НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ "ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ М. Є. ЖУКОВСЬКОГО "ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"

УНІВЕРСИТЕТ МІСТА ЖИЛІНА

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей тринадцятої міжнародної науково-технічної конференції

26 – 27 квітня 2023 року

Том 1: секції 1, 3, 4

Баку – Харків – Жиліна – 2023

УДК 004/681.3 doi: https://doi.org/10.32620/ ICT.23.t1

У збірнику подано тези доповідей тринадцятої міжнародної науково-технічної конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління". Розглянуті питання за такими напрямами: теоретичні та прикладні аспекти систем прийняття рішень, оптимізації та управління системами і процесами; комп'ютерні методи та засоби інформаційно-комунікаційних технологій та управління; безпека функціонування комп'ютерних систем та мереж; інформаційні технології у цивільній безпеці; сучасні інформаційно-вимірювальні системи; інформаційні технології у цивільній безпеці.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Тринадцята міжнародна науково-технічна конференція “Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління” проводиться 26 та 27 квітня 2023 року в режимі ONLINE. Тези доповідей доступні в INTERNET.

ТОМ 1

СЕКЦІЯ 1. Теоретичні та прикладні аспекти прийняття рішень, оптимізації та управління системами і процесами

Керівниця секції: д.т.н., проф. Н. Г. Кучук, НТУ «ХПІ», Харків
Секретар секції: к.т.н., доц. С. С. Бульба, НТУ «ХПІ», Харків

СЕКЦІЯ 3. Безпека функціонування комп’ютерних систем та мереж

Керівник секції: д.т.н., проф. О. А. Смірнов, ЦНТУ, Кропивницький
Секретар секції: к.т.н., доц. О. В. Сєвєрінов, ХНУРЕ, Харків

СЕКЦІЯ 4. Застосування інформаційно-комунікаційних технологій у різних галузях

Керівник секції: д.т.н., проф. В. В. Косенко, НУ «ПП», Полтава
Секретарка секції: к.т.н. Бельорін-Еррера О. М., НТУ «ХПІ», Харків

Підсекція 4.1. Сучасні інформаційно-вимірювальні системи

Підсекція 4.2. Інформаційні технології у цивільній безпеці

ТОМ 2

СЕКЦІЯ 2. Комп’ютерні методи і засоби інформаційно-комунікаційних технологій та управління

Керівники секції: д.т.н., проф. І. В. Рубан, ХНУРЕ, Харків
д.т.н., проф. А. А. Коваленко, ХНУРЕ, Харків
Секретар секції: к.т.н., доц. О. С. Ляшенко, ХНУРЕ, Харків

СЕКЦІЯ 1
ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ПРИЙНЯТТЯ РІШЕНЬ, ОПТИМІЗАЦІЇ ТА УПРАВЛІННЯ СИСТЕМАМИ І ПРОЦЕСАМИ

Керівниця секції: д.т.н., проф. Н. Г. Кучук, НТУ «ХПІ», Харків
Секретар секції: к.т.н., доц. С. С. Бульба, НТУ «ХПІ», Харків

ABOUT SOME ASPECTS OF USING A FLOCK OF UAVS

Hashimov E.G., Talibov A.M., Pashaev A.B., Sabziev E.N.
National Defense University, Baku, Azerbaijan

When solving military issues, it is considered expedient to use a flock of unmanned aerial vehicles (UAVs) to increase the probability of success of the task [1]. The use of a swarm of UAVs in combat operations arose due to the need to perform tasks that one UAV could not solve alone.

The introduction of a flock of UAVs for military purposes should include the solution of the following issues:

1. UAV flight control along the route to the combat zone.
2. Ensuring order of battle.
3. Target detection.
4. Targeting
5. Distribution of detected targets.
6. Safe transportation of dangerous goods.
7. Use of weapons.

The report discusses the tactics of using a swarm of UAVs, presents the principles and approaches to solving each issue.

UAV flight control to the operational zone along the route. The route (task) of a flock of UAVs consists of successive passage of points indicated by geographical coordinates and flight at a certain height above sea level. In order for a flock of UAVs to approach the target covertly, the route of movement is set in such a way that, as far as possible, it passes through such places as valleys and riverbeds, ravines [2]. However, the operator chooses the route in such a way that the UAVs can pass obstacles at a safe distance and without collisions with each other when flying around this route [3].

Ensuring order of battle. The number of UAVs used in a mission can vary depending on the number of targets and the size of the area. UAVs must search for and identify targets by video recording on the final section of the route. A flock of UAVs flies in formation towards the target. At a distance of 300 m from the target, UAVs line up side by side (in a chain). UAVs must hit the target immediately after the transition from the en-route flight mode to the appropriate battle formation.

Distribution of detected targets. For an attack from a battle formation, the distribution of targets between the UAVs must be carried out. According to the distribution algorithm, the target that each UAV will attack should be determined.

The detonation of the ammunition must be carried out using an electronic switch, the switch safety must be regulated by mechanical and electronic means.

Safe transportation of dangerous cargo. Depending on the purpose, the form of explosive and the type of fragmentation must be selected. The detonation of the explosive is carried out by an electric detonator. An intelligent electronic system must be created to ensure safety when installing the detonator. This system usually isolates the detonator from all lines.

Mechanism of action of the weapon. A device for working with weapons should be created with the implementation of mechanisms that ensure the safety of users. For this purpose, an autonomous power source is not provided in the explosive system circuit. The power supply to the explosive system is carried out only after the UAV takes off and by means of a special readiness command from the control panel, and the power explosive system is in readiness and awaits the command to explode.

Target detection. Algorithms and corresponding software modules should be developed to recognize objects on video camera images, point the UAV at a target and determine its location from these images. Artificial intelligence methods are used to identify objects in camera images.

It is planned to create a software module for recognizing targets on images from video cameras. To do this, it is necessary to carry out the following work: creation of a reference base of manpower silhouettes observed from different angles; development of an algorithm for identifying the silhouettes of manpower on images from video cameras; development and testing of a software module for target recognition in images.

In addition, a targeting system must be developed. This system involves guiding the UAV on images from the video camera in such a way that it flies over the target and is at a distance that can ultimately destroy the target. The solution of the problem requires the development of such a control strategy that at the stage of aiming at the target, its image remains in the center of the video camera image. The onboard intelligent processing system must estimate the current deviation of the target's vision from the center of the image and determine the recalculated direction of the UAV flight to eliminate this deviation.

References

1. Hasanov A.H., Pashayev A.B., Sabziyev E.N. Determining the direction of the UAV group towards the source of radio wave radiation // Republican scientific-practical conference dedicated to the 2nd anniversary of the victory in the 44-day national war. materials, November 2-3, 2022, Baku, pp. 190-192.

2. Sabziev E.N. Algorithm for determining the trajectory of maneuvers along the planned route on a geometric map of the terrain // Informatics and Control Problems, 40, No. 2 (2020), P. 43-49.

3. Alizade T., Nabadova G., Gurbanov A. Development of a local positioning system for unmanned aerial vehicles participating in a joint flight // Republican scientific-practical conference dedicated to the 2nd anniversary of the victory in the 44-day national war. materials, November 2-3, 2022, Baku, pp. 214-216.

ACOUSTOO-OPTICAL RECEIVER OF AN OBSTRUCTION PASSIVE RADAR SYSTEM

Rustamov A.R., Katekhliev V.M.
National Defense University, Baku, Azerbaijan

The complexity of separating signals against the background of passive obstacles in the receiving system of radar instruments of warships is due to the fact that the obstacle, like the useful signal, is also reflected in the bandpass filter [1, 2].

It is advisable to have an acousto-optic receiver as the main component of a passive radar system for radar obstacles on warships. At the same time, the effectiveness of radar barrage stations and dipole reflectors in detecting and neutralizing a radiation source directly depends on the characteristics of the receiver. In this case, the receiver itself must have high noise immunity in the operating conditions of radio transmission systems. All this testifies to the need to use special methods and means that provide high noise immunity in acousto-optical receivers of a passive radar system on warships [3].

Research aimed at eliminating defects found in the application of impulse barrier suppression methods created the conditions for the application of a new method called synchronous impulse barrier compensation [2]. In more detail, the way to compensate for impulse barriers can be explained by the block diagram shown in Fig. 1. Two band-pass filters (BF) were used in the circuit. The mixture of the signal and the obstacle $u_s(t) + u_{n1}(t)$ is selected with the help of BF1, and a part of the spectrum of the impulse barrier $u_{n2}(t)$ in frequency domain is selected with the help of BF2, which is hushed up, but has components [2, 4].

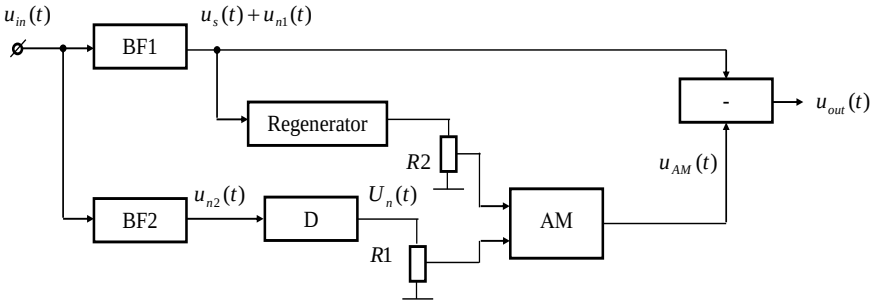

Figure 1 – Device for studying the method of synchronous compensation

The circuit also used an amplitude modulator (AM). An isolated voltage Un(t) is applied to its input. Zero-phase reference oscillations recovered from the output signal of (BF1) are fed to the second input of the AM. As a result, oscillations with amplitude modulation $U_{AM}(t)$ are formed in the AM. These generated oscillations act as an obstacle with a carrier frequency equal to the frequency of the desired signal. Such formation of a compensating signal can be expressed by the expression

$u_{AM}(t) = u_{n1}(t)$. The compensating signal $U_{AM}(t)$ is subtracted from the mixture of the signal $u_s(t) + u_{n1}(t)$ and the impedance in the corresponding device. Complete damping of the impulse barrier occurs:

$$u_{out}(t) = u_s(t) + u_{n1}(t) - u_{AM}(t) = u_s(t)$$

The selection of the modulating voltage by the potentiometer R1 and the amplitude of the carrier oscillations by the potentiometer R2 leads to complete compensation of the impulse barriers. Fig. 2 shows the doubling of the impedance amplitude and waveform at the output of the output device after a phase shift [5].

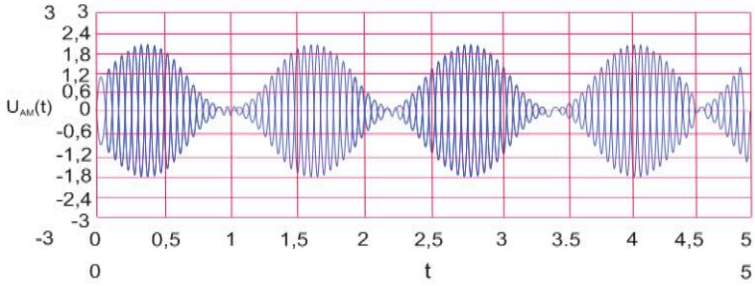

Figure 2 – Waveform at the output of the output device

Result

Having determined the influencing factors when receiving certain parameters in unobstructed and cluttered conditions, the difficulty of separating signals against the background of passive obstacles as a result of the use of an acousto-optic receiver of a passive radar system of surface ships, the reflection of an obstacle as a useful signal in a bandpass filter, facilitates the selection of an additional receiving channel necessary to weaken the blocking and targeting obstacles. Frequency response depends on tuning frequency

References

1. Rustamov A. R., Gurbanov M. A., Babashov E. Kh. Theoretical foundations of radio engineering observation. Baku, AAHM named after H. Aliyev, 2020, 208 p.

2. A. R. Hasanov, R. A. Hasanov, A. R. Rustamov Using the features of the photoelastic effect to measure the parameters of optoelectronic devices. Успехи прикладной физики, 2021, том 9, № 5 p.430-441

3. Gasanov A., Gasanov R., Rustamov A. Development of an axonometric model of photoelastic interaction in an acousto-optic delay line and its approval. technological audit and production reserves - No. 5/2(67), 2022, pp. 38-45

4. Gasanov R.A., Eynullaev V.S., Rustamov A.R. Method for synchronous compensation of impulse barriers. Patent-invention I 2013 0026.

5. A. R. Hasanov, R. A. Hasanov, A. R. Rustamov Broadband amplitude demodulator based on the photoelastic effect and optimization of its characteristics. Uspekhi Prikladnoi Fiziki (Advances in Applied Physics), 2023, vol. 11, № 1 p.81-88.

APPLICATION OF MEANS OF REMOTE RADIATION RECONNAISSANCE

Akhundov R.G.
Military Research Institute of the National Defense University, Baku, Azerbaijan

The high efficiency of the radiation protection of troops can be achieved provided that the military system for detecting the radiation, chemical and biological situation (MSDS) ensures timely receipt of data that makes it possible to adequately assess the possible losses of personnel engaged in combat operations in conditions for the use of nuclear weapons or radiation accidents.

In this regard, the fundamental requirements for this system are the efficiency and reliability of detecting the radiation situation [1]. The modern MSDS is built on a linear hierarchical principle and consists of subsystems of the same type in structure, each of which functions in the interests of the command of a certain military level, as a rule, at the tactical or operational-tactical level [2].

The structure of a typical modern subsystem MSDS includes a point of collection and processing of information (PCPİ) and a set of automated mobile complexes of radiation, chemical and biological reconnaissance (AMC RCBR), the number of which is determined depending on the level of the corresponding military unit. The central, system-forming element of each subsystem is the PCPİ, which in the formations and associations are, respectively, the settlement and analytical groups (SAG) and the settlement and analytical stations (SASt). Currently, a reconnaissance vehicle of the RCM-4 type can be considered as a typical AMC RCBR, equipped with automated reconnaissance devices and their control tools, as well as data transmission equipment to a telecode communication channel organized with a PCPİ.

Despite its good efficiency, modern MSDS nevertheless does not allow achieving a sufficiently high probability of obtaining complete and reliable intelligence data with the required efficiency in highly maneuverable, dynamic combat operations. This is due, first of all, to the low adaptive ability of the system to the losses of the AMC RCBR.

Thus, the disabling of even one AMC RCBR entails the loss of information about radiation levels in one of the areas controlled by the system of the region. If this information is of significant value when, for example, an important facility (object) is located in the area, then it should be considered that the effectiveness of MSDS in the current situation is unacceptably low.

An increase in the probability of detecting the situation can be achieved by increasing the regular number of AMC RCBR in each of the subsystems of the MSDS. Additional reconnaissance complexes can be a reserve of the system, used in the event of losses in order to maintain the effectiveness of detecting the situation at the required level.

However, it is obvious that such a direction of development requires significant economic costs both during the period of system modernization and at the stage of its operation. Therefore, it is necessary to find internal reserves of the system in order

to ensure its high efficiency even in difficult operating conditions, and without increasing the staffing number of the AMC RCBR and the resources necessary to identify the situation.

The general algorithm for the functioning of the MSDS with the introduction of remote reconnaissance means into its composition involves the following activities: tracking of radioactive clouds by remote reconnaissance complexes; determination of the configuration of the area of radioactive contamination of the area; calculation of coordinates of control points at which it is necessary to measure the parameters of infection; determination of exploration routes; conducting radiation reconnaissance AMC RCBR.

Management in MSDS should be aimed at dynamic refinement of the area of radiation reconnaissance by remote reconnaissance complexes on the basis of data received by local reconnaissance complexes. The interaction of local and remote reconnaissance complexes in the process of identifying the radiation situation will be carried out not directly, but through PCPI used as an intermediate link. When building a system according to this principle, it becomes possible to use separate communication channels for transmitting intelligence data and for transmitting cloud sounding results.

It should be noted, however, that the expediency of the stated direction of development of MSDS will be achieved only if the costs of introducing remote reconnaissance complexes into its composition are compensated by reducing the local reconnaissance complexes. In the event that the entire strip controlled by the MSDS subsystem is scanned by one remote reconnaissance complex, then its allowable cost has a maximum value and is determined by how much the required number of AMC RCBR can be reduced.

Thus, the analysis carried out shows that the improvement of the modern military system for detecting radiation, chemical and biological conditions involves the introduction of new reconnaissance complexes designed to remotely determine a number of parameters of damaging factors. Undoubtedly, the creation of highly effective remote NBC reconnaissance systems requires the solution of a number of complex scientific and technical problems, as a result of which they will be one of the most high-tech examples of modern military equipment. The introduction of these complexes, along with equipping the troops with other promising weapons, will allow the Armed Forces to successfully maintain parity with the armies of the technologically advanced countries of the world.

References

1. Manual on the combat use of chemical weapons - Baku: Military Publishing House, 2016. - 216 p.

2. Hashimov, E.G., Muradov, S.A. Application of stable navigation system in unmanned aerial vehicles for reconnaissance purposes / - Baku: National security and military sciences, - 2022. No. 3(9), - p.65-72.

