКТРОМАГНИТНИМИ ЗАВАДАМИ

В даний час для опубліковано досить багато робіт, які доказують, що для обмеження критично великих за значенням амплітуд струмів (до десятків ампер) і напруг (більше тисячі вольт), що виникають під дією потужних електромагнітних випромінювань (ПЕМВ) в лініях зв'язку радіоелектронної апаратури (РЕА) можна використовувати надпровідні захисні пристрої.

Час спрацювання надпровідного захисного пристрою визначається тривалістю фазового S-N переходу. Згідно з результатами досліджень фазовий стан надпровідного захисного пристрою можна визначити як:

$$\begin{cases} K_S = N_S h^2 l^2 (W - 2\lambda_l)^2, & 0 \le t < t_{c1}; \\ K_S(t) = N_S l^2 \left(Wh - 4\lambda_l^2 \dfrac{i(t)}{I_{c1}} \right)^2, & t_{c1} \le t < t_{c2}; \\ K_S = 0, & t_{c1} \le t < t_{Ц}. \end{cases} \quad (1)$$

де K_S - показник, що характеризує надпровідний фазовий стан тонкої плівки; N_S - коефіцієнт, що характеризує щільність надпровідних носіїв заряду n_S в масивному високотемпературному надпровіднику об'ємом в 1 $м^{3;}$ W, h, l – ширина, товщина і довжина надпровідної плівки.

Тоді значення струму, що протікає в колі, можна визначити як:

$$\begin{cases} i(t) = \dfrac{u_1(t)}{R_к + R_н} & 0 \le t < t_{c1}; \\ i(t) = \dfrac{-(R_к + R_н) + \sqrt{(R_к + R_н)^2 + 4Au_1(t)}}{2A} & t_{c1} \le t < t_{c2}; \\ i(t) = \dfrac{u_1(t)}{R_к + R_н + R_N} & t_{c1} \le t < t_{c2}, \end{cases} \quad (2)$$

де $R_н$, $R_к$, R_N опір навантаження (50 Ом), опір контактів і опір захисного пристрою в нормальному стані відповідно; $A = \dfrac{\rho_n l}{S I_{c2}}$. Напругу на захисному пристрої в момент фазового S-N переходу, враховуючи (1), можна записати як:

$$u_{зу}(t) = \frac{\left(-\left(R_н + R_к\right) + \sqrt{(R_н + R_к)^2 + 4Au_1(t)}\right)^2}{4A} \quad (3)$$

Тривалість фазового S-N переходу, враховуючи, що опір захисного пристрою в змішаному стані набагато більше Rн і Rк, можна визначити на підставі виразу

$$t_{S-N} = \frac{I_{c2}^2 A - I_{c1} R_н}{U_m\left(a_2 - a_1\right)} \quad (4)$$

Таким чином, щоб перевірити вірогідність отриманих співвідношень треба провести експериментальні дослідження напруги на виході захисного пристрою до впливу потужного електромагнітного імпульсу на вході пристрою і після електромагнітного удару.

Макетний зразок, побудований на основі мікрополоскової лінії передачі, виготовлявся з двох ВТНП плівок $YBa_2Cu_3O_7$, що напилені на різні підкладки. Поверх ВТНП плівки напилено на підкладку з TiSrO3, далі підкладка з $LaAlO_3$ з ВТНП плівкою, на якій вжигалися контакти (рис.1 світлим кольором). Приклеювання здійснювалася по боковій поверхні верхньої підкладки так, щоб клей не затікав на робочу поверхню нижньої ВТНП плівки. Нижня ВТНП плівка використовувалася в якості екрану, верхня ВТНП плівка є мікрополосковою лінією (рис. 1).

Для дослідження фазового S-N переходу була використана схема, показана на рис. 2. Імпульси тривалістю 100 нс і амплітудою в 0,05, 50 і 100 В із затримкою в 5 мкс подавалися на дільник напруги, утворений досліджуваним макетним зразком і опором навантаженням. Затримка вхідного сигналу імітувала одиночний вплив ПЕМІ. Напруга на навантаженні реєструвалася за допомогою осцилографа С8-14.

Осцилограми переходного процесу макетного зразка надпровідного захисного пристрою подані на рис.3. Розрахункові часові залежності напруги на навантаженні подані на рис. 4. Для наочності перехідного процесу вихідний сигнал на осцилограмах має зсув по горизонталі відносно вхідного на одну поділку.

Порівнюючи осцилограми з розрахунковими залежностями (рис. 4), слід зазначити досить хорошу збіжність результатів (розбіжність по часовим залежностям не перевищує 2%), що дозволяє сформулювати основні положення, які отримали експериментальне підтвердження:

1. Початок фазового S-N переходу супроводжується практично миттєвою зміною активного опору тонкої ВТНП плівки, що підтверджує правильність вибору швидкого токового механізму руйнування надпровідності;

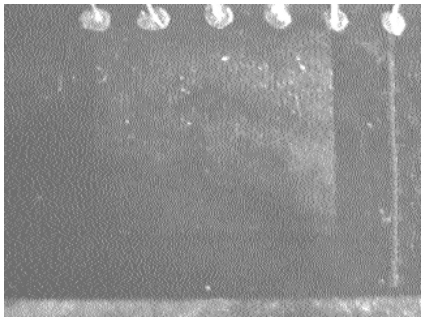


Рисунок 1 - Фотографія макетного зразка надпровідного мікрополосково захисного пристрою

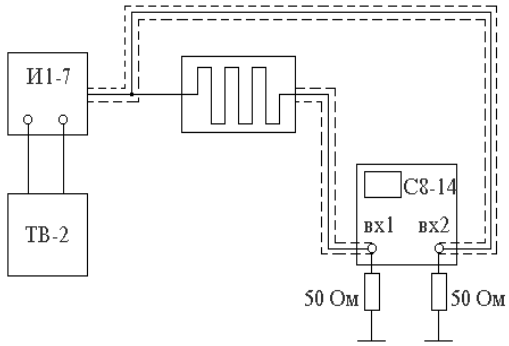


Рисунок 2 - Схема вимірювання тривалості фазового переходу надпровідного захисного пристрою

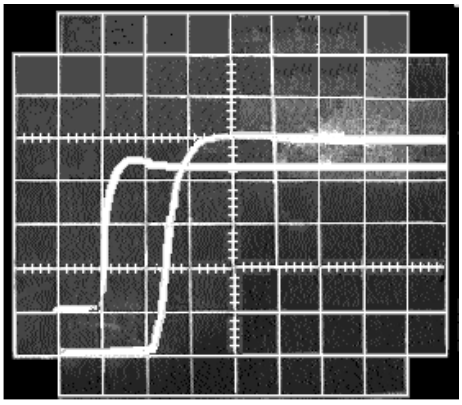


Рисунок 3 - Осцилограми фазового S-N переходу захисного пристрою, виконаного на основі МПЛ (меандр), зняті на навантаженні. Вхідний імпульс на нижньому промені, вихідний на верхньому. Вертикальні масштаби: для верхнього променя 10 В/поділ, для нижнього променя 0,05 В/поділ. Розгортка 5 нс/поділ

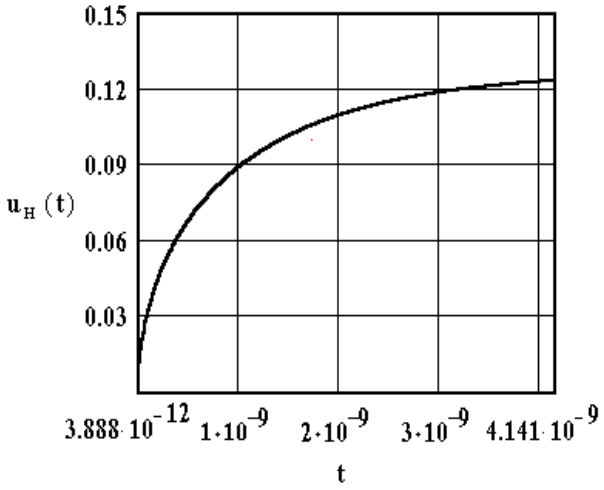


Рисунок 4 - Розрахункові часові залежності напруги на навантаженні в момент фазового S-N переходу захисного пристрою, який побудований на основі МПЛ (меандр)

2. Тривалість фазового S-N переходу не визначається конкретною величиною, а залежить від амплітуди вхідного сигналу і конструктівних параметрів надпровідника.

3. Закінчення фазового S-N переходу залежить від амплітуди вхідного сигналу і довжини тонкої ВТНП плівки при однаковій площі перетину.

4. Наведена конструкція мікрополоскової лінії може використовуватися в лініях зв'язку радіоелектронної апаратури для побудови від вигорання її чутливих елементів зі швикістю переключення (спрацьовування захисту) менше 1 наносекунди.

УДК 621.39

Сальніков О. М., Горбатюк П. М.

БЕЗПЕКА СУЧАСНИХ КОМП'ЮТЕРНИХ СИСТЕМ НА БАЗІ LINUX-LIKE РІШЕНЬ

В сучасних умовах, коли різко активізувалася як кіберзлочинність, так і відповідні служби зовнішніх розвідок ряду країн, представляється необхідним звернути увагу на безпеку комп'ютерних систем не тільки приватних осіб, але і державних установ. Видається актуальним розглянути в комплексі мережеві рішення, побудовані на базі операційної системи на ядрі Linux.

Структура даного сімейства операційних систем спочатку будувалася на постулаті безпеки встановленого програмного забезпечення з одного боку (включаючи захист від несанкціонованого доступу до ядра операційної системи) і захисту даних (включаючи поділ використання даних різними користувачами. на одному комп'ютері) з іншого боку.

Важливим моментом роботи даного сімейства операційних систем є той факт, що право на установку і видалення програмного забезпечення має виключно користувач з правами ROOT (привілейований користувач). Решта користувачів як локального комп'ютера, так і мережі, таких прав позбавлені. Таким чином, несанкціоноване видалення (як і установка) програмного забезпечення, а також його модифікація простим користувачем, що не володіє привілейованими правами, неможлива. Так само як і установка несанкціонованого програмного забезпечення.

Структура ядра Linux спроектована з урахуванням можливості спроб проникнення в операційну систему з метою отримання доступу до призначених для користувача даних і модифікації програмного забезпечення. Жорсткий поділ прав користувачів не дозволяє обійти заборону на читання «чужої» інформації. Необхідність введення пароля користувача root для запуску стороннього програмного забезпечення (а також для його установки) не дає можливості функціонувати в середовищі Linux вірусів, троянських коней і хробаків. Єдиний випадок успішного запуску хробака (так званий хробак Морріса) був відзначений в середовищі UNIX в 1988 році. З тих пір були враховані помилки в ядрі і на даний момент часу застосування цієї шкідливої технології не зафіксовано, чого не можна сказати про Windows. Що ж стосується спроб проникнення ззовні, то в ядро Linux вбудований фаєрвол, що перешкоджає таким спробам. Якщо такого роду захисник в середовищі Windows працює за принципом «що не заборонено, то дозволено» і таким чином не в змозі протистояти загрозам, про які не знає системний адміністратор, то в середовищі Linux дане програмне забезпечення працює за принципом «що не дозволено, то заборонено». Тому за замовчуванням відсутній навіть дозвіл на віддалений доступ до робочого столу і до разшарених файлів та каталогів.

З вищевикладеного логічно випливає той факт, що захист робочої станції знаходиться на належному рівні. З серверними рішеннями точнісінько так само. Причиною цього є той факт, що як сервер, так і робоча станція базуються на одному і тому ж ядрі. Що дозволяє з одного боку використовувати адміністратору мережі однаковий інструментарій на всіх комп'ютерах мережі (як робочих станціях, так і серверах), а з іншого боку мати потужні інструменти моніторингу всієї мережі, не вимагаючи для цього додаткових обчислювальних потужностей.

Отже вважається доцільним розглянути шляхи впровадження Linux-подібних операційних систем в інформаційно-телекомунікаційній системі Національної гвардії України.