MINIMIZATION OF MILITARY UAV ENERGY CONSUMPTION DURING RECONNAISSANCE FLIGHTS

Bayramov A.A.
İnstitute of Control Systems, Baku, Azerbaijan

During reconnaissance flight of military Unmanned Aerial Vehicle (UAV) for data gathering, one of the key tasks is to plan the path in such a way as to minimize the energy consumption. Most existing methods usually take the shortest flight distance as the optimal target for planning the optimal path, i.e. it is assumed that the shortest path means the least energy consumption of the UAV. However, it should be taken into account that a change in course can also consume the energy of the UAV in flight, because any change in the flight course is associated with the acceleration of the UAV. This in turn causes an increase in energy consumption [1, 2]. There have been considered and offered many options for saving energy consumption.

In this work, in order to achieve a solution to this problem, various criteria for an energy-saving UAV flight are considered. The following criteria for minimizing energy consumption during UAV flight have been developed:

1. UAV flight should be as low as possible, the higher the flight of the drone, the lower the air density, and the lower the lift, in order to compensate for this, it is necessary to increase the thrust, and this leads to an increase in energy consumption;

2. Most tactical UAVs fly at altitudes up to 1500 m. Considering that the air density changes by only 0.09% up to a height of 1000-1500 m, it is possible to quickly reach cruising speed when climbing, while energy consumption will be optimal;

3. After completing the task, when the UAV returns to the base, if possible, the gentlest descent from a given height at a minimum speed should be made;

4. One of the important criteria is the optimal flight during barrage with the choice of the shortest trajectories between given objects on the ground that are to be investigated;

5. When developing a flight task, choose such modes, in which the flight occurs, if possible, with uniform rectilinear motion, with the least curvature of the trajectory, with fewer turns;

6. When performing a reconnaissance flight, in which the task is to examine (photograph) some objects on the ground, it is recommended to use a wide-angle lens. This achieves the possibility of covering more objects in the frame with one shooting.

7. It is proposed to optimize the power of the radio transmitter, designed for data transmission. The more powerful the radio transmitter, the greater the power consumption.

8. Energy efficient planning by a system of several UAVs that track events and objects on the surface of the earth. UAVs themselves adjust their height so that each time they cover more or less objects. This self-control is achieved by radio communication between the UAVs and results in energy savings of up to 150% compared to the case when the UAVs are placed statically.

9. Joint optimization of both energy efficient (capacity) radio communication and UAV flight path.

10. Optimization of the operation of a reconnaissance remote sensing UAV flying in an energy-information-efficient mode, when information is transmitted using special filters.

11. The use of faster processors will allow the UAV to complete missions quickly and therefore save energy. This is because most of the UAV's energy is consumed by the motor, hence faster calculations can reduce mission time and energy accordingly. Improvement is achieved up to 5 times.

12. Planning the UAV monitoring path in such a way as to minimize the UAV power consumption. The bottom line is to minimize the amount of course change and maximize the amount of straight flight range.

13. To reduce the power consumption of the UAV, limit the number of UAV flight adjustments while still keeping the target in the camera's field of view.

14. Application of energy-efficient brushless DC motors for UAVs with electric motors. The use of these drives leads to a decrease in the dimensions and weight of the UAV and to a decrease in power consumption.

Thus, the paper notes the importance of choosing an energy-saving UAV flight mode. In order to minimize energy consumption, 14 criteria for UAV flight modes were considered and proposed to save energy consumption.

References

1. Bayramov A.A. Management of UAV energy consumption minimization. Journal of Defense Resources Management. Vol. 13(25), Is.2. 2022. p.113-118.

2. Bayramov A.A. Minimization of energy consumption for unmanned dynamic object / International Ankara Congress on Scientific Research IV. The Proceedings Book April 1-3, 2022 Ankara/ TURKEY. P.513.

ON AN İNVERSE PROBLEM FOR HYDROGEN ATOM EQUATİON

Panahov E.
Military Scientific Research Institute, National Defense University Azerbaijan

Abstract. İn this work it is considered of the existence of the transformation operator for the energy levels of the hydrogen atom which is important quantum mechanics.

Introduction. Consider the stationary Schrödinger equation for two particles in dimensionless variables,

$$-\left(\frac{\partial \emptyset}{\partial x}+\frac{\partial \emptyset}{\partial y}+\frac{\partial \emptyset}{\partial z}\right)+V(x,y,z)=k^2\emptyset. \qquad (0.1)$$

İf the potential function $V(x,y,z)$ depends only on $r^2=x^2+y^2+z^2$, i.e. $V(x,y,z)=V(r)$, then the variables in equation (0.1) can be separated by putting

$$\emptyset(x,y,z)=\frac{\varphi(r)}{\sqrt{r}}\,Y_m^l(\theta,\varphi) \qquad l=0,1,2,....$$

where $x=r\sin\theta\cos\varphi$, $y=r\sin\theta\sin\varphi$, $z=r\cos\theta$ and $Y_m^l(\theta,\varphi)$ are spherical harmonics. This gives a differential equation of the form

$$\frac{d^2\varphi}{dr^2}+\frac{1}{r}\frac{d\varphi}{dr}-\frac{\mu^2}{r^2}\varphi-V(r)\varphi+k^2\varphi=0. \qquad (0.2)$$

for the function $\varphi(r)$ where $\mu = l + \frac{1}{2}$, $(l = 0,1,2,\dots)$. If the potential function $V(r)$ satisfies the condition $\int_0^\infty rV(r)\,dr < \infty$, then for a solution of equation, which is regular at zero and normalized, so following asymptotic formula is satisfied

$$\sqrt{r}\varphi(r,k,\mu) = A(k,\mu)\sin\left[kr - \frac{\pi}{2}\left(\mu - \frac{1}{2}\right) + \delta(k,\mu)\right] + o(1).$$

For fixed μ and k and $r \to \infty$. In this formula $A(k,\mu)$ is called the scattering amplitude and $\delta(k,\mu)$ the scattering phase or phase shift [1– 3].

Main results. Consider the equation

$$\frac{d^2R}{dr^2} + \frac{2}{r}\frac{dR}{dr} - \frac{l(l+1)}{r^2}R - \left(E + \frac{2}{r}\right)R = 0 \quad (0 < r < \infty). \tag{1.1}$$

In quantum mechanics, the study of the energy levels of a hidrogen atom leads to this equation [4, 5] The substitution $R = \frac{y}{r}$ reduces equation (1.1) to the form

$$\frac{d^2y}{dr^2} + \left(E + \frac{2}{r} + \frac{l(l+1)}{r^2}\right)y = 0. \tag{1.2}$$

Just as in the case of Bessel equation, one can Show that, in a finite interval [0,1] the spectrum is discrete. As known [5], for a solution (1.2) which is bounde at zero, one has the following asimptotic formula for $\mu \to \infty$ $(E = \mu)$

$$\varphi(r,\mu) = \frac{e^{\frac{\pi}{2\mu}}}{\gamma(l+1+\frac{i}{\mu})}\frac{1}{\sqrt{\mu}}\cos\left[\sqrt{\mu}r + \frac{1}{\sqrt{\mu}}ln\sqrt{\mu}r - (l+1)\frac{\pi}{2} + \alpha\right] + o(1), \tag{1.3}$$

where $\alpha = arg\gamma\left(l + 1 + \frac{1}{\sqrt{\mu}}\right)$.

We study an inverse problem with two given spectra for a second order differential operator with singularity of the type $\frac{2}{r} + \frac{l(l+1)}{r^2}$ at zero point. It is well known [6, 7] that two spectra uniquely determine the potential function in a singular Sturm-Liouville equation defined on the finite interval. One of aims this work is to prove the generalized degeneracy of the kernel. In particular we obtain a new proof of Hochstadt's and Levitan theorems concerning the structure of the difference potentials:

$$K(r,s) = \sum_{i=0}^{N} c_i\varphi_i(r)\vartheta_i(s), \qquad q_1(r) - q_2(r) = 2\frac{dK(r,r)}{dr}$$

In conclusion, we note that in the study of many strategic problems, are often used methods for solving inverse problems of the theory of scattering, spectral analysis and potential theory.

References

1. Levitan, B.M., 1987, Inverse Sturm-Liouville Problems., Utrecht, Netherlands.
2. Marchenko, V.A., 1977, Sturm-Liouville Operators and their Applications. Naukova Dumka, Kiev.
3. Chadan, K., Colton, D., Paivarinta, L. and Randell, W., 1997, An introduction to inverse scattering and inverse spectral problems. SIAM,Philadelphia, USA
4. Jaulent,M., and Jean, C., 1972, The inverse s-wave scattering problem for a class of potentials depending on energy. Communications in mathematical Physics., v.28,pp. 177-220.
5. Fock, V.A., 1932, Fundementals of Quantum Mechanics, Leningrad University.
6. Panakhov, E.S., and Yılmazer, R. 2012, A Hochstadt-Liberman theorem fort he hydrogen atom equation. Applied and Computational Mathematics, vol. 11, no.1, pp. 74-80.

7. Panakhov, E.S. and Sat, M., 2012, Inverse problem for interior spectral data of the hirogen atom equation. Ukraine Math. Journal, vol.64, no.11, pp.1516-1525.

ESTIMATE TARGETS ACCORDING STRUCTURE AND DOCTRINE

Hashimov E.G., Huseynov M.A.
National Defense University, Baku, Azerbaijan

This paper explained the concept of target in the military publications of foreign countries contains information about the analysis, processing, classification, classification of targets and the implementation process of general target activities. The classification of targets in the armed forces of NATO countries and the factors that make this classification necessary are explained. The methods of target planning are explained and, taking into account some factors arising from these methods, a method of predicting the targets that will appear during any confrontation that will appear in accordance with the military structure of the armed forces of the enemy or the opposite party (with the possibility of a threat) is presented.

Targets are military and strategic objects and elements that makes essential for enemy's operations, whose destruction (fire strike, etc. impact, interventions) will affect the success of offensive and defensive operations of our troops [1].

Target management is the process of determining the necessary effects to achieve a military objective, using the appropriate course of action to create the desired effect with the available capabilities. Selecting and determining the value, prioritizing of targets, synchronizing fires with all military capabilities and evaluating their overall effects and replanning for the desired effect if necessary [2].

Classification of Targets Management. After identified targets, there have to done a planning process, and weapon systems must be selected based on the type of target to engage them [3]. However, planning and choosing weapons in advance is not always possible, it is depending on circumstance and conditions. Battlefield conditions and timing makes it necessary to take into account the planned targets as well as the pup up targets [4].

The target analysis planning activity is part of the MDMP process, it is a necessary activity that serves to achieve the commander's intent and purpose and is carried out to achieve the objective. Thus, target analysis and planning activities serve the same purpose as MDMP [5].

To achieve target planning process in advance it is necessary to have a preliminary forecast or a most probability of the targets of enemy. According doctrine and standard conditions may determine the targets and reallocate the necessary weapons.

The calculation of the number of targets in a target category can be done as follows, to give the probability of (expected) targets to be detected in an encounter with the armed forces of any enemy country. or potential adversary. The calculation of targets by level is directly proportional to the level of the unit, and the number of elements to be divided into categories must initially be determined, taking into account the size of the units and the type of troops.

For example: In an infantry (motorized rifle) brigade, let's assume a total of 6 deployment or command posts, including 1 brigade headquarters, 4 battalions, and 1 rear command post (supply point). A total of 5 targets, including 3 battery firing positions, 1 command and control post with 1 supply point in the same artillery division. The brigade is to be protected by 2 SAMs (OSA, OSA AKM), which means it will have 2 air defense targets. From here we can conclude that under standard conditions and tactical norms one motorized rifle brigade may have 6+5+2=13 targets (these figures are for approximate calculation).

$$Bh = h_1 + h_2 + \cdots + h_n = \sum_{i=1}^{n} h_i. \quad (1)$$

Similar to the above calculation, it is possible to estimate the number of targets that would appear under standard unit conditions at any level by making a calculation for other branches of the military units. During these calculations, as the level of the unit increases, the HQ of that unit and its support and combat elements must be taken into account. Thus, when conducting corps calculations, the number of subordinate brigades, subordinate units and, in addition, elements of corps headquarters and command posts and additional units must be added up. The calculation can be made using the following formula.

$$Kh = n \times Bh + k_1 + k_2 + \cdots + k_m = n \times Bh + \sum_{j=1}^{m} k_j. \quad (2)$$

Here " Kh " is the army corps target number, n is the constant number of brigades, k_m is the number of other units and headquarters in the corps, K_J is the number of type J corps targets. Using this method, we can estimate how many targets will appear in a particular category during a confrontation with an enemy or armed forces that are expected to be the enemy. By creating a computer program based on the mathematical rule in formulas 1 and 2, entering into the program the country, the kind of troops and the number of units, we can set the target probabilities of troop units to different army standards (brigade, corps, army and above). This calculation can help us calculate all resources for target reconnaissance, planning and demolitions.

References

1. Turkish Armed Forces Joint Target Management MDK-3-9, Ankara: General Staff Press, 2012, 62s.

2. Target Intelligence Directive KKY 30-5, Ankara: Land Forces Printing House, 2014, 83s. NATO Target Reporting Categories URL: https://ncap.org.uk/feature/nato-target-reporting-categories.

3. Tactics, Techniques, and Procedures for Field Artillery Target Acquisition, Vaşinqton: Department of the Army, 2002, 192s.

4. The methods of organization and planning of operations in the provinces, the instruction. Baku: 2021. 118s.

5. Laurean-Georgel Oprean. Target Acquisition and Targeting In The Enemy's Depth//-Buxarest: Revista Academiei Forţelor Terestre, Military Art and Science – 2015. №4, – s.406-410.

COMPARATIVE ANALYSIS OF DRONE DETECTION METHODS TO PREVENT UNLAWFUL USE OF UAV

Khaligov G.S.
National Defense University, Baku, Azerbaijan

With the continuous development of technology, drone companies such as DJI, Parrot and 3Drobotics produce various types of unmanned aerial vehicles (UAV) or systems (PUS). Due to their availability and ease of use, UAVs are widely used. However, the wide and rapid spread of UAVs poses a threat when they are used in crimes. Therefore, to solve this problem, anti-drone systems are intensively developed, and the problem of drone detection becomes relevant [1].

In addition, we are witnessing the widespread use of UAVs in new generation wars. The enemy's use of reconnaissance drones led to the determination of the positions of the troops and, as a result, they came under attack [2].

Considering the above, it is necessary to analyze drone detection methods. The main purpose of the analysis is to select the optimal method to achieve the goal of the detection system.

Based on research, the main methods that can be used for UAV detection and classification tasks are radar, radio frequency (RF), acoustic sensors and camera systems [3, 4].

Radar-based drone detection. Since radar systems are mainly designed to detect high-velocity ballistic trajectory targets such as aircraft, military UAV and missiles, they are unsuitable for detecting small UAVs flying with low-velocity non-ballistic trajectories.

The high price and structural complexity of radar systems are other reasons that make important the creation of a relatively inexpensive drone detection system [1].

Drone detection based on acoustic systems.

Acoustic detection systems use acoustic sensors or microphones to recognize the sound waves of UAV rotors even in poor visibility. The maximum operating range of these systems is in the range of 200-250 m. Acoustic systems are generally resistant to environmental parameters, but their limited effective range makes them less unprofitable.

In addition, the sensitivity of these systems to environmental noise, especially in noisy high-altitude areas or urban and in windy conditions, affects the detection effect.

Drone detection based on radio frequency. This systems detect and classify drones based on their radio signals. A radio-based detection system is a passive listener between the UAV and its ground controller, and unlike radar-based systems, it does not transmit any signals. But some drones do not have radio transmission, s so this approach is not suitable for detecting autonomous UAVs without communication channels.

Video based drone detection. It is known that detection and recognition abilities are highest when the target is visible. In addition to drone detection, cameras

have the advantage of providing the drone's model, dimensions, and other information. However, detection with this method is not considered effective at night, in cloudy, foggy and dusty weather conditions. In such situations, a combination with thermal cameras can be used. Thermal cameras can solve the problem of detection at night and sometimes even work better in rain, snow and fog, depending on the technology used. It should also be noted that high-quality thermal cameras are used for military purposes, and low-cost commercial thermal cameras may fail in high-humidity weather or other adverse environmental conditions [1].

A good balance between cost and detection range is achieved by using visual drone detection technologies that use images of observation areas. One of the main drawbacks of visual drone detection is the high number of false detections caused by the visual similarity of different objects, especially when they occupy several pixels in the image.

As a result, systems can make mistake between a bird or background, and vice versa. The problem is further complicated by the large changes in images caused by changing weather and lighting conditions.

At the same time, drones can reach a speed of 160 km per hour, which places additional requirements on detection speed. To solve these problems, the "Drone and Bird" detection problem was created. The goal is to detect the drones seen in the video without any mistake.

With this method, the detection system works on the basis of computer vision algorithms. These artificial intelligence algorithms are trained in advance on the types of drones to be classified, and thanks to this, the video stream from the cameras performs the process of first detecting and then recognizing the flying object in real time.

Considering the structural simplicity, relatively high detection range, high classification ability and perspective development of computer vision algorithms, the system of detection of unmanned aerial vehicles based on video images obtained by video cameras is more useful.

References

1. Seidaliyeva, U., Akhmetov, D., LLipbayeva, L., Matson, E. (2020), "Real-Time and Accurate Drone Detection in a Video with a Static Background", No. 20, p.1-4.

2. Hashimov, E.G., Khudeynatov E.K. Evaluation of the effectiveness of the use of UAV systems in modern wars // - Baku: Military knowledge, - 2022. No. 1 (January-March), - p. 11-17.