Козлов В. Є., Лазарев В. Д.

АНТЕННИЙ ПРИСТРІЙ ЯК ЕЛЕМЕНТ ЗАХИЩЕНОЇ ЛОКАЛЬНОЇ СИСТЕМИ РАДІОЗВ'ЯЗКУ

Для побудови локальних систем радіозв'язку, призначених для обміну конфіденціальною інформацією в діапазоні UHF в умовах штучних радіозавад і спроб несанкціонованого доступу до інформації, що передається, доцільно використовувати засоби радіозв'язку, антенна система яких може забезпечити фізичну скритність і візуальну скритність.

Антени зі штирьовим вібратором не можуть забезпечити скритність застосування через доступність прийому сигналу з будь-якого напрямку. Антени із кутковим дзеркалом (рефлектором) мають специфічний демаскуючий зовнішній вигляд. Антени, дзеркало яких має форму параболічного циліндра, мають той же недолік.

На рис. 1 наведено зовнішній вигляд бочки об'ємом 200 дм^3. Висота бочки біля 850 мм, радіус приблизно 280 мм [1]. Розміри відповідають необхідним для побудови відбивачів антен частотного діапазону UHF ($f_{сер}$ = 435 МГц). Якщо в бочці прорізати щілину вздовж твірної циліндра, а в середині бочки вздовж її фокальної осі розмістити лінійний опромінювач у вигляді одного або декількох оснащених контррефлекторами симетричних електричних або щілинних вібраторів, отримаємо антенну систему, демаскуючі ознаки в якій відсутні.

Рисунок 1 – Зовнішній вигляд бочки

Відмітимо, що якості спрямованості параболічного циліндра, циліндра і антени з кутковим дзеркалом таких же розмірів приблизно однакові, їх розрахунок виконується за одними й тими ж формулами [2, с. 279] або відповідно до методики, викладеної в додатку 2 [2, с. 464-466].

Діаграма спрямованості антенного пристрою, що використовує в якості дзеркала сталеву бочку зі щілиною шириною (0,3-0,7)λ, з опромінювачем – штирьовою антеною радіостанції «Kenwood», – отримана в результаті натурного експерименту, незначно відрізняється від розрахованої для однакових вихідних даних.

Очевидно, що запропоноване технічне рішення може забезпечити фізичну скритність завдяки вузькій ДН, а також візуальну скритність, обумовлену відсутністю демаскуючих ознак, і може бути використано як елемент захищеної локальної системи радіозв'язку.

Список літератури

1. ГОСТ 13950-91. Бочки стальные сварные и закатные с гофрами на корпусе. Технические условия. [Электронный ресурс]. – Режим доступа: http://www.vashdom.ru/gost/13950-91.

2. Кочержевский Г.И. Антенно-фидерные устройства/ Г.И. Кочержевский. – М.: Связь, 1972. – 472 с.

Козлов В. Є., Козлов Ю. В., Новикова О. О., Оленченко В. Т.

ВСТАНОВЛЕННЯ ВІДПОВІДНОСТІ ОЦІНОК, ОТРИМАНИХ ЗА ШКАЛАМИ ПОРЯДКУ

Система оцінювання вивченості (знань, умінь та навичок) суб'єктів навчання (СН) різних рівнів і процедури урахування балів при складанні різноманітних рейтингів у освітянській діяльності передбачають використання різних шкал порядку. Подання результатів із залишенням декількох знаків після коми відповідає відомому з метрології методу ноніуса [1], що дозволяє збільшити число градацій у межах однієї поділки основної шкали, не збільшуючи її довжини. Кожна з поділок будь-якої зі шкал може бути поділена на п'ять, десять або кратну їм кількість поділок, що забезпечує більш якісне розрізнення СН.

Використання ноніуса 1/100 в чотирибальній шкалі (ЧШ) порядку, що широко застосовується у педагогічній кваліметрії, дозволяє отримати так звану удосконалену чотирибальну шкалу (УЧШ). Це робить застосування десяти- і дванадцятибальної шкал для оцінювання рівня вивченості суб'єктів навчання недоцільним [2].

Імовірнісно-інформаційний підхід [3] дозволив отримати вираз для визначення оцінки будь-якої L-бальної логарифмічної шкали з основою два. Формула для розрахунку оцінок за логарифмічною чотирибальною шкалою (ЛЧШ) має вигляд

$$Q_{ЛЧШ} = 2 + \log_2[-8/(7q - 8)], \quad (1)$$

де q = 0…1 – частка повернутої об'єктом контролю інформації.

Апроксимація ЛЧШ трьома прямими в інтервалах оцінок 2,00 – 3,00; 3,00 – 4,00; 4,00 – 5,00, які відповідають значенням q в діапазонах 0 – 0,57; 0,57 – 0,86; 0,86 – 1, не змінює "логарифмічну сутність" шкали, але дозволяє спростити розбиття інтервалів на частки однакової довжини при абсолютних похибках, що, не перевищують 0,72. При цьому, значення величин, що відкладають на апроксимованій шкалі, відрізняються від відповідних значень логарифмічної шкали, але їх відносне положення не змінюється.

На рис. 1 наведено номограму з нанесеними шкалами: УЧШ, стобальна та відповідна їй шкала ESTC і апроксимована ЛЧШ. Стобальну шкалу можна використовувати для подання числових результатів вивченості як деякий коефіцієнт відповідності в діапазоні нормованих значень від нуля до одиниці.

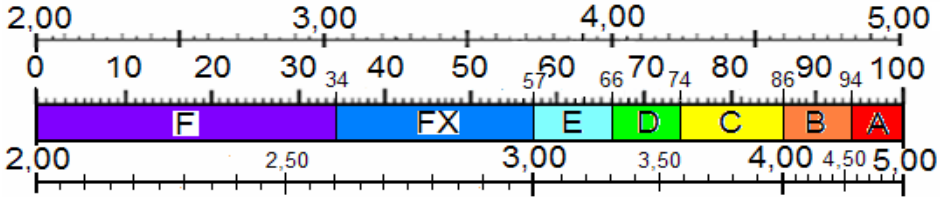


Рисунок 1 – Графічна номограма

Як показує приклад (див. рис. 1), оцінці 3,50 за УЧШ відповідає оцінка 50 за стобальною шкалою, FX за шкалою ESTC і 2,83 за апроксимованою ЛЧШ.

Таким чином, запропонована графічна номограма може забезпечити встановлення відповідності оцінок, отриманих за чотирьохбальними шкалами, стобальною шкалою та шкалою ESTC, і придатна до застосування в освітянський діяльності як інструмент, що заміщає відповідні обчислення.

Список літератури

1. Шишкин, И.Ф. Метрология, стандартизация и управление качеством / И.Ф. Шишкин; под ред. акад. Н.С. Соломенко. – Москва: Изд-во стандартов, 1990. – 342 с.

2. Козлов, В. Метод оцінювання рівня вивченості суб'єкта навчання / В. Козлов,

Ю. Козлов, В. Кобзєв, І. Мощенко // Інформаційні системи та технології ІСТ-2020: матеріали 9-ї Міжнародної науково-технічної конференції 17-20 листопада 2020 р., Харків, Україна. – Харків: ХНУРЕ, 2020. – С. 160-162.

3. Козлов, В.Є. Модель подання оцінних функцій викладача / В.Є. Козлов, В.Т. Оленченко, І.О. Юзьков// Системи обробки інформації. – Харків: ХУ ПС, 2009. – Вип. 6(80). – С. 233–236.

Каплун Є. О., Чуйков Д. В.

ЗАСТОСУВАННЯ РАДІОТЕХНІЧНИХ СИСТЕМ ДЛЯ БЛОКУВАННЯ (УРАЖЕННЯ) ЗАСОБІВ РАДІОЗВ'ЯЗКУ ПРИ ПРОВЕДЕННІ АНТИТЕРОРИСТИЧНИХ СПЕЦОПЕРАЦІЙ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Результати аналізу досвіду застосування засобів радіозв'язку на Сході України при проведенні Операції об'єднаних сил (Антитерористичної операції) доводять, що серед основних завдань боротьби з незаконними збройними формуваннями (НЗФ) є створення ефективного комплексу радіорозвідки (радіомоніторингу). Метою функціонування такого комплексу є своєчасне блокування засобів радіозв'язку противника. Комплекс радіомоніторингу за роботою засобів радіозв'язку НЗФ дозволить викривати систему управління терористів і надавати потрібну інформацію для функціонування власних (які належать до складу підрозділів Національної гвардії України) засобів радіоелектронної боротьби і дезінформації. Крім того, останнім часом при проведенні Операції об'єднаних сил на сході України збільшилась частка застосування НЗФ радіокерованих вибухових пристроїв (наприклад, фугасів, мін тощо). Отже, це підтверджує актуальність дослідження щодо створення елементів комплексу радіорозвідки (радіомоніторингу) для блокування засобів радіозв'язку противника.

Радіотехнічні системи, які входять до сучасних комплексів радіомоніторингу, повинні виконувати наступні функції:

– пошук і пеленгування джерел радіовипромінювань (засобів радіозв'язку);

– вимірювання параметрів сигналів (центральної частоти, зайнятої смуги частот, девіації частоти тощо) та визначення режимів роботи засобів радіозв'язку;

– розпізнавання джерел радіовипромінювання та складання описів непізнаних (незареєстрованих) джерел;

– пеленгування місця розташування джерела радіовипромінювання;

– розпізнавання джерел радіозв'язку, здійснене за результатами вимірювання параметрів сигналів шляхом порівняння з еталонами, що зберігаються у банку даних;

– настроювання апаратури контролю на радіовипромінювання за пеленгом і частотою;

– первинна обробка результатів вимірювання;

– радіоблокування (радіо придушення), у разі необхідності, засобів радіозв'язку, інших радіозасобів (наприклад, засобів радіокерування вибуховими пристроями);

– розрахунок за результатами вимірювань відношення сигнал/завада у пункті приймання радіосигналу потужності постановників радіозавад.

Результати аналізу використання можливих засобів радіозв'язку НЗФ, амплітудно-частотно-часових характеристик радіотехнічних сигналів указують на те, що радіомоніторинг необхідно здійснювати у визначеному частотному діапазоні з різноманітною тривалістю сигналу сканування (посилки) [1-3].

Для блокування (ураження) засобів зв'язку НЗФ з метою порушення системи управляння при організації та здійсненні заходів антитерористичної спецоперації у доповіді запропоновано застосування надширокосмугових радіотехнічних сигналів і відповідних

антенних пристроїв. Основним елементом таких антенних пристроїв є тракт формування та випромінювання надширокосмугових сигналів. Питання щодо використання надширокосмугових сигналів теоретично достатньо добре відпрацьовані. Тому запропонований підхід щодо застосування надширокосмугових сигналів в антенному тракті може бути покладено в основу при розробці та створенні конкурентно здатних засобів функціонального блокування (ураження) засобів радіозв'язку НЗФ.

В доповіді показано, що під функціональним блокуванням засобів радіозв'язку розуміється такий вплив на засоби та канали радіозв'язку НЗФ, при якому здійснення зв'язку не можливе. Змістом функціонального ураження є потрібний вплив сформованим електромагнітним імпульсом, який гарантовано виводить з ладу окремі елементи або пристрої засобів радіозв'язку НЗФ. При цьому виключається самостійне відновлення функціонування радіоелектронних систем засобів радіозв'язку НЗФ (наприклад, після закінчення впливу електромагнітного імпульсу), а відновлення справності можливо тільки після проведення ремонтно-відновлювальних заходів спеціальними підрозділами.