3. Zhang, X., Kursini, K. (2021), "Autonomous long-range drone detection system for critical infrastructure safety", No. 80, p.23723-23727

4. Hashimov,EG, Maharramov, R.R. Methods of effective detection of unmanned aerial vehicles // Проблеми інформатизації. Тези доповідей 9- і міжнародної науково-технічної конференції. Том 1. -Черкаси – Харків-Баку – Бельсько-Бяла: 18 – 19 листопада**,** -2021, -с.118-119.

THE EFFECTIVENESS OF AIR DEFENSE SYSTEM

Hashimov E.G., Khudeynatov E.K.
The National Defense University, Baku, Azerbaijan

Effectiveness is the degree to which something can produce the desired outcome or result. It is a measure of how successful or efficient something is in achieving a specific goal or objective.

The effectiveness of a defense system refers to its ability to deter, defend against, and defeat threats to national security. Defense systems can include a wide range of interrelated components, such as military forces, intelligence agencies, other security agencies, and diplomatic and economic instruments of national power.

The effectiveness of an air defense system refers to its ability to detect, track, and engage airborne threats to protect friendly forces and critical infrastructure from aerial attacks.

Modern Air and Missile Defense (AMD) systems use radar paired with a gun or missile weapon system to detect and destroy an array of threat types that includes theater ballistic missiles (TBMs), cruise missiles (CMs), and unmanned aerial systems (UASs) [1,2]. The radar and other sensors are used to detect and track incoming threats, while the weapons are used to intercept and destroy them. The command-and-control system coordinates the activities of the various components of the air defense system, ensuring that they can operate effectively together.

One of the key factors that determine the efficiency of an air defense system is its ability to detect threats. This is typically done using radar, which can detect the presence of aircraft or missiles by detecting the electromagnetic signals they emit. The range and accuracy of the radar system are important factors in its ability to detect threats, as is its ability to differentiate between real threats and false targets.

Another factor that affects the efficiency of an air defense system is its ability to track threats once they have been detected. This is typically done using a combination of radar and other sensors, such as infrared cameras or laser rangefinders. The accuracy and speed of the tracking system are important factors in its ability to keep up with fast-moving threats, as is its ability to maintain a clear picture of the situation even in complex or cluttered environments.

There are several ways to improve the effectiveness of an air defense system:

1. Increase the number of sensors: Adding more sensors, such as radar or infrared detectors, can improve the coverage and detection range of the air defense system.

2. Enhance the capability of the sensors: Improving the sensitivity and resolution of the sensors can help to detect smaller, more stealthy targets at greater distances.

3. Increase the number and types of interceptors: Adding more interceptors, such as surface-to-air missiles or fighter jets, increases the likelihood of successfully intercepting incoming threats.

4. Improve the accuracy of the interceptors: Developing better guidance systems, such as those that use multiple sensors or advanced algorithms, can improve the accuracy and effectiveness of the interceptors.

5. Enhance the command-and-control system: Improving the communication and decision-making capabilities of the air defense system can help to coordinate the efforts of multiple interceptors and sensors.

6. Taking advantage of the capabilities of satellites: Satellites can be used to provide real-time or near-real-time surveillance and reconnaissance of large areas, allowing air defense systems to detect and track potential threats such as aircraft or missiles [3].

7. Integrate the system with other systems: Connecting the air defense system to other systems, such as air traffic control or intelligence networks, can provide additional information and enhance situational awareness.

8. Conduct regular training and exercises: Regular training and exercises can help to maintain the readiness and effectiveness of the air defense system.

Air defense systems must be designed and operated in a way that ensures the widest possible range, incorporates the latest technologies and cybersecurity protocols, and provides adequate resources to maintain readiness and effectiveness. Effective training and education programs, sound management practices, and a strategic approach to air defense planning can also help to mitigate common weaknesses in air defense systems.

To improve the effectiveness of an air defense system, it is important to assess its strengths and weaknesses, identify areas for improvement, and implement changes to address those areas. This may involve investing in new sensors and weapons, improving training and education programs for personnel, enhancing command and control systems, and strengthening partnerships with other countries and international organizations.

In addition, the effectiveness of an air defense system may also depend on the threat environment and the specific tactics and capabilities of potential adversaries. Thus, an air defense system needs to remain adaptable and responsive to changing threats and emerging technologies.

References

1. Brian Wade, Paul Chang, New Measures of Effectiveness for the Air and Missile Defense Simulation Community: [Electronic resource] – December, - 2015, URL: https://www.researchgate.net/publication/303640832_New_Measures_of_Effectiveness_for_the_Air_and_Missile_Defense_Simulation_Community

2. Hashimov, E.G., Khudeynatov E.K. Evaluation of the effectiveness of the use of UAV systems in modern wars // - Baku: Military knowledge, - 2022. No. 1 (January-March), - p. 11-17.

3. Joint Publication 3-14, Space operation: [Electronic resource] – April, - 2018, p-11, URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdf.

MATHEMATICAL METHOD OF CONVERTING GEOGRAPHICAL COORDINATES DETERMINED THROUGH UAV INTO A RECTANGULAR COORDINATE SYSTEM

Huseynov B.S.
National Defense University, Baku, Azerbaijan

Recent wars and military conflicts including Second Karabakh War and Russian-Ukrainian war have obviously proved that modern military operations vary from each-other with their number of features. So that, unusual strategies of running battles have been widely applied in both wars, the accuracy and targeting potentials of modern weapons have extensively been benefited, information confrontations have been mostly preferred, the planning of military operations has been computerized, state-of-art management and intelligence systems have been involved in order to fulfill this mission. In these wars mentioned above, if the application of regular piloted aviation was impossible and not expedient (the intense reflection of enemy air defense systems, radiation in the war zone, in case chemical and bacteriological weapons are used, in addition, if there is strong need to observe enemy troops for a while), aircrafts for exploratory purposes or armed aerial vehicles were widely used with the purpose of completing various tasks [1,2].

Despite the bravery and courage of Azerbaijan soldiers in The Second Karabakh War and Ukrainian militants in Russian-Ukrainian War, number of foreign commentators supported the idea of victory of modern technology in these wars. It is considered that, 1st time in the military history employing unmanned aerial vehicles in Second Karabakh War practically decided the destiny of the conflict. In this regard, the military specialists and experts of leading armies of the world still have been analyzing the results of this war, likewise in their discussion they earnestly advise to take some lessons from the consequences of these wars [3].

The analyzing of military operations involving unmanned aerial vehicles indicates these crafts are not only available for reconnaissance and striking, but also are used to direct high precision weapons and artillery fire.

The coordinates achieved through unmanned aerial vehicles and aviation systems are typically found in geographic coordinate system. In general units of the army while conducting measurements and calculation affairs on the map the rectangular coordination system is particularly helpful. In devices for artillery majority of reports are made in rectangular coordination system. Besides, this system is relatively basic for reports. Commonly regarding the features of task and demanding accuracy, objects on earth are located in different coordinate systems.

These coordinate systems are as follows: geograpich coordinate system; rectangular coordinate system; polar coordinate system; bipolar coordinate system [4, 5].

Practically, rectangular coordinate system is elaborated on the basis of Gaussian transverse cylindrical projection. Passing through once every 6 degrees meridians split earth surface into 6 sections.

Thereby, calculations are carried out according to 60 sections and th meridian "0" is accepted as "Greenwich".

Let's have a glipmse at how geographic coordinate system converts into rectangular coordinate system:

$\Psi = 40^0\ 21'\ 33''$ - geographic latitude (X in rectangular coordinate system).

$\lambda = 48^0\ 15'\ 30''$ - geographic longitude (Y in rectangular coordinate system).

The length of meridians are same everywhere. The length of 1^0 meridian are 40009 km : $360^0 \approx 111136$ m, the length of 1' meridian are 111136 : 60 ≈ 1852 m, the length of 1'' meridian arc 1852 : 60 ≈ 31 m/

As we mentioned Ψ- geographical latitude, is represented as X in rectangular coordinate system;

$\Psi = 40^0\ 21'\ 33''$

$40^0 = 40 \times 111136 = 4445440$

$21' = 21 \times 1852 = 38892$ $\qquad \Psi = (0^0 \div 90^0)$

$33'' = 33 \times 31 = 1023$

4485355

X = 4485355 - this point stands in the North 4485 km 355 m away from the equatorial line. Geographical latitude itself is shown as North and South latitudes.

The convertion of X into Ψ.

$X = 4485355 : 111136 = 40{,}35915454^0$ - 40 is the formula to find remainder.

Actual remainder 0,35915454 x 60 = 21,5492724 – 21 in order to find the remainder.

$0{,}5492724 \times 60 \approx 33''$. Out of here $\Psi = 40^0\ 21'\ 33''$

λ- geographic longitude – is represented as Y in rectangular coordinate system.

$\lambda = 48^0\ 15'\ 30''$. In the parallel 40^0 $\quad \lambda = (0^0 \div 180^0)$

1^0 – arc = 85400 m. $1'$ – arc = 1423 m. $1''$ – arc = 24 m.

$48^0 = 48 \times 85400 = 4099200$

$15' = 15 \times 1423 = 21345$

$30'' = 30 \times 24 = 720$

4121265

Y = 4121265, it indicates it is 4121265 m away from the meridian "Greenwich".

References

1. Hashimov E.G, Huseynov B.S. Development of the method of test firing with UAV in artillery units // Baku : Military knowledge - 2021. №3(july-december), -p.7-11.

2. Hashimov E.G.,Huseynov B.S "Some aspects of the combat capabilities and application of modern UAVs" // Baku : "National Security and military knowledges" - 2021. №3(7), -p.14-24.

3. NATO held an extraordinary secret meeting in Berlin to analyze the experience of the Azerbaijani army. The drone footages were extensively examined one by one. : [Electron resource] / - Baku, 29th december, the year of 2020. URL: https://bit.ly/39KY0p6.

4. Gasimov R. Coordinate systems used in military topography // Baku:, Military knowledge №3, 2014, p. 17-24.

5. Military topography // Baku: – 2020. 392 p.

STUDY OF THE 44 DAY CIVIL WAR

Ender Guner
National Defense University, Baku, Azerbaijan

The counter-offensive operation of the Armed Forces of the Republic of Azerbaijan, referred to as the "Second Karabakh War", "Homeland War", "44-Day War" or "Iron Fist" operation, opened a wide discussion to the researches and assumptions of local and international military-political researchers, is a bright example of the 21st century war in the South Caucasus [1-3].

Combat activities began on September 27, 2020 with a counter-offensive operation, were conducted for 44 days and ended with Victory on November 9. Information about the chronology of combat activities during the war, researches of military experts at the strategic level are widely available in open sources. The second Karabakh war attracted the attention of many foreign researchers and experts in terms of both the modernity of the technology used and the specificity of the combat tactics, even in some military institutions and organizations, various aspects of this war were investigated, and it was decided to teach the results in special military educational institutions. American military expert Mikhail Kofman emphasizes that the United States has determined the direction of investment in the armed forces in the future by studying many conflicts such as the 1973 Arab-Israeli war. As a result, the Russian-Ukrainian conflict and the Armenian-Azerbaijani war are also deeply analyzed. According to Gustav Gressel, Europe should begin absorbing military lessons from this war. The researcher claims that the armies of most European countries (with the exception of France and Germany) can fall into the same pitiable situation as the Armenian army in modern wars. Paul Iddon mentions that retrospective analysis may take several years, but in the end it will be clear that countries like Azerbaijan with small but advanced weapons systems should be taken seriously in modern warfare. Uzi Rubin highlights that this war created a momentary vision of the future battlefields where air defense systems and electronic warfare systems will dominate. According to the researcher, in this war, the Azerbaijani Armed Forces paralyzed the ground forces of the enemy by means of UAVs and ensured that their troops advanced and captured strategic positions. U. Rubin says that Israel should improve its HHM systems and fighter planes by drawing conclusions from this war [1,4].

After the ceasefire agreement was signed on May 12, 1994, the future activities of both sides of the Karabakh conflict (the Republic of Azerbaijan and the Republic of Armenia) were being planned. The President of the Republic of Azerbaijan, Commander-in-Chief of the Armed Forces, Mr. Ilham Aliyev, during an interview with the Russian media on September 24, 2021, said in response to a question about the planning of the "Iron Fist" operation: "Although it is in a state of frozen conflict, for all situations of life in a country at war the plan of conducting military operations, beyond doubt, was developed long ago. Unquestionably, changes were made to this plan from time to time, taking into account new realities, new capabilities of

Azerbaijan, including technological capabilities, and each time those changes were approved by me. This is natural. I also know that the Armenian side also had an action plan related to the war." [5].

As a result of the successful counter-offensive and offensive operations launched by the Azerbaijani Army in Karabakh on September 27, 2020, 5 cities, 4 settlements and 286 villages were liberated from occupation until November 9.

During the days starting from November 10, 2020 and lasting until the end of 2020, according to the "Statement of the President of the Republic of Azerbaijan, the Prime Minister of the Republic of Armenia and the President of the Russian Federation" during the liberation of the regions after the war, commanders and chiefs of all levels are reorganizing the troops and they carried out a large amount of work in the areas of ensuring the security of the service (especially on the transition from minefields), conducting anti-terrorist activities. Armenia withdrew its troops from Aghdam by November 20, Kalbajar by November 25, and Lachin by December 1. Peacekeeping in the region was entrusted to the Peacekeeping Forces of the Russian Federation. The Turkey-Russia Joint Monitoring Center monitors compliance with the ceasefire regime [2].

As a result of high-level planning and conducting of battle preparation and combat preparation measures, command-staff exercises, and training of personnel to operate in difficult terrain during the preparation phase of the Patriotic War, the Azerbaijani side was superior in the process of planning and execution of activities.

Although the defense was prepared and strengthened over a long period of time, the correct organization of the offensive activity gave its positive result. The use of high-tech means in the war made it possible to increase the pace of advancement of the Ground Forces.

The anti-terrorist operation, which started with a counter-attack, resulted in Victory due to deception, proper distribution of targets, proper organization of troops and fire control.

References

1. Piriev H.K., Hashimov E.G. Second Karabakh War: military-political and military-technical aspects // “Scientific Works” of the Military Institute named after Heydar Aliyev, 2023, Iss. 1 (40), p. 7-16

2. Piriev, H.K. Second Karabakh war. Military-political analysis / H.K. Piriyev, R.K. Tahirov, Kh.İ.. Iskanderov. - Baku: Military Publishing House, 2022. - 168 p.3.

3. Hashimov, E.G., Khudeynatov E.K. Evaluation of the effectiveness of the use of UAV systems in modern wars // - Baku: Military knowledge, - 2022. No. 1 (January-March), - p. 11-17.

4. Iskandarov, Kh., Gawliczek, P. Characteristic features of the second Karabakh War // Journal of Scientific Papers «Social Development and Security», 2021. 11(3), – p. 30-40.

5. President Ilham Aliyev's interview with the prestigious Russian magazine "Nasionalnaya oborona": [Electronic resource] / - 24.09.2021 URL: https://azertag.az/xeber/.

ESTIMATING METHODOLOGY OF A 5TDF ENGINE MOTOR RESOURCE CONSUMPTION UNDER DIFFERENT OPERATING MODES OF THE MACHINE

Chalapko V., Sirosh V., Moskalenko V.
Military Institute of Tank Troops of National Technical University, Kharkiv
Voitenko V., Melnyk I., Kolesnyk V.
Hetman Petro Sahaidachnyi National Army Academy, Lviv

The service life of a tank engine depends on the quality of diesel engine oil, timely maintenance, serviceability of the diesel engine fuel system and other internal combustion engine systems. Diesel units are also extremely sensitive to overheating, which requires constant monitoring of the cooling system. The engine life of an internal combustion engine depends on its design features, as well as individual operating conditions.

The **goal** of the study is to develop a method for estimating the consumption of engine life 5TDF engine in different modes of operation of the machine [1].

It was shown the possibility to make a conclusion about the nonlinear nature of the dependence of the engine life on time with different engine operation at different load modes.

Engine operating modes, which are determined by load resistance, are characterized by the number of revolutions of the engine crankshaft and the amount of power developed by the engine, largely determine its energy and economic performance of the engine and engine consumption [2, 3].

The testing ground for the consumption of the motor resource of the machine, depending on the readings of the engine hours counter, can be formed on the basis of the data obtained from the results of the operation of the machine in different conditions.

The analysis of the results of the research carried out that finding dependence of a 5TDF engine motor resource can be presented as the sum of two regressions – linear and hyperbolic. The readings of the engine hours counter will be recorded and further processed when the 5TDF engine is running in I-V and VI, VII gears, respectively. Such realization will make it possible to use the regression equation directly for the car crew.

References

1. Makogon H., Sirosh V., Guba S, Lavrut O., Zagrebelnuy S. and Rudiy A. (2022), Development of the estimating methodology of a 5TDF engine motor resource consumption under different operating modes of the machine. *Advanced Information Systems,* Vol. 6, No. 3. P. 45-51.

2. (1986), *Tank "Ural". Tekhnicheskoye opisaniye i instruktsiya po ekspluatatsii. (172 M)*, Kniga 2, Voyennoye izdatel'stvo, Moscow, SU.

3. (1986), Ob’yekt 447A (437A). *Tekhnicheskoye opisaniye i instruktsiya po ekspluatatsii*, Kniga 2, Voyennoye izdatel'stvo.