Енергетичний потенціал постановника завад або функціонального блокування (ураження) засобів радіозв'язку НЗФ залежить від потужності завади та коефіцієнта підсилення антени. Коефіцієнт підсилення антени визначається шириною її діаграми спрямованості. Використання лінійно поляризованих антен у широкому куті призводить до зниження енергетичного потенціалу засобів блокування (ураження). Тому доцільним є використання засобів функціонального блокування (ураження) каналів радіозв'язку з направленими антенами у вузькому куті (секторальних антен). Можливість секторного огляду такої антени за азимутом передбачає зменшення потужності, яка випромінюється, в напрямах, відмінних від напряму головного максимуму діаграми спрямованості. Це значно впливає на рішення задачі електромагнітної сумісності при використанні надширокосмугових сигналів засобу функціонального блокування або знищення (ураження) із засобами зв'язку підрозділів Національної гвардії України і засобами захисту особового складу від електромагнітного випромінювання.

В доповіді наведено результати розрахунків тактико-технічних характеристик елементів антенного тракту та параметрів випромінювача надширокосмугової антени засобу функціонального блокування (ураження). Запропонована антена представляє собою конічну спіраль. Розроблений випромінювач забезпечує випромінювання електромагнітного поля шириною, що дозволяє внести заваду у роботу засобів радіозв'язку на території приблизно одного квадратного кілометру.

Представлена у доповіді розроблена методика розрахунку потужності ненавмисної завади на вході основного каналу прийому засобу радіозв'язку НЗФ. Методика дозволяє розраховувати показники електромагнітної сумісності для ослаблення впливу розробленої антени на радіоелектронні та радіотехнічні засоби підрозділів Національної гвардії України. Для цього запропоновано використовувати комбінації різного роду організаційних способів забезпечення електромагнітної сумісності радіоелектронних засобів: частотного, просторового або часового.

Обґрунтовано підхід до здійснення радіоелектронної протидії радіокерованим вибуховим пристроям, які як правило використовують НЗФ (терористи) при проведенні терористичних акцій, який полягає у впливі на них потужним електромагнітним імпульсом. При цьому найбільш уразливими при впливі потужного електромагнітного імпульсу є радіоелектронні елементи вхідних трактів приймальних каналів вибухових пристроїв, побудованих на основі напівпровідників (діодів, транзисторів і мікросхем), функціональне ураження яких викликає відмову в роботі засобів радіокерування вибуховими пристроями.

Обґрунтовано основну перевагу використання надширокосмугових засобів для функціонального блокування (ураження) засобів радіозв'язку НЗФ (терористів). Вона обумовлена тим, що не потребує точного знання характеристик радіотехнічного

або радіоелектронного засобу, що уражається.

Список літератури

1. Лаврут О.О. Новітні технології та засоби зв'язку у Збройних Силах України: шлях трансформації та перспективи розвитку О.О. Лаврут, О.К. Климович, Т.В. Лаврут, Ю.М. Здоренко // Наука і техніка Повітряних Сил Збройних Сил України. – Х., 2019. – Вип. 1 (34). 91-101. – DOI: 10.30748/nips.2019.34.13

2. Лаврут О.О. Стан та перспективи застосування сучасних технологій та засобів радіозв'язку в Збройних Силах України / О.О. Лаврут, О.К. Климович, М.Л. Тарасюк, О.Л. Антонюк // Системи озброєння та військова техніка. – Х. : ХНУПС, 2017.– Вип. 1 (49). – С. 42–49.

3. O. Klymovych, V. Hrabchak, O. Lavrut, T. Lavrut, V. Lytvyn and V. Vysotska. The Diagnostics Methods for Modern Communication Tools in the Armed Forces of Ukraine Based on Neural Network Approach. Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT+DS 2020). Volume I: Main Conference Lviv-Shatsk, Ukraine, June 2-3, 2020.- P. 198-208.- URL: http://ceur-ws.org/Vol-2631/paper15.pdf

УДК 343.985

Семенко Є. Ю., Яковлев М. Ю., Стрижак О. Є.

МЕТОД РАНЖУВАННЯ ВАРІАНТІВ СТРУКТУРИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ НА ЕТАПІ ЇЇ СТВОРЕННЯ

Необхідність в ранжуванні альтернатив виникає в багатьох сферах людської діяльності, пов'язаних з розв'язанням прикладних задач, що сприяють ефективному прийняттю обґрунтованих науково-технічних та управлінських рішень. Складність і різноманіття ситуацій вибору вимагає врахування великої кількості різних факторів і критеріїв.

У доповіді запропоновано метод ранжування варіантів структури інформаційно-аналітичної системи (ІАС) Національної гвардії України (НГУ) на етапі її створення. Розглянуто його сутність, основні етапи, відмінність від відомих, основні переваги та недоліки. Показано, що він заснований на онтологічному представленні задачі ранжування варіантів структури ІАС НГУ. Кожна онтологія містить інформаційні описи, на основі об'єктно-орієнтованої процедури формалізації, а також описи інтерпретаційних функцій, які є функціональним проявом властивостей об'єктів (концептів), що складають онтологію, та які управляють на основі цього процесом поставки інформаційного ресурсу на усіх етапах прийняття рішень. Тому цілком виправданим є представлення інформаційної моделі у вигляді певної онтології. Як відомо, в основі онтологічної методології лежить об'єктно-орієнтований підхід, при якому предметна прикладна область представляється у вигляді сукупності об'єктів, взаємодія між якими може бути представлена за допомогою семантичного зв'язування висловлювань, тверджень та суджень.

Під час формування методу ранжування на основі онтології виникає необхідність у визначенні певного перетворення. Задача ранжування описується набором альтернатив (варіантів структури ІАС НГУ) A, для кожної з яких задаються значення певних показників (критеріїв). Розв'язком такої задачі є встановлення лінійного порядку над множиною альтернатив, а цей порядок дозволяє визначити альтернативи, що мають найкращі (за сукупністю) значення критеріїв (та які в загальному випадку відрізняються різною важливістю). Формально математичну модель задачі ранжуван-

ня представлено: множиною альтернатив; множиною критеріїв; функцією, що визначає значення альтернатив за певним критерієм; правилом ранжування, яке дозволяє встановити лінійний порядок для множини альтернатив.