FIXED ZONE METHOD OF MILITARY GAME FOR RETROSPECTIVE ANALYSIS OF COMBAT EXPERIENCE

Isakov O., Vradii S., Babkin Yu., Bazeliuk V., Logvinenko O.
Military Institute of Tank Troops of National Technical University
"Kharkiv Polytechnic Institute", Kharkiv
Novik S.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv

The process of combat operations sustainment initiated and managed by the commander is at the same time a well-described, determined, defined process, and an art, which combines both the analytical work of the headquarters, comprehensive objective analysis and detailed calculation, as well as the subjective judgments of the commander (chief), which are based on his intuition, which, in turn, is a combination, a mixture of experience and intelligence (mind) and creativity [1].

To study and implement the experience of combat operations in terms of forming lessons, according to the authors, it is interesting to use the method of a fixed zone, which includes a detailed analysis of an important area of the terrain, direct contact with the enemy, and the boundary of forcing a water obstacle or a landing site.

Within the limits of this method, working out the planned table of interaction allows to analyze the experience of combat operations in coordination in time and space in relation to the actions of the enemy.

Determining the phases of the operation, the most probable actions of the enemy, and decision-making points for the military actions of the units makes it possible to form a lesson on the study of combat experience.

Conducting a military raffle with real initial data will provide an opportunity to form a lesson on the study of military experience based on a comparison of simulation results with real events [2, 3].

The technical implementation of this method **is proposed to** be carried out using computer graphics in the format of overlays.

References

1. Methodical recommendations for planning and organizing a battle according to NATO standards. Part II. [online]. − available at: https://sprotyvg7.com.ua/lesson/rekomendacii-z-planuvannya-ta-organizacii-boyu-za-standartami-nato-chastina-2.

2. (2022). *Doctrine of studying and implementing experience in the Armed Forces.* The Main Department of Doctrine and Training of the General Staff of the Armed Forces together with the Center for Operational Standards and Training Methods of the Armed Forces. 34p.

3. (2022) *Temporary instructions for the study and implementation of experience in the Armed Forces.* The Main Department of Doctrine and Training of the General Staff of the Armed Forces together with the Center for Operational Standards and Training Methods of the Armed Forces. 22p.

DEVELOPMENT OF MILITARY-TECHNICAL TRANSLATION SKILLS IN THE FIELD OF THE ARMORED WEAPONS AND MILITARY EQUIPMENT OPERATION

Vasyliev M., Yanishen A., Piskun S.
Military Institute of Tank Troops of National Technical University
"Kharkiv Polytechnic Institute", Kharkiv
Novik S.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv
Ryzhov Ye., Pashchetnyk O., Marchenko O.
Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine

The intensification of international defense cooperation measures can rightly be considered a factor in the evolution of military translation around the world. And the beginning of large-scale military operations highlighted the need for users to improve their military-technical and military-special translation skills, first of all, in conditions of access to special dictionaries and limited time for translation. Military discourse has a special communicative-functional orientation, it represents a combination of two functional language styles − official-business and scientific-technical ones − the priority of which changes depending on the topic of the document [1]. A distinctive feature of a military translation is greater terminology and an extremely accurate, clear presentation of the material with a relative absence of figurative and emotional means of expression. Military vocabulary is distinguished by its great variety and quantity. This is especially acute when processing operating instructions, repair manuals, logistics instructions, etc. [2]. To translate the instructions correctly, one need specialized knowledge and practical experience. For an adequate and high-quality translation, translators have to use highly specialized dictionaries, compile glossaries for each topic and expand electronic databases with new terms, access to which is limited in real conditions.

In this regard, the authors consider the issue of the development of military general educational skills necessary for comprehensive reading and the use of various types of transformations, which, in turn, will contribute to the basic concepts assimilation of the technical literature translation: the phenomenon of equivalence and ways of finding it, as well as the use of the obtained results in the translation of technical texts, namely texts in the field of the armored weapons and military equipment operation.

References

1. Struk I. V., Semyhinivska T. H., Sitko A. V. Formation and translation of military terminology / I. V. Struk, T. H. Semyhinivska, A. V. Sitko // Вчені записки Таврійського національного університету імені В. І. Вернадського, 2022. - Том 33 (72). - С. 29-33.
2. H. Grote und J. Feldhusen. Dubbel Taschenbuch fur den Maschinenbau: 22.Auflage K., 2007. 703S.

ADVANCING HEALTHCARE WITH GENERATIVE AI: CURRENT AND FUTURE RESEARCH

Hlavcheva D.
KeenEthics LLC, Lviv, Ukraine
Podorozhniak A.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

In 2022, AI platforms such as ChatGPT, DallE, Synthesia, and Chatsonic revolutionized the AI industry and became the most talked-about topic in IT innovation. However, the groundwork for these incredible advancements was laid through years of research [1]. Today, researchers continue to explore the potential of generative AI in various fields, including education, logistics, e-commerce, and healthcare, which is considered one of the most intriguing and controversial areas for the application of generative AI.

The healthcare industry is increasingly recognizing the significance of AI-powered tools in the next wave of healthcare technology. AI is considered to have the potential to enhance various aspects of healthcare operations and delivery. Notably, cost reduction is a significant motivator for the implementation of AI applications within the healthcare system [2].

The conventional AI approach of using Convolutional Neural Networks for medical image analysis [3, 4] has had a significant impact on healthcare processes and operations.

However, recent research trends indicate that Generative Adversarial-Based Networks will be the next generation of AI technologies in the industry.

The purpose of this report is to provide an overview of significant trends in the application of generative AI to healthcare industry problems, including medical chatbots, precision medicine, virtual nursing assistance, and medical imaging. The report aims to present a comprehensive analysis of research conducted in the past six months, along with ideas for future directions of generative AI applications.

References

1. Cao Y. et al. A Comprehensive Survey of AI-Generated Content (AIGC): A History of Generative AI from GAN to ChatGPT // arXiv preprint arXiv:2303.04226. – 2023. https://doi.org/10.48550/arXiv.2303.04226.

2. Bohr A., Memarzadeh K. The rise of artificial intelligence in healthcare applications // Artificial Intelligence in healthcare. – Academic Press, 2020. – pp. 25-60. https://doi.org/10.1016/B978-0-12-818438-7.00002-2.

3. Hlavcheva D. et al. Comparison of CNNs for lung biopsy images classification // 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON). – IEEE, 2021. – pp. 1-5. https://doi.org/10.1109/UKRCON53503.2021.9575305.

4. Hlavcheva D., Yaloveha V., Podorozhniak A. Application of convolutional neural network for histopathological analysis // Advanced Information Systems. – 2019. – Vol. 3. – №. 4. – pp. 69-73. https://doi.org/10.20998/2522-9052.2019.4.10.

TRANSFER LEARNING TECHNIQUE APPLIED TO MULTISPECTRAL IMAGES CLASSIFICATION PROBLEM

Yaloveha V., Podorozhniak A.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

In recent years deep learning approaches are effectively used in a wide range of applications. Among various models and methods Convolutional neural networks (CNNs) show high performance for image classification tasks and object detection [1, 2]. Scientists have introduced a pretrained set of different convolutional neural networks that successfully were applied in multiple fields of study. As it is known deep neural network models must be trained with a huge number of parameters that requires a lot of computational resources in pair with a big amount of training time. The transfer learning technique is used for repurposing a model trained on one task to a comparable task that requires some adaptation. Transfer learning enables model parameters to start with good initial values that only need minimal tweaks to be better curated for the new problem [3].

The VGG-16 is a state of art convolutional neural network that has been used for image classification issues since 2014. ResNet includes a skip connection, which transfers the inputs of the previous layer to the next layer. Such a property makes the neural network lighter. The Xception neural network architecture consists of separable convolution layers.

The idea behind the DenseNet is based on direct connections between any two layers of a convolutional neural network with the same feature-map size. EfficientNetV2 was announced in 2021. This model represents a new family of smaller and faster neural networks.

The purpose of the report is to research multiple pretrained convolutional neural network families to serve as baseline models for the remote sensing dataset benchmarking.

In [4] it was shown that calculating spectral indexes based on given bands improves overall model performance metrics. So in addition, we evaluated spectral bands and their combinations.

References

1. Benhammou Y. et al. Sentinel2GlobalLULC: A Sentinel-2 RGB image tile dataset for global land use/cover mapping with deep learning, Scientific Data, 2022, vol. 9, no. 1, pp. 1-20.
2. Kuchuk H. et al. System of license plate recognition considering large camera shooting angles, Radioelectronic and computer systems, 2021, no. 4, p. 82-91.
3. Yogapriya J. et al. Gastrointestinal tract disease classification from wireless endoscopy images using pretrained deep learning model, Computational and mathematical methods in medicine, 2021, vol. 2021, article ID 5940433.
4. Yaloveha V., Podorozhniak A., Kuchuk H. Convolutional neural network hyperparameter optimization applied to land cover classification, Radioelectronic and computer systems, 2022, no. 1, p. 115-128.

DYNAMIC CHANGE IN THE DIMENSION OF THE CURRENT POPULATION USING GENETIC ALGORITHMS

Skakalina O.
National University «Yuriy Kondratyuk Poltava Polytechnic», Poltava, Ukraine

Genetic algorithms (GA) are designed to solve optimization and modeling problems by successively selecting, combining and changing desired parameters using mechanisms reminiscent of biological evolution. There are a large number of ways to encode individuals, as well as operators of mutation, crossover, selection, selection, and, finally, niche and constraint methods. This shows that an extremely wide variety of genetic algorithms can be proposed, differing in coding methods, structure, genetic operators used, and generally accepted GA parameters.

The main parameters of genetic algorithms include: the dimension of the initial and current populations, the criteria for stopping the operation of the genetic algorithm, the analytical expression of the so-called fitness function, which is an external criterion for assessing the degree of optimality of the resulting solution [1].

The purpose of the report is study of the influence of dynamic change in the dimension of the current population on the quality of the obtained quasi-optimal solution using hybrid genetic algorithms in solving practical problems from subject areas.

The report contains the results of constructing an optimal general seasonal plan for the transportation of large national agricultural holdings [2], a modification of the well-known computer game

The Heroes of Might and Magic 3 (HoMM3) [3] was developed by embedding a genetic algorithm into the game in order to achieve the preservation of the game balance, finding simple winning strategies or conditions under which winning is impossible in principle are sufficient. For the HoMM3 game, a new crossover operator was also constructed with the ability to ignore the null substring of a binary coded individual.

The presented results demonstrate the ability of genetic algorithms to find acceptable solutions in an acceptable time for many classes NP - complex problems that cannot be solved in an acceptable time by any other methods except heuristics.

References

1. Bhandari D, Murthy C A and Pal S K 2012 Variance as a Stopping Criterion for Genetic Algorithms with Elitist Model [Text] *Fundamenta Informaticae* vol 120 pp 145–164. doi:10.3233/FI-2012-754.

2. Skakalina E 2018 Development of Methodological Foundations of Logistical Intellectual Control of Complex Systems Based on Hybrid Heuristic Algorithms *International Journal of Engineering & Technology v*ol 7 No 4.8 pp 534-538. DOI: 10.14419/ijet.v7i4.8.27301

3. https://store.steampowered.com/app/297000/Heroes_of_Might__Magic_III__HD_Edition

APPLICATION OF EXPERT ASSESSMENT METHODS IN CONSTRUCTION MODELS OF THE QUALITY OF ARTIFICIAL INTELLIGENCE SYSTEMS

Feoktystova O.I., Zmiivskyi V.S.
National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine

Scientific and technical progress is accompanied by the continuous complication of decision-making objects, which at one time led to problems with the creation of adequate analytical models of the behavior of such objects and, as a result, to the increasingly widespread use of artificial intelligence systems in the informatization of processes in many areas of human life.

At the same time, the complexity of the relevant artificial intelligence systems is also constantly increasing, which determines the urgency of the problem of providing "explainable intelligence".

An effective way to solve the mentioned problem is the use of special models for evaluating the quality of artificial intelligence systems, in particular, by analyzing the non-functional characteristics of such systems.

The authors of the work [1] proposed the initial (conceptual) model of the quality of artificial intelligence, as well as the methodology for construction a basic model based on it.

In addition, this work presents a development methodology based on the basic-applied quality model for a specific artificial intelligence systems. In specified methods involve the involvement of experts to determine the importance of certain quality characteristics and their mutual influence.

The report presents an option for improving the technology of construction basic and applied quality models of the artificial intelligence system, which involves:

forming a team of experts (expert commission);

obtaining a generalized expert assessment of the importance of including specific characteristics of the quality of artificial intelligence in the composition of the model;

increasing the level of consistency of expert testimony;

combining expert opinions to achieve a conjunctive consensus between the assessments of individual experts [2].

References

1. Kharchenko V.S., Fesenko H.V., Illiashenko O.O. Bazova model nefunktsiinykh kharakterystyk dlia otsinky yakosti shtuchnoho intelektu // Radioelectronic and Computer Systems. – 2022/ - vol. 2. P. 131-144. DOI: 10.32620/reks.2021.4.07.

2. Shostak O.I. Rozrobka pidkhodu do formuvannia ekspertnykh komisii shchodo otsiniuvannia skladu komand vykonavtsiv vysokotekhnolohichnykh proektiv // Tekhnolohycheskyi audyt y rezervy proyzvodstva. – 2016. – № 4/2 (30). – S. 20-25.

WAYS TO IMPROVE THE SOFTWARE OF TRUCK TRANSPORT MANAGEMENT SYSTEMS

Shulga I.M., Feoktystov S.O.
National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine

In the modern world, the organization of logistics processes plays a decisive role in practically all areas of social life.

Among these processes, the most im-portant are those related to the transportation of various goods by road, air, sea, and rail transport. In general, the efficiency of the organization of transport logistics depends on the solution of a set of tasks related to the de-termination of rational routes, the type of vehicles, customs clearance (in the case of international transportation) [1].

Existing computer systems focused on the automation of transport logistics processes have the form of ready-made environments, based on which appropriate software applications are created [2].

At the same time, the specified development environments, regardless of whether they are commercial products or belong to proprietary software, do not have in their composition means that could reflect the specifics of the implementation of specific cargo delivery tasks in the conditions of the current realities in Ukraine and its partner countries on countering aggression. A vivid example of such a task is the construction of a transport logistics chain for the delivery of weapons, ammunition and military equipment from military bases located on the territory of the USA to Ukraine.

The purpose of the report is to discuss ways to improve software systems focused on the automation of cargo transportation processes by expanding the functionality of these systems and improving the usability of their interface. The theory of software agents, ontological engineering and interactive cognitive graphics are the methodological basis for the modernization of such systems.

The implementation of the mentioned innovations in the computer means of organizing transportation will make it possible to increase the efficiency of logistics systems in the following aspects: reducing the risk of making irrational decisions, due to the reduction of the number of alternative logistics chains, and improving the ergonomics of the interface of the logistician-dispatcher, who in this case acts as the person making the decision.

References

1. Geronimus B. A. Ekonomiko-matematicheskiye metody v planirovanii na avtomobilnom transporte / B.A. Geronimus . – M. : Transport. 2002. – 240 s.

2. Perebiinis V.I. Transportno-lohistychni systemy pidpryiemstv: formuvannia ta funktsionuvannia : monohrafiia / V.I. Perebiinis, O.V. Perebiinis. – Poltava : RVV PUSKU, 2005. – 207 s.

ПОЯСНИЙ МЕТОД ВІЙСЬКОВОГО РОЗІГРАШУ ДЛЯ РЕТРОСПЕКТИВНОГО АНАЛІЗУ ДОСВІДУ БОЙОВИХ ДІЙ

Ковальов І.О., Білоус О.В., Хліманцов Т.В., Дяченко Д.В., Мосійчук М.В.
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна
Лаврут О.О., Заболотнюк В.І.
Національна академія сухопутних військ ім. гетьмана Петра Сагайдачного, Львів, Україна

Ініційований та керований командиром (начальником) процес всебічного забезпечення бою є водночас й добре описаним, обумовленим, визначеним процесом, і мистецтвом, де поєднуються як аналітична робота штабу, всебічний об'єктивний аналіз і детальний розрахунок, так і суб'єктивні судження командира (начальника), що ґрунтуються на його інтуїції, яка, у свою чергу, є комбінацією, сумішшю досвіду та інтелекту (розуму) і творчості [1]. На ефективність всебічного забезпечення бою впливають такі фактори:

обсяг наявної інформації, яку необхідно обробити;

наявний час для проведення планування;

якість керівних вказівок з планування операції тощо.

Для вивчення та впровадження досвіду бойових дій у розрізі формування уроків, на думку авторів, цікавим вбачається використання методу поясів *(belt*).

Пояси повинні включати розіграш дій по всьому фронту та на всю глибину виконання завдання в межах тактичного епізоду (вихідний район, вихідний рубіж форсування, рубежі розгортання, рубіж переходу в атаку); введення резерву / здійснення контратаки; захоплення об'єкта / ураження противника.

Проведення військового розіграшу із реальними вихідними даними надасть можливість сформувати урок вивчення військового досвіду на основі порівнянні результатів моделювання із реальними подіями [2,3].

Технічну реалізацію цього методу пропонується здійснити із використанням комп'ютерної графіки у форматі overlays.

Список літератури

1. Методичні рекомендації з планування та організації бою за стандартами НАТО [on-line]. – Режим доступу: https://sprotyvg7.com.ua/lesson/rekomendacii-z-planuvannya-ta-organizacii-boyu-za-standartami-nato-chastina-2

2. Доктрина з вивчення та впровадження досвіду у ЗСУ. − Головне управління доктрин та підготовки ГШ ЗСУ спільно з центром оперативних стандартів і методики підготовки ЗСУ, 2022. – 34с.