Показано, що ІАС НГУ є системою, призначеною для підтримки процесів виконання службово-бойових завдань НГУ. Основними її завданнями є зчитування вхідної інформації (можливо, слабо-структурованої) і реалізація на її основі інформаційних та інформаційно-розрахункових задач. Наведено загальну структуру ІАС НГУ та розглянуто основні її варіанти для ранжування з урахуванням завдань, які вона має виконувати й інших умов і обмежень.

УДК 343.985

Яковлев М. Ю., Стрижак О. Є., Ходич О. В., Майборода І. М.

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ З ПІДТРИМКИ ПРОЦЕСІВ ВИКОНАННЯ СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ НАЦІОНАЛЬНОЮ ГВАРДІЄЮ УКРАЇНИ

Основу аналітичної діяльності експертів у сфері охорони громадського порядку, забезпечення громадської безпеки, становлять інформаційні ресурси, наративи яких характеризують властивості й функціональність процесів виконання службово-бойових завдань (СБЗ) Національною гвардією України (НГУ).

Однак без наявності відповідних аналітичних сервісів, ці ресурси є пасивною компонентою інформаційного простору Міністерства внутрішніх справ України. Для їх оброблення треба мати відповідне програмно-інформаційне забезпечення, спроможне реалізовувати інтелектуальні когнітивні сервіси інтегрованого аналітичного оброблення усього наративу описів процесу виконання СБЗ НГУ. Ці сервіси мають обов’язково забезпечувати процеси семантичного контент-аналізу та структурного відображення результатів цього аналізу усіх системних складових, а саме: їх властивості, функціональні характеристики та міжсистемні зв`язки, включаючи посилання на технологічні процеси виробництва з урахуванням національних, та міжнародних стандартів тощо.

У доповіді на основі проведеного аналізу стану розвитку інформаційних систем встановлено дві основні проблеми, які потребують вирішення щодо ефективного створення та впровадження інформаційно-аналітичної системи для підтримки процесів виконання СБЗ НГУ.

Проведено аналіз процесів автоматизації виконання СБЗ НГУ та визначено, що за кожним з напрямів створені окремі компоненти інформаційних систем, проте вони є різнорідними за часом створення, ступенем завершеності, використаними технологіями, обсягом охоплення процесів, обсягом розгортання та наповнення даними, а також можливістю інтеграції до єдиної системи з урахуванням принципів та стандартів НАТО. Стан інформаційно-аналітичної інфраструктури, яка спрямовується для забезпечення потреб керівного складу структурних підрозділів НГУ не відповідає сучасним викликам у галузі виконання СБЗ. Інтеграція інформаційних систем за окремими напрямами відсутня або здійснюється фрагментарно, а це призводить до дублювання та недостатньої достовірності і повноти інформації щодо комплексного управління в сфері охорони громадського порядку та забезпечення громадської безпеки в цілому.

Наведено перелік основних питань щодо створення сучасного інформаційно-аналітичного забезпечення НГУ, які залишаються не вирішеними.

Визначено основні завдання інформаційно-аналітичного забезпечення процесів виконання СБЗ НГУ та основні етапи їх реалізації.

Запропоновано основні завдання інформаційно-аналітичної системи підтримки процесів виконання СБЗ НГУ.

Таким чином, в доповіді розглянуто сучасний стан, перспективи та напрями розвитку інформаційно-аналітичної діяльності з підтримки процесів виконання СБД НГУ.

ЗМІСТ

АБЕТКОВИЙ ПОКАЖЧИК АВТОРІВ ПУБЛІКАЦІЙ

Овсянніков В. В.	- кандидат технічних наук, провідний науковий співробітник	***64,66***
Паламарчук Н. А. (Palamarchuk N.)	- начальник науково-дослідної лабораторії	***62,65,66***
Паламарчук С. А.	- заступник начальника науково-дослідного відділу	***64,65,66***
Побережець Т. В.	- науковий співробітник	***66***
Сергієнко А. В.	- провідний науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації	***21***
Сівоха О. М.	- молодший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації	***37***
Терещенко Т. П.	- старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації	***40***
Ткач В. О.	- старший науковий співробітник	***65***
Черниш Ю. О.	- старший науковий співробітник	***64,65***
Штонда Р. М.	- начальник науково-дослідного відділу Наукового центру зв'язку та інформатизації	***40***
Bondarenko T.	- науковий співробітник	***62***
Tsymbal I.	- старший науковий співробітник	***62***

Головне управління Національної гвардії України, м. Київ

Kolomoyets M.	- старший офіцер служби підготовки з ППО відділу ППО УБЗ Головного управління Національної гвардії України	***14***

Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, м.Чернігів

Kukobko S.	- кандидат технічних наук, старший науковий співробітник, начальник науково-дослідного відділу	***34***

Державний університет інфраструктури та технологій, м. Киів

Яновська В. П.	- доктор економічних наук, професор, завідувач кафедри	***83***

Дніпропетровський державний університет внутрішніх справ

Завістовський О. Д.	- старший викладач, віце-президент Федерації поліцейського хортингу України	***79***

Київський національний університет будівництва і архітектури

Хлапонін Ю. І.	- доктор технічних наук, професор, завідувач кафедри	***86***

Київський фаховий коледж транспортної інфраструктури

Яновська Т. Г.	- викладач	***83***

Комунальний заклад «Харківська гуманітарно-педагогічна академія» Харківської обласної ради

Русскін В. М.	- кандидат технічних наук, доцент, завідувач кафедри	***60***

Міжнародна федерація поліцейського хортингу, м. Київ

Шаповалов Б. Б.	- кандидат психологічних наук, доцент, президент федерації	***79***