3. Тимчасова інструкція вивчення та впровадження досвіду у ЗСУ. − Головне управління доктрин та підготовки ГШ ЗСУ спільно з центром оперативних стандартів і методики підготовки ЗСУ, 2022. – 22 с.

ВИВЧЕННЯ І ВПРОВАДЖЕННЯ ДОСВІДУ БОЙОВИХ ДІЙ ЗА ОПЕРАТИВНИМИ СТАНДАРТАМИ НАТО

Серпухов О.В., Макогон О.А., Маєр Л.В., Клімов О.П., Акіншин О.Г.
Військовий інститут танкових військ Національного технічного університету "Харківський політехнічний інститут", Харків, Україна
Лаврут Т.В.
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна

Елементи методології будівництва структури збройних сил, планування, підготовки та управління військами у ході військових операцій прийнято називати оперативними стандартами НАТО. У даній роботі розглядається можливість використання для вивчення та впровадження досвіду бойових дій методів, традиційно рекомендованих для військового розіграшу: поясів (*belt*), проходження в глибину (*avenue-in-depth*) та фіксованої зони (*box*).

Для опису бойового досвіду пропонується використовувати методи планової таблиці взаємодії та фіксації подій окремого тактичного епізоду. Ефективність вибудування бойового порядку у цьому випадку аналізується шляхом синхронізації дій у часі. Уроки з вивчення досвіду формуються на основі таблиць аналізу варіантів дій – прийнятого та альтернативного рішення. Як відомо, метод фіксації подій являє собою короткі замітки щодо наміру командира, положення підрозділів та їх завдань.

Командир та штаб наносять положення підрозділів на робочій карті, робочій таблиці, дошці (*white board*) [1].

В проекції вивчення і впровадження досвіду бойових дій сутність такої фіксація подій дає можливість "розкадрування" тактичного епізоду та аналізу поставлених завдань, очікуваних та реальних дії та протидії противника, відповіді на протидії противника, необхідних та наявних сил й засоби для цього, необхідного та реального часу для ефективного виконання завдання, тощо [2, 3].

Список літератури

1. Методичні рекомендації з планування та організації бою за стандартами НАТО [on-line]. – Режим доступу: https://sprotyvg7.com.ua/lesson/rekomendacii-z-planuvannya-ta-organizacii-boyu-za-standartami-nato-chastina-2

2. Доктрина з вивчення та впровадження досвіду у ЗСУ. − Головне управління доктрин та підготовки ГШ ЗСУ спільно з центром оперативних стандартів і методики підготовки ЗСУ, 2022. – 34 с.

3. Тимчасова інструкція вивчення та впровадження досвіду у ЗСУ. − Головне управління доктрин та підготовки ГШ ЗСУ спільно з центром оперативних стандартів і методики підготовки ЗСУ, 2022. – 22 с.

ПРОГНОЗУВАННЯ ТЕХНІЧНОГО СТАНУ РАДІОТЕХНІЧНИХ ЗАСОБІВ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ПРИ ВИКОНАННІ ЗАВДАНЬ ЗА ПРИЗНАЧЕННЯМ В ОСОБЛИВИХ УМОВАХ

Крючков Д.М., Скорик А.Б., Моргун Є.В., Титаренко Р.В.
Харківський національний університет Повітряних Сил, Харків, Україна

Встановлено, що в особливих умовах суттєвий вплив на планування застосування та на результати виконання завдань за призначенням радіотехнічних засобів спеціального призначення має технічний стан об'єктів експлуатації. Висока точність прогнозування технічного стану дозволяє розробляти довгострокові плани експлуатації засобів з мінімізацією експлуатаційних розходів, тобто підвищувати її ефективність. Разом з тим встановлено, що більшість існуючих методів прогнозування [1-3] не враховують особливих умов експлуатації засобів та виникаючих з цього приводу пошкоджень, що суттєво знижує їх достовірність та збільшує терміни відновлення.

Метою доповіді є обґрунтування пропозицій щодо удосконалення прогнозування технічного стану радіотехнічних засобів спеціального призначення при виконанні завдань за призначенням в особливих умовах.

У доповіді приведені результати аналізу можливих вражаючих факторів, що виникають при виконанні спеціальними радіотехнічними засобами завдань за призначенням в особливих умовах, та статистичні характеристики можливих ушкоджень.

Отримані результати дозволяють розробити пропозиції щодо комплектації ремонтних. В припущенні комплектації ремонтних комплектів ЗІП з урахуванням наведених пропозицій запропонований статистичний метод прогнозування технічного стану спеціальних радіотехнічних засобів при їх експлуатації в особливих умовах.

Список літератури

1. Герасимов С.В., Гречка А.В., Рощупкин Е.С., Рощупкина А.Е., Кукобко С.В. (2020). Адаптивный метод технической диагностики системы разнесенных радиотехнических устройств. Azərbaycan dövlət dəniz akademiyasının elmi əsərləri (ISSN 2220-1025), 2, 129–137. https://doi.org/10.5281/zenodo.5035853.

2. Туринский А.В., Певцов Г.В., Крючков Д.Н., Рощупкин Е.С. (2020). Методы повышения достоверности и эффективности контроля технического состояния радиотехнических систем подвижных объектов. Azərbaycan dövlət dəniz akademiyasının elmi əsərləri (ISSN 2220-1025), 1, 176–182. https://doi.org/10.5281/zenodo.5035847.

3. 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, iss. 8, 2020, p.p. 4502-4507, https://doi.org/10.30534/ijeter/2020/74882020.

ПРОПОЗИЦІЇ ЩОДО ПІДВИЩЕННЯ МОЖЛИВОСТЕЙ РАДІОТЕХНІЧНОГО ЗАСОБУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ПО ВИЯВЛЕННЮ ТА СУПРОВОДЖЕННЮ БАЛІСТИЧНИХ ЦІЛЕЙ

Кісіль О.А., Романюк М.М., Коробков Ю.В.
Харківський національний університет Повітряних Сил, Харків, Україна
Кукобко С.В.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Чернигів, Україна

Встановлено, що балістичні засоби нападу застосовуються для руйнування критично важливих об’єктів держави, що підриває її економічну, промислову та соціальну міць та має метою примушення до капітуляції внаслі-док виникнення важких умов для супротиву.

У доповіді за результатами аналізу відкритих джерел наведені результати впливу балістичних засобів нападу на об’єкти критичної інфраструктури України та наведені прогнози можливих наслідків у майбутньому.

Ефективним способом боротьби з балістичними цілями є їх знищення у повітрі та нейтралізація їх носіїв з використанням радіотехнічних засобів спеціального призначення [1-3].

За результатами аналізу існуючих засобів протидії балістичним цілям з’ясовані проблемні питання, розв’язання яких потребує ефективна боротьба с балістичними засобами нападу.

Наведені пропозиції щодо підвищення можливостей радіотехнічного засобу спеціального призначення по виявленню та супроводженню балістичних цілей, сутність яких полягає в удосконаленні способів обробки перевідбитих сигналів, що є одним з ефективних шляхів за критерієм "ефективність-вартість" та не потребує суттєвої переробки існуючих засобів.

Метою доповіді є доведення до широкої міжнародної наукової спільноти результатів проведених досліджень та їх обговорення.

Список літератури

1. 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.

2. Великоапертурна (рознесена) радіолокаційна система: пат. 148518 Україна : G01S7/42, H01Q21/00 / Є.С. Рощупкін, С.В. Герасимов та інш.. – u 202100336; заявл. 29.01.2021; опубл. 18.08.2021, бюл. № 33/2021, – 7 с. https://iprop-ua.com/inv/qnptergc.

3. Крючков Д.М., Рощупкін Є.С., Титаренко Р.В., & Шулежко В.В. (2019). Шляхи підвищення можливостей засобів протиповітряної оборони при роботі з об'єктами, що рухаються по балістичній траєкторії. Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів, 104-105. https://doi.org/10.5281/zenodo.5651545.

ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ РОБОТИ СИСТЕМ РАДІОТЕХНІЧНОГО ЗАСОБУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З СИГНАЛАМИ РІЗНИХ ТИПІВ, ПРИ ПЕРЕХОДІ З РЕЖИМУ У РЕЖИМ ТА ЗМІНІ ТИПІВ СИГНАЛІВ

Марченко Б.С., Джус В.В., Сургай М.В., Борисов В.В.
Харківський національний університет Повітряних Сил, Харків, Україна

Встановлено, що функціонування радіотехнічних засобів спеціального призначення в різних режимах роботи суттєво залежить від синхронної роботи його складових систем [1-4].

У доповіді приведені результати аналізу впливу нестабільності роботи системи синхронізації на виконання завдань за призначенням радіотехнічних засобів.

Встановлено, що виникаюча при цьому неузгодженість спрацювання окремих систем призводить к суттєвому зниженню потенційних можливостей виробу спеціального призначення, зростанню потрібного часу і, в деяких випадках, зриву виконання поставленого завдання.

Із аналізу особливостей побудови та функціонування системи синхронізації спеціального радіотехнічного засобу встановлено, що нестабільність видачі нею імпульсів (стробів) та флуктуація їх рівнів насамперед пов'язані з застарілою елементною базою.

В зв'язку з наведеним запропоновано викори-стання побудованої на сучасній елементній базі системи на заміну існуючої.

Метою доповіді є доведення до широкої міжнародної наукової спільноти результатів проведених досліджень, пропозицій щодо розв'язання пору-шених проблемних питань та їх обговорення.

Список літератури

1. 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.

2. Dzhus, V., Roshchupkin, Y., Kukobko, S., Herasymov, S., Drob, N., & Trofymova, M. Estimation of noise radiance point sources multichannel direction finding systems resolution by linear prediction method. Sistemi obrobki informacії. 2021. № 4(167). С. 19-26. https://doi.org/10.30748/soi.2021.167.02.

3. Герасимов С.В. Підвищення боєготовності зенітних ракетних військ шляхом оптимальної закупівлі комплектуючих виробів ЗРК / С.В. Герасимов, Д.М. Ізосімов, Є.С. Рощупкін, В.В. Старцев // Системи озброєння і військова техніка. – 2010. – № 1(21). – С. 55-59. http://nbuv.gov.ua/UJRN/soivt_2010_1_13.

Artikula, A., Britov, D., Dzhus, V., Haibadulov, B., Haibadulova, A., Herasymov, S., Kaluhin, D., Kukobko, S., Roshchupkin, Y., & Tytarenko, R. (2021). Measurement errors affecting the characteristics of multi-position systems, and ways to reduce them. InterConf, 333-346. https://doi.org/10.51582/interconf.7-8.06.2021.035.

АНАЛІЗ ФАКТОРІВ, ЩО ВПЛИВАЮТЬ НА ПІДГОТОВКУ ДО ЗАСТОСУВАННЯ ВІЙСЬКОВИХ ЧАСТИН (ПІДРОЗДІЛІВ) ЗЕНІТНИХ РАКЕТНИХ ВІЙСЬК

Помогаєв І.В., Ткачук О.А., Резніченко О.А., Молчанов Д.В., Васильєва Н.М.
Харківський національний університет Повітряних Сил, Харків, Україна

Встановлено, що на підготовку до застосування зенітних ракетних військ (ЗРВ) впливають: рівень навченості особового складу (о/с) військових частин (в/ч) і підрозділів, злагодження органів управління (штабів) тактично-го рівня, в/ч (підрозділів) з метою досягнення їх готовності до виконання за-вдань за призначенням в будь-який час.

Підвищення рівня цих факторів досягається шляхом підтриманням та підвищенням рівня навченості о/с, його психологічної готовності до виконання завдань, злагодженості в/ч (підрозділів, кораблів) та набуттям ними визначених бойових спроможностей [1-3].

У доповіді розглядається підготовка підрозділів забезпечення, а саме порядок організації та проведення тактико-спеціальних навчань (ТСН). Наведено, що при проведенні ТСН підвищується злагодженість в/ч (підрозділів) логістичного забезпечення під час підготовки і бойових (спеціальних) дій, перевірки готовності до виконання завдань за призначенням. Розглянутий порядок оцінювання ефективності ТСН з підрозділами ЗРВ.

Метою доповіді є розгляд та обґрунтування пропозиції щодо удосконалення (підвищення ефективності) організації та проведення ТСН з підрозділами забезпечення, що безпосередньо впливає на рівень підготовки до застосування в/ч ЗРВ.

Список літератури

1. Джус В, Шулежко В, Рощупкін Є, Гречка О, & Сургай М. (2020). Особливості організації та проведення практик курсантів факультету зенітних ракетних військ, Освітній процес: методика, досвід, проблеми, 3-4 (157-158), 70–74. https://doi.org/10.5281/zenodo.6618969.

2. Резніченко, О., Шулежко, В., Удовенко, А., Рощупкін, Є., Крючков, Д., & Титаренко, Р. (2021). Досвід активізації та мотивації навчально-пізнавальної діяльності курсантів при підготовці фахівців " в умовах карантинних обмежень. Освітній процес: методика, досвід, проблеми, 3-4 (161-162), 61–69. https://doi.org/10.5281/zenodo.7273873.

3. Ткачук, О.А., Рощупкін, Є.С., Помогаєв, І.В., Калита, О.В., & Крючков, Д.М. (2022, November 22). Особливості фізичної підготовки військовослужбовців частин (підрозділів) зенітних ракетних військ у процесі відпрацювання питань відновлення озброєння та військової техніки на тактичних (тактико-спеціальних) заняттях. VI Міжнародна науково-практична конференція "Сучасні тенденції та перспективи розвитку фізичної підготовки та спорту Збройних Сил України, правоохоронних органів, рятувальних та інших спеціальних служб на шляху євроатлантичної інтеграції України", Київ. https://doi.org/10.5281/zenodo.7501178.

АНАЛІЗ ФАКТОРІВ, ЩО ВПЛИВАЮТЬ НА ЕФЕКТИВНІСТЬ ВІДНОВЛЕННЯ РІЗНОТИПНИХ РАДІОТЕХНІЧНИХ ЗАСОБІВ СКЛАДНОЇ СИСТЕМИ ПІД ЧАС ВИКОНАННЯ ЗАВДАНЬ ЗА ПРИЗНАЧЕННЯМ В ЕКСТРЕМАЛЬНИХ УМОВАХ

Рощупкін Є.С., Гречка О.В., Галицький О.Ф., Гайбадулов Б.В.
Харківський національний університет Повітряних Сил, Харків, Україна

Встановлено, що під відновленням радіотехнічних засобів розуміють комплекс взаємопов'язаних заходів з управління, технічної розвідки, евакуація, ремонту та поповнення.

Таким чином, зменшення термінів проведення та (або) витрат на виконання усього комплексу або окремих його складових призводить до підвищення ефективності відновлення, під яким будемо розуміти співвідношення витрат відповідних ресурсів при реалізації заходу до отриманого результату відновлення.

У доповіді наведені результати аналізу можливих витрат ресурсів при реалізації кожного з заходів. Встановлено, що одним з ефективних шляхів максимізації вихідного ефекту є вдосконалення технічної розвідки та ремонту радіотехнічних засобів з застосуванням сучасної вимірювальної апаратури та методів технічної діагностики [1-4].

Запропоновано використання уніфікованої контрольно-вимірювальної апаратури та методики пошуку несправностей системи різнотипних радіотехнічних засобів при її функціонуванні в особових умовах.

Метою доповіді є доведення отриманих в результаті проведених досліджень результатів, обговорення їх та подальших напрямків досліджень.

Список літератури

1. Герасимов С.В. Теоретические основы оценки ошибок значений сигналов с гармонически меняющимися параметрами / С.В. Герасимов, Е.С. Рощупкин // Озброєння та військова техніка. – 2018. – № 2. – С. 43-49. http://nbuv.gov.ua/UJRN/ovt_2018_2_9.

2. Герасимов С.В. Синтез вимірювальних сигналів для визначення технічного стану систем автоматичного управління / С.В. Герасимов, С.В. Кукобко, Є.С. Рощупкін, О.О. Расстригін // Озброєння та військова техніка. – 2016. – № 4. – С. 32-36. http://nbuv.gov.ua/UJRN/ovt_2016_4_7.

3. Herasimov, S., Borysenko, M., Roshchupkin, E. et al. Spectrum Analyzer Based on a Dynamic Filter. J Electron Test 37, 357–368 (2021), https://doi.org/10.1007/s10836-021-05954-0.

4. Борисенко М.В. Визначення оптимального переліку засобів вимірювальної техніки в складі контрольно-перевірочної апаратури зенітного ракетного озброєння / М.В. Борисенко, А.П. Волобуєв, Є.С. Рощупкін // Системи озброєння і військова техніка. – 2011. – № 2(26). – С. 114-116. – Режим доступу: http://nbuv.gov.ua/UJRN/soivt_2011_2_27.

МЕТОД ЗНИЖЕННЯ РІВНЯ ВИСОКОЧАСТОТНИХ СКЛАДОВИХ ЕЛЕКТРИЧНИХ СИГНАЛІВ СИСТЕМ УПРАВЛІННЯ

Герасимов С.В.
Національний технічний університет «ХПІ», Харків, Україна
Сорока В.В.
Державний університет інфраструктури та технологій, Київ, Україна

Надійність роботи електричних схем комп'ютерної техніки і мікроелектроніки залежить від форма електричних сигналів. Тому потрібно контролювати реальну форму електричних сигналів для забезпечення безаварійної роботи систем управління різними технічними об’єктами або технологічними процесами [1].