Національна академія Національної гвардії України, м. Харків

Алфімова Л. Д.	- кандидат хімічних наук, доцент, завідувач кафедри	***24***
Баулін Д. С.	- кандидат технічних наук, доцент, старший науковий співробітник науково-дослідної лабораторії Науково-дослідного центру	***18***
Власов К. В.	- старший викладач кафедри	***17***
Волков П. Ю.	- ад'юнкт	***18***
Воронін О. І.	- старший викладач кафедри	***30***
Гончар Р. О.	- кандидат військових наук, старший дослідник, старший науковий співробітник Науково-дослідного центру	***9***
Горєлишев С. А.	- кандидат технічних наук, доцент, старший науковий співробітник науково-дослідної лабораторії Науково-дослідного центру	***18***
Душкін В. Д.	- кандидат фізико-математичних наук, доцент, професор кафедри	***24***
Єльчанінов О. Д.	- кандидат технічних наук, доцент, професор кафедри	***73***
Іохов О. Ю.	- доктор технічних наук, с.н.с., доцент, начальник кафедри	***75***
Казіміров О. О.	- кандидат військових наук, доцент, доцент кафедри	***96***

Каплун Є. О.	- ад'юнкт	***114***
Козлов В. Є.	- кандидат технічних наук, доцент, доцент кафедри	***112,113***
Лазарев В. Д.	- старший викладач кафедри	***112***
Майборода І. М.	- кандидат військових наук, доцент, доцент кафедри	***107, 117***
Малюк В. Г.	- кандидат технічних наук, доцент, професор кафедри	***75,96***
Мельник В. М.	- старший викладач кафедри	***24,44***
Нефедов О. П.	- кандидат технічних наук, доцент, доцент кафедри	***44***
Оленченко В. Т.	- кандидат технічних наук, заступник начальника кафедри	***107,113***
Павлов С. П.	- кандидат технічних наук, доцент, начальник факультету	***68***
Романюк В. А.	- кандидат технічних наук, доцент, доцент кафедри	***105***
Сальніков О. М.	- кандидат технічних наук, доцент, доцент кафедри	***30,111***
Семенко Є. Ю.	- ад'юнкт	***116***
Сидоренко І. І.	- кандидат педагогічних наук, доцент, доцент кафедри	***44***
Ткаченко К. М.	- ад'юнкт	***75,103***
Фик О. І.	- доктор технічних наук, доцент, доцент кафедри	***107,108***
Флорін О. П.	- кандидат технічних наук, доцент, доцент кафедри	***107***
Шамшин О. П.	- кандидат фізико-математичних наук, доцент, доцент кафедри	***97***
Яковлев М. Ю.	- доктор технічних наук, професор, старший науковий співробітник науково-дослідної лабораторії Науково-дослідного центру	***116***
Glushchenko M.	- старший викладач кафедри	***101***
Novykova O. ***(Новикова О. О.)***	- кандидат технічних наук, доцент кафедри	***101,113***

Національна академія Служби безпеки України, м. Київ

Ходич О. В.	- кандидат технічних наук, старший викладач кафедри	***117***

Національна академія Сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів

Болцарівський А. І.	- курсант	***42***
Дзюба А. О.	- начальник факультету	***42***
Корнієнко О. В.	- начальник науково-дослідної лабораторії факультету	***39,42,43***
Кравець М. О.	- курсант	***50***
Кравець Т. М.	- кандидат географічних наук, викладач кафедри	***50.53***
Левкович П. В.	- викладач кафедри	***42,43,51***
Олійник С. Е.	- викладач кафедри	***15***
Пастухов В. В.	- науковий співробітник науково-дослідної лабораторії науково-дослідного відділу (підготовки військ) Наукового центру Сухопутних військ	***39,43***
Петлюк І. В.	- кандидат технічних наук, старший науковий співробітник науково-дослідного відділу (інженерних військ) Наукового центру Сухопутних військ	***48***
Полець О. П.	- старший викладач кафедри	***53***
Поліщук А. М.	- старший викладач кафедри	***39***
Сівак О. І.	- науковий співробітник науково-дослідної лабораторії факультету	***39,43***
Щерба А. А.	- кандидат технічних наук, доцент, старший викладач кафедри	***48***
Lavrut O. ***(Лаврут О. О.)***	- доктор технічних наук, доцент, професор кафедри	***8,44***
Lavrut T.	- кандидат географічних наук, доцент, старший науковий співробітник науково-дослідного відділу (систем управління військами) Наукового центру Сухопутних військ	***8***

Національний авіаційний університет, м. Київ

Гайченя Д. В.	- курсант	***80***
Грозан О. С.	- курсант	***82***
Кульбашевський В. А.	- викладач кафедри	***80,82***
Маліновський А. В.	- старший викладач кафедри	***83***
Марценюк С. О.	- старший викладач кафедри	***81***
Міщук В. П.	- курсант	***81***
Приходько Ю. І.	- кандидат педагогічних наук, доцент, старший викладач кафедри	***25***
Ткаченко В. А.	- кандидат технічних наук, доцент кафедри	***80,81,82***
Целіщев І. О.	- старший викладач кафедри	***80***
Яновська Т. Г.	- викладач кафедри	***83***
Яновський П. О.	- кандидат технічних наук, доцент, професор кафедри	***80,81,82,83***

Яременко В. В.	- старший викладач кафедри	***81,82***

Національний педагогічний університет імені М. П. Драгоманова, м. Київ

Кільдеров Д. Е.	- доктор педагогічних наук, професор, декан факультету	***28***
Пригодій М. А.	- доктор педагогічних наук, професор, завідувач кафедри	***28***

Національний технічний університет «КПІ імені Ігоря Сікорського», м. Київ

Даник Ю. Г.	- доктор технічних наук, професор	***46***

Національний університет оборони України імені Івана Черняховського, м. Київ

Batkovskiy S.	- слухач	***33***

Одеська національна морська академія

Кучер Д. Б.	- доктор технічних наук, професор, професор кафедри	***108***

Український державний університет залізничного транспорту, м. Харків

Ковтун І. В.	- кандидат технічних наук, доцент, доцент кафедри	***45***

Харківський національний університет будівництва та архітектури

Орлов М. М.	- доктор наук з державного управління, професор кафедри	***103***

Харківський національний університет внутрішніх справ

Коршенко В. А.	- кандидат юридичних наук, завідувач науково-дослідної лабораторії	***23***
Мордвинцев М. В.	- кандидат технічних наук, доцент, провідний науковий співробітник науково-дослідної лабораторії	***84***
Ницюк С. П.	- старший науковий співробітник науково-дослідної лабораторії	***84***
Пашнєв Д. В.	- кандидат юридичних наук, доцент, провідний науковий співробітник науково-дослідної лабораторії	***23***
Хлєстков О.В.	- старший науковий співробітник науково-дослідної лабораторії	***84***

Харківський національний університет імені В. Н. Каразіна

Дядюн С. В.	- кандидат технічних наук, доцент, доцент кафедри	***99***

Харківський національний університет міського господарства імені О. М. Бекетова

Метешкін К. О.	- доктор технічних наук, професор, професор кафедри	***60***

Харківський національний університет Повітряних Сил імені Івана Кожедуба

Бекіров А. Е.	- кандидат технічних наук, старший викладач кафедри	***5***
Борисов В. В.	- викладач кафедри	***35***
Гайбадулов Б .В.	- заступник начальника кафедри	***31,35***
Галицький О. Ф.	- кандидат технічних наук, доцент, професор кафедри	***31***
Губін С. Д.	- викладач кафедри	***36***
Камчатний М. І.	- кандидат технічних наук, доцент, доцент кафедри	***31***
Коробков Ю. В.	- викладач кафедри	***36***
Красноруцький А. О.	- кандидат технічних наук, викладач кафедри	***27***
Моргун Є. В.	- старший викладач кафедри	***31***
Олексін О. О.	- старший викладач кафедри	***27***
Помогаєв І. В.	- старший викладач кафедри	***36***
Сєчіна А. С.	- курсантка	***5***
Скорик А. Б.	- кандидат технічних наук, доцент, доцент кафедри	***31,35,36***
Сургай М. В.	- старший викладач кафедри	***35***
Таршин В. А.	- доктор технічних наук, професор, начальник кафедри	***36***
Титаренко Р. В.	- викладач кафедри	***35***
Chmil Yu.	- помічник начальника навчального відділу факультету	***32***
Djus V.	- кандидат технічних наук, доцент кафедри	***32***
Grechka A.	- викладач кафедри	***33***
Herasimov S.	- доктор технічних наук, професор, заступник начальника кафедри	***10,34***
Kalugin D.	- кандидат технічних наук, с.н.с., старший науковий співробітник Наукового центру Повітряних Сил	***33***
Kovalenko S.	- кандидат технічних наук, доцент, доцент кафедри	***14***
Kovalenko V.	- магістрант кафедри	***35***

Kriuchkov D.	- викладач кафедри	***35***
Kudryashov V.	- кандидат технічних наук, с.н.с., доцент кафедри	***13***
Kutsenko V.	- кандидат технічних наук, доцент кафедри	***15***
Kuzmenko D.	- магістрант кафедри	***35***
Litovchenko D.	- кандидат технічних наук, старший викладач кафедри	***13***
Muhartov A.	- бакалавр кафедри	***33***
Pavlenko M.	- доктор технічних наук, професор, начальник кафедри	***35***
Pluzhnik O.	- магістрант кафедри	***35***
Reznichenko A.	- начальник факультету	***32***
Roshchupkin E.	- кандидат технічних наук, с.н.с., старший викладач кафедри	***10,34***
Roshchupkina A.	- студентка	***34***
Shulezhko V.	- кандидат військових наук, доцент, начальник кафедри	***34***
Sikachov O.	- бакалавр кафедри	***33***
Skopintsev O.	- доцент кафедри	***32***
Taran M.	- магістрант кафедри	***34***
Volkov A.	- завідувач кафедри	***14***
Zaberezhniy D.	- керівник групи навчально-тренувального комплексу факультету	***32***

Харківський національний університет радіоелектроніки

Бабічева А. К.	- студентка	***52***
Баранник В. В.	- доктор технічних наук, професор кафедри	***27***
Безкоровайний В. В.	- доктор технічних наук, професор, професор кафедри	***71,77***
Безугла Г. Є.	- старший викладач кафедри	***49***
Борзенков Б. І.	- кандидат технічних наук, доцент, професор кафедри	***96***
Васильцова Н. В.	- кандидат технічних наук, с.н.с., доцент, професор кафедри	***52,54***
Гребенюк В. О.	- старший викладач кафедри, директор Центру технологій дистанційного навчання	***69***
Єрошенко О. А.	- асистент кафедри	***102***
Каук В. І.	- кандидат технічних наук, доцент кафедри, науковий керівник Центру технологій дистанційного навчання	***68,69,70***
Канашевич Д. В.	- магістрант	***87***
Козлов Ю. В.	- кандидат технічних наук, доцент, докторант	***113***
Кузьма Є. А.	- студентка	***54***
Ляшик В. А.	- аспірант	***89***
Мустафаєв Є. О.	- магістрант	*90*
Новікова К. А.	- студентка	*102*
Прасол І. В.	- доктор технічних наук, доцент, професор кафедри	*102*
Пуголовок К. М.	- провідний інженер Центру технологій дистанційного навчання	***70***
Судік А. О.	- студент	***71***
Циблієва Н. О.	- магістрантка	***92***
Швець К. В.	- магістрантка	***94***
Шубін І. Ю.	- кандидат технічних наук, доцент, професор кафедри	***87,89,90,92,94***
Шульгін С. С.	- кандидат технічних наук, докторант кафедри	***27***
Fedorenko Y. ***(Федоренко Є.)***	- студентка	***106***
Kirichenko L. ***(Кіріченко Л. О.)***	- доктор технічних наук, професор, професор кафедри	***106***
Kobziev V. ***(Кобзєв В .Г.)***	- кандидат технічних наук, с.н.с., доцент кафедри	***106***

Управління стандартизації та кодифікації Міністерства оборони України, м. Київ

Чуйков Д. В.	- старший офіцер	***114***

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, м. Київ

Полторак М. Ф.	- кандидат військових наук, доцент, старший науковий співробітник	***5***
Chernykh O. ***(Черних О. Б.)***	- старший науковий співробітник	***5,6***

Центральний науково-дослідний інститут озброєння та військової техніки, м. Киів

Стрижак О. Є.	- доктор технічних наук, професор, провідний науковий співробітник	***116***

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.