Форма електричних сигналів залежить від високочастотних складових: чим їх менше, тим менше завад налічую сигнал [2].

При синтезі електричних сигналів із потрібним складом високочастотних складових застосовується три методи:

мінімізація спектру гармонійного сигналу,

виділення та видалення періодичного сигналу довільної форми з високочастотними складовими,

проведення інтегрування певної кількості високочастотних сигналів із необхідним співвідношенням частот [3].

У доповіді наведено результати розробки методу зниження рівня високочастотних складових електричних сигналів систем управління. Розроблений метод заснований на формуванні цифрової форми синусоїдального сигналу. Суть методу полягає у поданні вихідного синусоїдального сигналу ступінчастою апроксимацією.

Поліпшення технічних характеристик генератора електричних сигналів за діапазоном зміни високочастотних складових і гармонійного складу досягається заміною синусоїдального сигналу ступінчастим.

Запропоновані співвідношення для визначення високочастотних скла-дових синтезованого ступінчастого сигналу та оцінювання взаємозв'язку між параметрами такого сигналу та параметрами сходинок.

Список літератури

1. Герасимов С.В., Рощупкин Е.С. Теоретические основы оценки ошибок значений сигналов с гармонически меняющимися параметрами. *Озброєння та військова техніка*. 2018. № 2. С. 43-49. http://nbuv.gov.ua/UJRN/ovt_2018_2_9.

2. Герасимов С.В. Синтез вимірювальних сигналів для визначення технічного стану систем автоматичного управління / С.В. Герасимов, С.В. Кукобко, Є.С. Рощупкін, О.О. Расстригін // Озброєння та військова техніка. – 2016. – № 4. – С. 32-36. http://nbuv.gov.ua/UJRN/ovt_2016_4_7.

3. Herasimov, S., Borysenko, M., Roshchupkin, E. et al. Spectrum Analyzer Based on a Dynamic Filter. J Electron Test 37, 357–368 (2021), https://doi.org/10.1007/s10836-021-05954-0.

ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ВИЯВЛЕННЯ ТА СУПРОВОДЖЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ РАДІОТЕХНІЧНИМ ЗАСОБОМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Швидкий А.В., Чміль Ю.О., Шулежко В.В., Гордієнко Р.О.
Харківський національний університет Повітряних Сил, Харків, Україна

Встановлено, що можливості сучасних безпілотних літальних апаратів (БПЛА), їх мала ефективна поверхня розсіювання (ЕПР) та рух на малих висотах з низькою швидкістю викликали необхідність підвищення спроможностей існуючих радіотехнічних засобів спеціального призначення по боротьбі з ними [1-3].

У доповіді приведені результати аналізу приймально-передавальної системи спеціального радіотехнічного виробу.

Проведені дослідження показали, що вона в цілому задовольняє вимогам до сучасних засобів виявлення та супроводження цілей з малою ефективною поверхнею розсіювання, що рухаються на малих висотах з низькою швидкістю.

Разом з тим виникає необхідність збільшення рівня потужності, що приймається, без внесення суттєвих конструктивних змін.

Пропонується для збільшення рівня потужності використовувати енергію сигналів комбінаційних частот, що виникають при перетворенні коливань при випромінюванні та прийманні сигналу.

Недоліком запропонованого рішення є жорсткі технічні вимоги до пристроїв перетворення та компенсації.

Метою доповіді є доведення отриманих результатів та обговорення напрямків подальших досліджень.

Список літератури

1. Герасимов С.В. Оцінка параметрів руху повітряних об'єктів при об'єднанні результатів незалежних первинних вимірювань в активній багатопозиційній системі радіолокації / С.В. Герасимов, Д.М. Ізосімов, Є.С. Рощупкін, О.М. Богдановський // Системи озброєння і військова техніка. – 2010. – №3. – С. 110-113. http://nbuv.gov.ua/UJRN/soivt_2010_3_28.

2. Герасимов С.В. Оценка параметров движения маневрирующих воздушных объектов в активной некогерентной системе при обработке информации от нескольких неравноточных источников с разным темпом обзора пространства / С.В. Герасимов, Е.С. Рощупкин, Г.А. Федак, Я.В. Бабий // Військово-технічний збірник. – 2012. – № 1. – С. 18-26. http://nbuv.gov.ua/UJRN/vtzb_2012_1_6.

3. Brytov, O., Bieliaiev, D., Kukobko, S., Chmil, Y., Dzhus, V., Herasymov, S., Korobkov, Y., Pomohaiev, I., & Roshchupkin, Y. (2021). Justification of the method of evaluation of the efficiency of air reconnaissance by unmanned aviation of ground (sea) objects. InterConf, (93), 471-485. https://doi.org/10.51582/interconf.21-22.12.2021.050.

ВПЛИВ ВИКОРИСТАННЯ ПРОРАМ ДЛЯ АВТОМАТИЧНОЇ ГЕНЕРАЦІЇ ТЕКСТІВ НА ОСВІТНІЙ ПРОЦЕС: ChatGPT

Главчева Ю.М., Главчев М.І.
Національний технічний університет
«Харківський політехнічний інститут», Харків, Україна

У світі давно існують та застосовуються у різних сферах діяльності людини програми для автоматичної генерації текстів. До теперішнього часу більшість автоматично написаних текстів могли бути легко визначені експертом та потребували додаткового опрацювання людиною. Новий сервіс ChatGPT значно підвищив якісний рівень штучно згенерованих текстів. Це дозволило зробити створені ChatGPT тексти максимально схожими на текст, створений людиною, що викликало появу низки актуальних проблемних питань у сфері освіти та науки.

Метою доповіді є аналіз впливу нового сервісу ChatGPT на освітній процес в закладах вищої освіти.

В доповіді аналізуються можливі наслідки використання нового сервісу ChatGPT студентами в процесі навчання та визначаються перспективні актуальні напрями роботи для нівелювання наслідків, що є негативними.

Університети світу вже працюють в цьому напряму та публікують на офіційних сайтах коментарі, рекомендації та політики використання подібних сервісів [1–3].

Одним з негативних наслідків можна вважати недоброчесну поведінку студентів, а саме використання сервісу при написанні письмових робіт, що дуже складно відстежити та розкрити. На сучасному етапі використовуються технології розпізнавання автоматично згенерованого тексту, але вони не дають точного результату.

Таким чином, використання мовних моделей штучного інтелекту, таких як ChatGPT, у закладах вищої освіти піднімає комплекс важливих етичних, правових і технічних проблем.

На основі проведеного аналізу в наступних дослідженнях планується конкретизувати та систематизувати актуальні проблемні питання використання ChatGPT у сфері освіти та науки та визначити напрями роботи для їх вирішення.

Список літератури

1. University leaders issue AI guidance in response to growing popularity of ChatGPT. URL: https://yaledailynews.com/blog/2023/02/12/university-leaders-issue-ai-guidance-in-response-to-growing-popularity-of-chatgpt/.
2. Practical Responses to ChatGPT and Other Generative AI. URL: https://www.montclair.edu/faculty-excellence/practical-responses-to-chat-gpt/.
3. AI Guidance. URL: https://poorvucenter.yale.edu/AIguidance.

РОЗШИРЕННЯ ОБЛАСТІ ЗАСТОСУВАННЯ AOSP ДЛЯ ВИКОРИСТАННЯ В БОРТОВИХ КОМП'ЮТЕРНИХ СИСТЕМАХ НА ЗАЛІЗНИЧНОМУ ТРАНСПОРТІ

Главчев Д.М.
Національний технічний університет
«Харківський політехнічний інститут», Харків, Україна

Сьогодні на базі Android Open Source Project (AOSP) [1] побудовано багато рішень пов'язаних з бортовими комп'ютерами, що використовуються в автомобільному транспорті [2]. AOSP надає повний набір системних компонентів, які можуть бути доповнені у відповідності до поставлених задач. Це дає змогу для виробників автомобілів створювати Automotive прошивки для бортових комп'ютерів (БК), які можуть виконувати роль, як мультимедійних систем, так і систем для діагностики автомобіля та взаємодії з водієм [2]. Проте, область застосування AOSP може бути розширена за рахунок використання відомих підходів для створення прошивок для БК, але не на автомобільному, а на залізничному транспорті.

Метою доповіді є аналіз існуючих підходів до створення прошивок, для бортових та мультимедійних систем на автомобільному транспорті. Аналіз існуючого досвіду в сфері авто, та можливості розширення області застосування AOSP та створення повноцінних залізничних операційних систем (ОС).

В доповіді аналізуються питання створення на базі AOSP, ОС для БК потяга. Для проведення тестів першим кроком пропонується залишити як є Car Service та Car API [2, 3]. При цьому на рівні з Car API створити Train API (рис. 1).

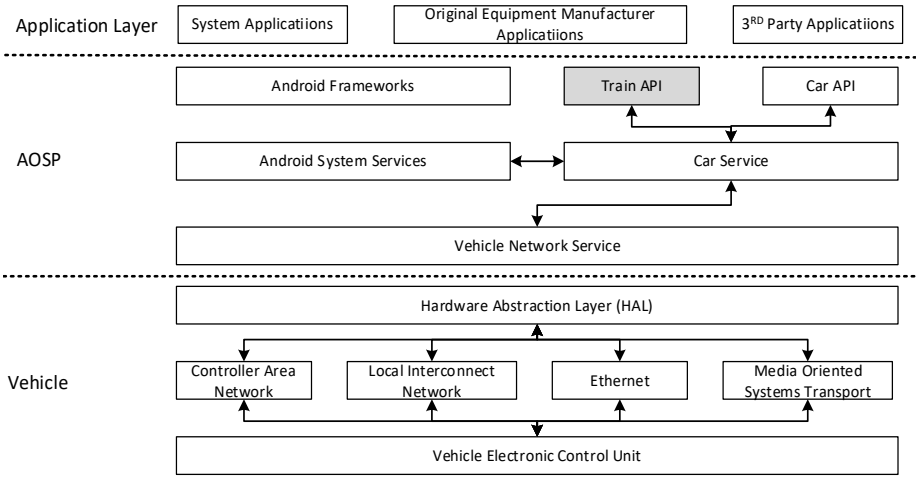

Рисунок 1 – Доповнена структура Automotive AOSP

Новий компонент позначений на рис. 1 більш темним кольором.

Потяг та автомобіль мають схожі параметри і перевірити роботу системи можна, наприклад, отримавши інформацію про швидкість, та пройдений шлях.

Важливо зазначити, що на даному етапі Car Service залишається, та побудова Train API будується поверх нього, з імплементацією того функціоналу та даних, які можуть співпадати у автомобіля та потяга, як у рухомого об'єкта. Таким чином, можна зв'язати Car Service з Hardware Abstraction Layer потяга, для обміну сигналами між датчиками і системами потяга, та безпосередньо прошивкою.

Варто звернути увагу на те, що питання використання Automotive прошивок вже розглядалося [4, 5], і їх застосування на залізничному транспорті виглядає доцільним, проте стандартні можливості, які пропонуються автомобільною прошивкою, не можуть повністю розкрити потенціал операційної системи під час використання в БК потяга.

Таким чином, розширення області застосування AOSP для використання на залізничному транспорті, цілком можливе.

Створення відповідного Train API у вигляді першого кроку, дасть можливість будувати спеціалізовані залізничні додатки, що взаємодіють з датчиками та системами потяга. При цьому, взаємозв'язок між операційною системою та обладнанням потяга виконується через Car Service, який вже має той функціонал, який може бути використаний для побудови прошивки, що може бути застосована на бортовому комп'ютері потяга.

В майбутньому, після аналізу особливості роботі прошивки в БК потяга, можна буде підняти питання відходу від Car Service в напрямку більш спеціалізованого рішення, але на даному етапі, доступного фунціоналу нам цілком достатньо.

Список літератури

1. Automotive AOSP. URL: https://source.android.com/devices/automotive.
2. Android for Cars. URL: https://developer.android.com/cars.
3. Android OS Core Topics. AOSP. URL: https://source.android.com/core.
4. Hlavchev D. Train driver decision support system based on android open source project // Hlavchev D. // Informatics, control and artificial intelligence. Theses of the ninth international scientific and technical conference. – Kharkiv: NTU "KhPI", 2022. – 160 p., p. 22.
5. Главчев Д.М. Розробка системи ідентифікації машиніста на основі Android Auto та Apple Carplay для бортового комп'ютера потяга на базі Android Open Source Project // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 12-ї міжнар. наук.-техн. конф., 27-28 квітня 2022 р., Баку–Харків–Жиліна : [у 2 т.]. Т. 1 : секція 1-4 / Військ. акад. збройних сил Азербайджанської Республіки [та ін.]. – Харків : Петров В. В., 2022. – 185 с., с. 14.

ВИКОРИСТАННЯ ВЕБ-САЙТУ «RAPID TEST FOR STUDENTS» ЯК ЗАСОБУ ПЕРЕВІРКИ ЗНАНЬ ПРИ ОН-ЛАЙН ТЕСТУВАННІ

Азнаурян І.О., Петруньок Т.Б., Погребняк Ю.М.
Київський національний університет будівництва і архітектури, Київ, Україна

На сьогодні для України надважливо підготувати висококваліфікованих спеціалістів, які мають будувати країну сучасною, сильною, європейською державою. Тому виникає потреба у забезпеченні країни висококваліфікованими фахівцями будівельної галузі.

Реалізація фундаментальної підготовки висококваліфікованих фахівців будівельної галузі у дистанційному режимі вимагає постійного пошуку інноваційних технологій, використання засобів телекомунікаційного зв`язку, що призводить до інформатизації навчального процесу [1]. Закладам вищої освіти необхідно впроваджувати у свою діяльність сучасні інноваційні розробки, активно використовувати досягнення науки, які і є рушійною силою для суттєвих перетворень у системі освіти та її розвитку. Наразі, актуально навчання, що здійснюється з використанням ресурсів та технологій глобальної мережі інтернет, тому необхідно змінювати підходи в освітньому процесі, використовуючи веб-сайти, веб-додатки та інші програмні інструменти.

Метою доповіді є представлення створеного студентом веб-сайту «Rapid test for students», який розроблений для впровадження його в освітній процес у закладах вищої будівельної освіти, що містить тестові завдання і використовується як засіб перевірки знань студентів на практичних та лабораторних заняттях, під час поточного та підсумкового контролю. Веб-сайт базується на таких компонентах:

– головна мова створення веб-сайту – Python;

– мова програмування, яка дозволяє змінювати елементи на сайті без перезавантаження сторінки, що дозволяє покращити досвід користувача (приємніше користуватися сайтом) – Javascript;

– стандартні інструменти для розмітки веб-сторінок та задавання їм дизайну Html, css;

– фрейморк на основі якого створено веб-сайт – Flask;

– доповнення до головного фреймворка (до flask), що забезпечує реєстрацію на сайті та розмежовує права доступу – Flask-login;

– доповнення до головного фреймворка (до flask) за допомогою якого можна звертатися до бази даних без використання SQL запитів, що забезпечує більш швидку і зручну розробку – SQLAlchemy;

– бібліотека, яка створює хеш-суму для паролю; в базі даних ми не зберігаємо пароль, лише хеш-суму, що не дає можливості побачити справжній пароль навіть при крадіжці бази даних – Werkzeug;

– бібліотека, що дозволяє звертатися до бази даних через SQL запити (іноді так зручніше) – sqlite3;

– бібліотека за допомогою якої можна створювати таблиці exel (результати студентів зручніше зберігати та обробляти в exel форматі) – openpyxl;

– бібліотека для перемішування значень (допомагає перемішувати запитання та відповіді до запитань при виведенні) – random;

– бібліотека за допомогою якої ми можемо дізнатися реальний час та проводити різні маніпуляції з ним (при завершенні студентом тесту записуємо в таблицю час) – time;

– бібліотека, що забезпечує взаємодію між додатком та операційною системою (допомагає зберігати зображення при додаванні їх в тест) – os.

Тестування нині стає органічною невід`ємною частиною сучасного освітнього процесу, найважливішим засобом встановлення зворотнього зв'язку, завдяки якому навчання перетворюється на диференційований, особистісно-орієнтований процес, що забезпечує індивідуальний темп навчання, усунення суб'єктивізму та авторитаризму в оцінці рівня навчальних досягнень студентів, засобом об'єктивізації експертизи якості освітнього процесу та його індивідуалізації.

В доповіді наведено результати апробації веб-сайту, які показують, що він має зручний та зрозумілий інтерфейс для створення викладачем тестових завдань: можливість внесення формул, рисунків, графічних зображень, додавання варіантів відповідей, доповнення вже створеного тесту новими питаннями.

Викладач (у ролі адміністратора) має можливість: визначати та змінювати кількість питань у тесті, задавати та змінювати час проходження тесту, миттєво переглядати результати (у відсотках) роботи студента (учня) у «Таблиці результатів», має можливість завантажувати результати тестів у Excel таблиці для подальшої обробки та збереження інформації, видаляти з програми результати тестування по мірі необхідності, закривати та відкривати доступ до відповідного тесту у будь який час, надавати право адміністрування іншим особам (за необхідністю). Перевагами для студентів є:

доступний інтерфейс тестів,

можливість прийняти участь у тестуванні з любого гаджета,

можливість проходити тестування за відсутності на занятті (у любому місці),

зручне заповнення авторизації у програмі, миттєвий перегляд результатів роботи з можливістю перескладання.

Список літератури

1. Петруньок Т.Б. Формування у майбутніх фахівців будівництва та цивільної інженерії знань про використання сучасних досягнень фізики в будівельній галузі. Наукові записки Бердянського державного педагогічного університету. Серія : Педагогічні науки : зб. наук. пр. – Вип.1. – Бердянськ : БДПУ, 2020. – 388 – 394 с. https://pedagogy.bdpu.org/wp-content/uploads/2020/05/44.pdf

2. Shakhina I.U., Ilyina A.I. Organization of quality control knowledge students with electronic test // Physical and Mathematical Education: scientific journal. – 2016. – Issue 4(10). – P. 152-157.

ВИКОРИСТАННЯ ІКТ ПРИ ІНКЛЮЗИВНОМУ НАВЧАННІ В УНІВЕРСИТЕТІ

Кірвас В.А.
Харківський гуманітарний університет
«Народна українська академія», Харків, Україна

Реалізація державної політики у сфері вищої освіти забезпечується рівними умовами доступу до вищої освіти, додатковою підтримкою в освітньому процесі осіб з особливими освітніми потребами, створенням для них вільного доступу до інфраструктури закладу вищої освіти; підготовкою фахівців з числа осіб з інвалідністю на основі спеціальних освітніх технологій [1]. Однією з найбільш актуальних проблем є інклюзивна освіта, зокрема осіб з вадами зору (ВЗ) або слуху (ВС). Такі учні повинні йти в ногу з часом та вільно користуватися комп'ютером, інтернетом, смартфоном. І одне з головних завдань освіти в умовах цифровій трансформації – навчити учнів та студентів, у тому числі осіб із ВЗ, ВС, користуватися сучасними ІКТ.

В умовах глобальної цифровізації сучасні інформаційні й комунікаційні технології (ІКТ) мають потужні інструменти для роботи з текстовою, числовою та графічною інформацією, а у поєднанні з інтернетом і дистанційними технологіями вони створили ефективне за своїми можливостями всесвітнє середовище навчання. Дані технології дозволяють учням з ВЗ і ВС брати активну участь у навчальному процесі, а викладачам використовувати адаптований під індивідуальні особливості учнів контент.

Спеціальні апаратні та програмні засоби дозволяють незрячим та слабозорим або із ВС навчатися з використанням комп'ютерної техніки та більшості стандартних користувацьких можливостей. «Спілкування» інвалідів включає використання мов, текстів, абетки Брайля, тактильного спілкування, великого шрифту, доступних мультимедійних засобів, так само, як і друкованих матеріалів, аудіо засобів, звичайної мови, читців, а також підсилювальних і альтернативних методів, способів та форматів спілкування, зокрема, доступних ІКТ. Якщо студент має проблеми зі слухом, в першу чергу викладач повинен продумати чітку програму для нього, можна використовувати відео, включаючи субтитри, або робити відео і в ньому повинен бути текст, так само можна використовувати сурдоперекладача, і тоді студент розумітиме все, що розповідає викладач. Якщо студент має вади слуху і він користується слуховим апаратом, його треба садити на передні парти та розповідати більш чітко весь матеріал.

Для забезпечення ефективності та доступності освітнього процесу необхідне спеціалізоване технічне оснащення навчальних закладів сучасною комп'ютерною технікою, у тому числі тифлопристроїми, комп'ютерними тифлотехнологіями і відповідними педагогічними програмними засобами, електронними підручниками, спрямованими на полегшення процесу навчання осіб із ВЗ та ВС.

АЛГОРИТМ ВИЗНАЧЕННЯ ПРОСТОРОВОЇ ТРАЄКТОРІЇ ПОЛЬОТУ БПЛА НА ОСНОВІ ПАРАЛЕЛЬНОГО ХВИЛЬОВОГО ТРАСУВАННЯ

Дергачова Д.К.
Харківський національний університет радіоелектроніки, Харків, Україна

Одним із перспективних напрямків використання безпілотних літальних апаратів (БПЛА) є проведення різних видів моніторингу – кліматичного, будівельних об'єктів, об'єктів критичної інфраструктури та ін. При плануванні маршрутів моніторингу БПЛА виникає задача раціонального визначення траєкторії руху БПЛА у 3D-просторі зі штучними або натурними перешкодами, що можуть пересуватися з часом.

Для планування таких траєкторій був розроблений алгоритм 3D хвильового трасування.

У якості елементарних дискретів у цьому алгоритмі використовуються кубоїди – елементи простору що характеризуються геометричним центром та розмірами. Кубоїди, що містять перешкоди у певних відлік часу забороняються для планування руху.

На наступному етапі алгоритму проводиться моделювання паралельного розповсюдження числової хвилі із двох джерел: початкового положення та мети руху до їх зустрічі. На останньому етапи ідентифікується траєкторія руху [1].

Розроблений дозволить проводити визначення раціональних траєкторій польоту БПЛА у середовищі з динамічними перешкодами, обирати необхідний алгоритм скеровування у випадку появи нових перешкод для руху. У якості засобів розробки використана мова програмування Python, бібліотеки Python QT, numpy, pandas, matplotlib.

Метою доповіді є побудова алгоритму просторового хвильового трасування та використання його для планування маршруту руху БПЛА у динамічному просторі з перешкодами, а також розробка програмного забезпечення для реалізації цього алгоритму.

В доповіді наведені результати – етапи алгоритму просторового хвильового трасування, а також результати моделювання процесу побудови маршруту для БПЛА у просторі з динамічними перешкодами.

Список літератури

1. Kulik, Anatoliy, et al. "Development of Technical Solutions For Realisation Of Intelligent Transport Systems." Transport Problems 8.1 (2013): 27-33.

2. Karak, A., & Abdelghany, K. (2019). The hybrid vehicle-drone routing problem for pick-up and delivery services. Transportation Research Part C: Emerging Technologies, 102, 427-449.

ОЦІНКА ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Носик А.М.
Національний технічний університет "Харківський політехнічний інститут", Харків, Україна
Кучеренко Ю.Ф.
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

Функціонування автоматизованих систем управлінні спеціального призначення (АСУ СП), як то, систем державного та військового управління, які є складними організаційно-технічними системами, що працюють в умовах здійснення повномасштабної агресії з боку російської федерації відбувається в умовах впливу на них низки зовнішніх і внутрішніх факторів, а тому цей процес характеризується динамікою зміни станів їх основних елементів, як взаємопов'язаної сукупності, що їх утворюють [1–3].

Метою доповіді є формування пропозицій щодо вибору певного підходу (методики) з оцінки ефективності функціонування АСУ СП в короткі терміни на основі визначення ефективності їх основних складових основ.

В доповіді надані пропозиції щодо застосування методики оцінки ефективності функціонування АСУ СП, що дозволяє здійснити поточну оцінку ефективності функціонування у стислі терміни через оцінку їх основних складових основ, а саме: функціональної (якість виконання функціональних завдань), організаційної (якість роботи користувачів системи та персоналу, що її обслуговує та технічної (технічний стан комплексів засобів автоматизації та засобів зв'язку). Для оцінки вказаних основ АСУ СП використовуються методи експертної оцінки, а також правило "вузького місця", тобто загальна ефективність функціонування АСУ СП визначається за найгіршим значенням однієї з її основних складових основ, які були оцінені за п'ятибальною шкалою їх оцінки, що значно спрощує визначення поточної загальної ефективності функціонування АСУ СП.

Список літератури

1. Іванов А. О. Теорія автоматичного керування: Підручник. — Дніпропетровськ: Національний гірничий університет. — 2003. — 250 с.

2. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення. – К.: Укр-НДІССІ, 1994. – 92 с.

3. Кучеренко Ю.Ф. Методика оцінки загального стану автоматизованої системи військового призначення на основі визначення технічного стану комплексів засобів автоматизації, що її складають. *Системи обробки інформації*. 2017. №3 (149). С.118-120. DOI: https://doi.org/10.30748/ soi.2017.149.23.

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОПТИМІЗАЦІЇ ФУНКЦІОНУВАННЯ КОМ'ЮТЕРНИХ МЕРЕЖ: АНАЛІЗ ЕФЕКТИВНОСТІ ТА МОЖЛИВОСТЕЙ ВДОСКОНАЛЕННЯ

Пилипенко А.О., Сокирко М.А., Завизіступ Ю.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

Оптимізації функціонування комп'ютерних мереж показує, що застосування штучного інтелекту може покращити функціонування комп'ютерних мереж.

Дослідження в цій області може допомогти зрозуміти, які саме методи штучного інтелекту найбільш ефективні для оптимізації роботи мереж та як їхнє використання може покращити їх функціональність [1].

Також є доцільним огляд поточних технологій та алгоритмів штучного інтелекту, які використовуються в комп'ютерних мережах [2].

Дослідження може включати аналіз використання навчання з підкріпленням, глибокого навчання, нейронних мереж та інших методів машинного навчання для управління мережевим трафіком [3], виявлення помилок та захисту від кібератак.

Для підтвердження можливості використання методів штучного інтелекту стосовно оптимізації функціональності комп'ютерних мереж, дослідження може проводитися шляхом аналізу та оцінки, як штучний інтелект може бути застосований для створення автономних мереж, що забезпечують максимальну доступність та ефективність передачі даних у різних умовах з'єднання та топології мережі.

Метою доповіді є дослідження переваг використання штучного інтелекту для оптимізації функціональності комп'ютерних мереж з метою сприяння розумінню цього питання. Було застосовано систематичний та структурований підхід для збору та аналізу даних, і на його основі були представлені висновки та рекомендації.

Отримані результати свідчать про те, що використання методів штучного інтелекту допомагають покращити роботу комп'ютерних мереж та забезпечити більш ефективний та надійний обмін даними між комп'ютерами та пристроями у мережі.

Список літератури

1. С. Рассел, П. Норвиг. «Искусственный интеллект: современный подход», 4-е издание, «ДИАЛЕКТИКА», 2021, 704 с.

2. Schapire, R. E. The boosting approach to machine learning: An overview. In Denison, D. D., Hansen, M. H., Holmes, C., Mallick, B., and Yu, B. (Eds.), Nonlinear Estimation and Classification. Springer. 2003.

3. Christopher M. Pattern Recognition and Machine Learning», Bishop, 2006, 738 p.

КОДУВАННЯ ДЛЯ ЗМЕНШЕННЯ ЕНЕРГІЇ РУХУ ДАНИХ

Ярещенко В.В., Косенко В.В.
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна.

Питання енергоспоживання та розсіювання потужності в інформаційних системах та мережах стає все більш актуальним. Висока комутаційна активність спричиняє серйозні втрати в надійності зв'язку через його об'єми між лініями комунікацій.

Нові технології енергонезалежної пам'яті з байтовою адресацією дають змогу створювати системи з великою постійною пам'яттю, підвищуючи надійність і потенційно зменшуючи енергоспоживання. Однак ці технології підтримують тільки обмежену кількість операцій запису на комірку й витрачають значну частину своєї потужності на зміну біта під час запису [1]. Для рішення цих завдань сьогодні розповсюджено використання коду Грея, що має низку недоліків [2].

Метою дослідження є розроблення методу побудови кодів одиничної відстані, розрахунку та аналізу характеристик виявлених кодів.

В дослідженні пропонується для розгляду метод побудови кодів одиничної відстані що базується на моделі гіперкуба та алгоритму пошуку Гамільтонового шляху у графі [3-5]. В результаті використання запропонованого методу було згенеровано набір кодів та розраховано їх характеристики. Визначено, що виявлені під час дослідження коди відрізняються за цими властивостями від коду Грея.

В результаті дослідження розроблено метод побудови кодів одиничної відстані, розраховано та проаналізовано характеристики виявлених кодів. Використання запропонованого методу під час створення інформаційних систем дозволяє аналізувати та відбирати коди з найкращими властивостями, що в свою чергу дає можливість отримувати кращі результати з точки зору затримок в мережі, енерговитрат та інших обмежень при розробці цифрових систем.

Список літератури

1. Bittman D. et al. Optimizing Systems for Byte-Addressable NVM by Reducing Bit Flipping // FAST. – 2019. – P. 17-30.

2. Lee D., O'Connor M., Chatterjee N. Reducing Data Transfer Energy by Exploiting Similarity within a Data Transaction // IEEE International Symposium on High Performance Computer Architecture (HPCA). – 2018. – P. 40-51.

3 Mütze T., Nummenpalo J. Efficient computation of middle levels Gray codes // ACM Transactions on Algorithms (TALG). – 2018. – V. 14. – №. 2. – P. 1- 29.

4. Kandel A., Bunke H., Last M. Applied Graph Theory in Computer Vision and Pattern Recognition // Springer, 2007. – 261 p.

5. Thulasiraman K. Handbook of Graph Theory, Combinatorial Optimization, and Algorithms // New York: Chapman & Hall/CRC, 2015. – 1244 p.

МЕТОД ПОБУДОВИ ТОПОЛОГІЇ МОБІЛЬНИХ БЕЗПРОВІДНИХ МЕРЕЖ

Лазуренко Б.О., Охрименко М.Ю.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Безпровідні мережі майбутнього покоління (5G) мають бути надзвичайно щільними, неоднорідними та, імовірно, оснащеними пересувними та повітряними базовими станціями (БПЛА). Застосування дистанційно керованих БПЛА дозволяє створити спеціальну повітряну однорангову коміркову мережу FANET, де її пристрої передають інформацію один одному у неліцензованому спектрі з використанням технології WLAN IEEE 802.11 [1].

Метою доповіді є обґрунтування застосування БПЛА, що забезпечує топології більшу дальність передачі, підтримку наземних мереж зв'язку, допомогу у обміні даними між пристроями та засобами IoT.

Основною відмінністю цієї мережі є той факт, що вона не має інфраструктури. Пристрої, що входять до складу мережі, мають можливість взаємодії один з одним, діючи у якості маршрутизаторів. Переміщення у тривимірному просторі ускладнює проблеми мобільності, оскільки переміщення призводить до відключення поточних користувачів.

Таким чином мережа FANET повинна бути самокерованою, самоорганізованою та готовою до раптових змін топології, організації та зв'язку. Під час руху БПЛА маршрути, зазвичай, переробляються, для продовження зв'язку між пристроями. Тому маршрутизація повинна виконуватися динамічне, а протокол маршрутизації слід робити ефективним і простим, підвищуючи автономність БПЛА та зменшуючи затримку доставки інформації між ними. За рахунок високої мобільності БПЛА в мережі FANET оновлення місця розташування усіх вузлів в мережі є критичним фактором. Кожен з БПЛА повинен знати місце розташування інших пристроїв у режимі реального часу, що вимагає необхідність отримання надійного і стабільного зв'язку між пристроями для підтримання відповідного рівня якості обслуговування (QoS) та якості взаємодії (QoE).

Поєднання показників рівня мобільності, напряму переміщення БПЛА, пропускної здатності каналів зв'язку та індикації потужності прийнятого сигналу складають інтегральний показник для прийняття рішення щодо передачі обслуговування між пристроями. Таким чином слід застосовувати інтелектуальний метод передачі обслуговування за рахунок інтеграції елементів штучного інтелекту до безпровідної мережі мобільного зв'язку.

Список літератури

1. IEEE Std 802.11b. The Institute of Electrical and Electronics Engineers,1999.89 c.

ПОРУШЕННЯ ПРАЦЕЗДАТНОСТІ НАПІВПРОВІДНИКОВИХ ПРИЛАДІВ В УМОВАХ ДІЇ ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ

Серков О.А., Охрименко М.Ю., Яковенко І.В.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Метою доповіді є створена фізична модель виникнення зворотних відмов напівпровідникових приладів в умовах, коли дія стороннього випромінювання призводить до відхилення їх робочих характеристик від норми. Причиною появи таких змін є процеси трансформації енергії наведених зовнішнім випромінюванням струмів на енергію власних коливань напівпровідникових приладів.

Проведено аналіз основних типів порушень працездатності електрорадіовиробів в умовах дії електромагнітного випромінювання.

Доведено. що більшість існуючих методик, не враховують ефектів зміни їх робочих характеристик в умовах дії стороннього випромінювання, коли межу критичної енергії ще не досягнуто. Визначені кількісні параметри сторонніх електромагнітних полів, що є причиною появи незворотних відмов напівпровідникових приладів, та здійснено аналіз існуючих методик, які визначають межу їх працездатності. Розглянуто та класифіковано типи електромагнітних коливань, які існують на межі розподілу середовищ.

Зазначено, що основні їх відмінності полягають у їх електромагнітних властивостях, які створюють поверхневі поляритони (хвилі Фано). При цьому були використані рівняння електродинаміки, а саме: рівняння Максвела, матеріальні рівняння та граничні умови, за допомогою яких визначають закони дисперсії поверхневих електромагнітних коливань. Спектр поверхневих поляритонів було визначено в умовах наближення до холодної плазми та нехтування затуханиям, яке обумовлено зіткненнями. Для знаходження механізму загасання поверхневих плазмонів, яке обумовлено їх взаємодією з електронами провідності на межі розподілу середовищ, застосовувалися рівняння електродинаміки в умовах нехтування ефектами запізнювання. При цьому отримане дисперсійне рівняння для системи потік заряджених частинок – напівпровідникова надгратка в умовах, коли частинки потоку проходять крізь середовище з постійною швидкістю. Знайдені власні частоти коливань, сформульовано умови розвитку нестійкостей та отримані вирази для різних окремих випадків. При цьому вирішено важливе питання про можливість збудження поверхневих коливань в умовах резонансної взаємодії хвиль та частинок, коли потік електронів та періодична структура розділені у просторі. Наведено кількісні оцінки втрат енергії наведених струмів на збудження поверхневих коливань. При цьому величина енергії випромінювання власних коливань напівпровідникових приладів складає $10^{-7} - 10^{-8}$ *Дж*. Цей тип коливань визначає ефективність їх взаємодії зі струмами, що наведені зовнішнім випромінюванням.

АЛГОРИТМ ФРАКТАЛЬНОГО СТИСНЕННЯ ДЛЯ НАБОРІВ ЗОБРАЖЕНЬ ПРИРОДНИХ ОБ'ЄКТІВ, ЩО ВИКОРИСТОВУЮТЬСЯ У МАШИННОМУ НАВЧАННІ

Домнін Д.В., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В.Н. Каразіна**,** Харків, Україна

Метою доповіді є дослідження алгоритму фрактального стиснення, для створення такого варіанту цього методу стиснення, що якнайкраще відповідатиме задачі оптимального зберігання специфічних наборів даних. Мова передусім йде про об’ємні набори однотипних даних, зокрема зображення, що широко використовуються для навчання штучних нейромереж, що розпізнають образи. Виникає необхідність оптимального зберігання величезних масивів подібних даних. У випадку зображень природних об’єктів, метод фрактального стиснення проявляє ряд властивостей, що вигідно вирізняють його серед інших [1, 2].

Фрактальне стиснення – метод стиснення з втратами, заснований на застосуванні системи ітерованих функцій [1]. При використанні цього алгоритму для зображень природних об'єктів досягається великий коефіцієнт стиснення за прийнятної якості зображення; ефективність стиснення може бути збільшена при більшій комплексності зображень; завдяки особливостям кодування не виникає проблем зі зміною роздільної здатності фотографій; при достатньо довгому процесі кодування зображень алгоритм забезпечує швидкий процес декодування [3].

Аналіз існуючих відкритих публікацій за темою дослідження показав, що основним недоліком цього методу є його низька швидкодія. У ході роботи було створене спеціалізоване програмне забезпечення, що реалізує базовий алгоритм фрактального стиснення для визначеного типу зображень. Це дозволило провести експерименти, результати яких також вказують на низьку швидкодію методу. Частково це може бути викликано неоптимізованою імплементацією, але більшою мірою проблема в самому алгоритмі, що перевантажений циклами перебору. На сьогодні відома досить велика кількість алгоритмів оптимізації перебору, найбільш перспективними з яких виявилися метод виділення особливостей і метод класифікації доменів, використання яких дозволить покращити швидкодію алгоритму [3].

Список літератури

1. Salomon, D., Motta, G. Handbook of Data Compression Fifth Edition. London: Springer-Verlag. 2010. 1370 p. ISBN 978-1-84882-902-2.

2. Mandelbrot, B. The Fractal Geometry of Nature. USA: Echo Point Books & Media, LLC. 2021. 500 p. DOI: https://doi.org/10.1119/1.13295.

3. Soumitro Banerjee. Fractal Image Compression. Available at: https://youtu.be/Lte3xpmH2_g (accessed 23.03.2023).

МОДЕЛЮВАННЯ ВИКЛАДАЦЬКОЇ ДІЯЛЬНОСТІ У ТЕХНІЧНОМУ УНІВЕРСИТЕТІ

Чепела С.П.
Харківський національний університет радіоелектроніки, Харків, Україна
Бельорін-Еррера О.М.
Національний технічний університет «ХПІ», Харків, Україна

Сучасний рівень розвитку суспільства, проникнення практично в усі сфери людської діяльності нових інформаційних технологій, суттєве збільшення темпу появи нових знань, підвищення вимог до знань, умінь і навичок учнів, – ось далеко не повний перелік причин для необхідності здійснення якісного стрибка в педагогічній діяльності. На наш погляд, для якісної зміни педагогічної діяльності у вишах необхідне проведення глибокого наукового аналізу усіх сторін педагогічної праці [1]. Моделювання, як метод дослідження педагогічної діяльності, має ряд переваг. По-перше, моделювання педагогічних процесів дозволяє скоротити матеріальні та людські ресурси. По-друге, обґрунтовано та детально задані у процесі моделювання обмеження та припущення призводять до того, що можна дослідити саме ті сторони педагогічної діяльності, які вивчаються дослідником цієї діяльності. По-третє, скорочується час, необхідний для проведення досліджень і збільшується кількість даних для аналізу за допомогою багаторазового прогону моделі [2].

Метою доповіді є розгляд підходів до розроблення математичної моделі процесу викладацької діяльності у технічному університеті.

У доповіді наведені та обґрунтовані обмеження та припущення, властиві викладацькій діяльності в технічному університеті. Розроблено математичну модель даного процесу із застосуванням теорії нечітких множин та алгебри відношень Запропоновано низку аксіом для визначення потужності отриманих відношень. Проведені дослідження показали, що використовуючи сучасний математичний апарат, зокрема теорію нечітких множин та алгебру відношень, можна розробити моделі викладацької діяльності у технічному університеті при заданих обмеженнях та припущеннях. Розробка таких моделей (функцій приналежності викладача) відкриває великі можливості у створенні методичних систем навчального призначення.

Розроблені моделі у сукупності із запропонованими у доповіді аксіомами можуть бути використані при обчисленні рейтингу викладачів у вишах у рамках автоматизованої системи управління технічним вишем.

Список літератури

1. Дубасенюк О. А. Концептуальні моделі педагогічної освіти: наукові пошуки та здобутки. Професійно-педагогічна освіта: сучасні концептуальні моделі та тенденції розвитку: Монографія Житомир: Вид-во ЖДУ ім. І. Франка, 2008. С. 8-29.

2. Пономарьов О. С., Середа Н. В., Чеботарьов М. К. Моделювання діяльності фахівця : навч.-метод. посібник. Харків : НТУ «ХПІ», 2015. 58 с.

ІНФОРМАЦІЙНА СИСТЕМА НАУКОВОГО ТОВАРИСТВА

Турчина А.В., Бельорін-Еррера О.М.
Національній технічний університет «ХПІ», Харків, Україна

В доповіді розглянуто основні положення розробленого веб-застосуноку за допомогою мови програмування JavaScript, який має функцію розподілення на ролі адміністратора та читача Блогу. В веб-застосунку реалізований такі функціональні області, як головна сторінка, керуючі органи, новини, статті, форми реєстрації та входу. Для користувача в ролі адміністратора реалізований особистий кабінет, в якому користувач може здійснювати управління сайтом, а саме додавати, видаляти та змінювати інформацію статей.

Як результат даної роботи може бути використаний для доступу до інформації українського науково-освітнього IT товариства.

Список літератури

1. M. Mozhaiev, V. Peresichansky, V. Roh, O. Bellorin-Herrera. Метод аналізу показників якості комп'ютерної мережі інформаційної системи критичного застосування. Системи управління, навігації та зв'язку. 2023. Т. 1, № 71. С. 118–121. DOI: https://doi.org/10.26906/SUNZ.2023.1

СИСТЕМА РОЗПІЗНАВАННЯ ЗОБРАЖЕНЬ

Малахова К.В., Бельорін-Еррера О.М.
[1]Національній технічний університет «ХПІ», Харків, Україна
Дяченко В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У доповілі розглянуто згорткові мережі, популярні архітектури цих мереж, методи навчання та проблематика даного питання. Було проаналізовано методи та технології для розпізнавання та класифікації зображень. Розглянуто принципи роботи алгоритмів навчання та використання передавального навчання для отримання кращих результатів. Розроблене програмне забезпечення може виконувати такі функції як, вибір координат, зберігання координат для подальшого використання, вибір проміжку часу, завантаження супутникових зображень за вибраний проміжок часу, розпізнавання зображень.

Розроблена система є десктопним додатком, з яким працює оператор та відповідно до його дій дозволяє отримувати зображення для обраної області за вибраний період. Модульність основних функцій цього засобу дозволяють у майбутньому за невеликий час модифікувати їх для використання у повністю автоматизованих системах, не потребуючих керівництва оператора.

Список літератури

1. M. Mozhaiev, V. Peresichansky, V. Roh, O. Bellorin-Herrera Метод аналізу показників якості комп'ютерної мережі інформаційної системи критичного застосування. Системи управління, навігації та зв'язку. 2023. Т. 1, № 71. С. 118–121. DOI: https://doi.org/10.26906/SUNZ.2023.1

ІНТЕЛЕКТУАЛЬНІ ТРАНСПОРТНІ СИСТЕМИ

Кучук Н.Г., Шиман А.П.
Національній технічний університет «ХПІ», Харків, Україна

В доповіді розглянуто основні інтелектуальні транспортні системи. Вони являють собою широкий спектр різноманітних технологій, які включають комунікаційні, інформаційні, автоматичні та вимірювальні рішення та методи управління, які використовуються на транспорті для захисту життя учасників дорожнього руху, підвищення ефективності та ефективності транспортної системи. та охороняти природне середовище. Нейронна мережа дає можливість отримувати результати для короткострокового прогнозу. Тому його можна використовувати в системах управління трафіком, які вимагають включення безпрецедентного параметра для процесу оптимізації, напр. у вигляді інтенсивності або довжини черги. Для прогнозування умов руху використовуються інтелектуальні транспортні системи та нейронні мережі, а особи, які приймають рішення, можуть використовувати запропоновану авторами модель для вирішення проблем управління трафіком.

Список літератури

1. Karakatič S., Podgorelec V. A survey of genetic algorithms for solving multi depot vehicle routing problem // Applied Soft Com-puting. 2015. Vol. 27. P. 519–532. doi: https://doi.org/10.1016/j.asoc.2014.11.005

2. Kooperativ interagierende Automobile / Stiller C., Burgard W., Deml B., Eckstein L., Flemisch F. // at – Automatisierungstechnik. 2018. Vol. 66, Issue 2. P. 81–99. doi: https://doi.org/10.1515/auto-2017-0129.

РОЗРОБКА ІНФОРМАЦІЙНО СИСТЕМИ WEB-МАГАЗИНУ

Лисиця Д.О., Григоренко Є.В., Червоний О.Ю.
Національній технічний університет «ХПІ», Харків, Україна

В доповіді розглянуто процес створення інтернет-сайту та розміщення його в Інтернеті. Це один з альтернативних методів позиціонування компанії та інформування цільової аудиторії. Саме в Інтернеті багато хто шукає докладну, і свіжу інформацію, на основі якої можна отримати уявлення про цікавій компанії, товари і послуги.

Мета дослідження полягає в розширенні знань в області електронної комерції, а саме аналізу існуючих веб-магазинів та їх взаємодії з користувачами.

Одержані результати можуть бути використані в практичній діяльності як звичайних користувачів так і невеликих підприємств.

Список літератури

1. Лисиця Д.О., Калінін Є.І., Нечаусов А.С., Криховецький Г.Я., Асимптотика системи оптимального управлінняз двомамалими сингулярно-збурюючими параметрами, Сучасні інформаційні системи. 2022. Т. 6, No 1, С. 37-42.

MULTI-SERVICE NETWORK LOAD MANAGEMENT INFRASTRUCTURE

Filonenko A., Zhmutsky I., Rakityansky M.
National Technical University «KhPI», Kharkiv, Ukraine

The Report considers the possibility of step-by-step creation of multi-service networks. From the parallel coexistence of NGN with existing networks to their absorption by the first. In the foreseeable future, there will be requirements to increase the bandwidth of access networks. The concepts of multi-service network infrastructure management based on software switching technology are analyzed, the main features of using Softswitch technologies are defined and analyzed. The basic network architectures of multi-service networks are presented and described, focusing on the aspect of network management during the creation of national-level multi-service traffic exchange networks.

It is shown that the longer the packet length in the transport network, the greater the efficiency of the link-layer protocol and the higher the quality of service parameters can be provided by the network. This is because the smaller the packet length, the more packets can be placed in one container and, accordingly, with a minimum packet size, the overhead will be maximum, since the headers of all IP packets, MPLS labels and container overhead will be taken into account, and the efficiency of the transport protocol at this will be minimal.

References

1. Filonenko A., Molchanov H., Bellorin-Herrera O. The method of calculating the capacity of the cloud component of the distributed multiservice network. Control, Navigation and Communication Systems, 2022, № 4(70), pp. 117-121. DOI: 10.26906/SUNZ.2022.4.117

MODELING OF ADAPTIVE ROUTING PROCESSES IN TELECOMMUNICATION NETWORKS

Tykhtylo D., Filonenko A.
National Technical University «KhPI», Kharkiv, Ukraine

The purpose of the report is to improve the efficiency of data packet delivery by developing new and improving existing models and methods of adaptive routing.

Various aspects of classical routing models and algorithms are indicated by the method of determining the shortest routes. An analysis of scientific sources, known methods of finding the shortest paths in a graph, which use modern routing protocols, is carried out, and the main paradigms of dynamic routing methods are also given, each of which has both strengths and weaknesses, so the choice of an approach to solving each specific problem is determined by its specificity

The advantages and disadvantages of each of the adaptive routing methods are revealed. For the adaptive centralized method, the disadvantage is low reliability and periodically necessary recalculation of routing tables. For distance-vector, this is

poor convergence, difficulties in expanding the network. When one of the nodes is disconnected from the network, the "Count down to infinity" problem occurs. For channel state routing method - reduction of bandwidth of data transmission channels, complexity of network expansion. For the broadcast routing method, these are problems when changing the structure and load of the network.

References

1. Filonenko A., Molchanov H., Bellorin-Herrera O. The method of calculating the capacity of the cloud component of the distributed multiservice network. Control, Navigation and Communication Systems, 2022, № 4(70), pp. 117-121. DOI: 10.26906/SUNZ.2022.4.117

НАВАНТАЖЕННЯ У СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ

Коломійцев О.В., Хмель І.Ю., Юнхель І.В.
Національній технічний університет «ХПІ», Харків, Україна

Мета доповіді – оптимізація опорно-транспортних мереж та їх навантаження для підвищення продуктивності систем мобільного зв'язку наступного покоління.

Проведено аналіз процесів встановлення та завершення з'єднань інформаційних потоків, які проходять транспортною мережею системи мобільного зв'язку. Проаналізовано загальні технічні вимоги щодо побудови та розвитку транспортних мереж систем мобільного зв'язку. Запропоновано метод оптимізації конфігурації фізичної структури транспортних підсистем широкосмугових мобільних мереж та їх логічних потоків.

Список літератури

1. Kolomiitsev O. Formal representation of the pixel-by-pixel classification process using a modified wang-mendel neural network. / O. Kolomiitsev, V. Pustovarov // No 3 (13) (2020): Innovative Technologies and Scientific Solutions for Industries "ENGINEERING and INDUSTRIAL TECHNOLOG". pp. 122-128.

2. Альошин Г.В., Коломійцев О.В. та ін. Кібербезпека та інформаційні технології. Монографія. – Х.: ТОВ «ДІСА ПЛЮС», 2020. – 380 с.

СТРУКТУРНА ЖИВУЧІСТЬ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Коломійцев О.В., Влад Ю.В., Дьяконенко І.В.
Національній технічний університет «ХПІ», Харків, Україна

Метою доповіді є підвищення структурної живучості телекомунікаційних мереж для забезпечення їх безвідмовного функціонування. проведено аналіз сучасного стану питань оцінки та підвищення структурної живучості телекомунікаційних мереж. Визначено етапи розвитку, а також фактори, які впливають на рух і формування інформаційного суспільства. Показано, що активний розвиток телекомунікаційних та інформаційних технологій чинять вирішальний вплив на

розвиток телекомунікацій. Показано важливість задач оцінки та підвищення структурної живучості телекомунікаційних мереж. Розглянуто основні причини та фактори, що викликають пошкодження або руйнування елементів телекомунікаційних мереж. Визначено складові властивості живучості та види живучості, критерії та показники живучості телекомунікаційних мереж. Показано, що підвищення структурної живучості є одним з важливих напрямків забезпечення ефективного функціонування та працездатності телекомунікаційних мереж.

Список літератури

1. Kolomiitsev O. Formal representation of the pixel-by-pixel classification process using a modified wang-mendel neural network. / O. Kolomiitsev, V. Pustovarov // No 3 (13) (2020): Innovative Technologies and Scientific Solutions for Industries “ENGINEERING and INDUSTRIAL TECHNOLOG”. pp. 122-128.

2. Альошин Г.В., Коломійцев О.В. та ін. Кібербезпека та інформаційні технології. Монографія.. – Х.: ТОВ «ДІСА ПЛЮС», 2020. – 380 с.

МОНІТОРИНГ НАВАНТАЖЕННЯ КОМПОНЕНТІВ ПЕРСОНАЛЬНОГО КОМП’ЮТЕРА

Панченко В.І., Любенко А.І.
Національній технічний університет «ХПІ», Харків, Україна

Метою доповіді є дослідження процесу процесу моніторингу навантаження компонентів персонального комп'ютера.

Програми діагностики комп'ютера вже відповідають за діагностику як компонентів комп'ютера, так і системи в цілому. З їх допомогою можна виявити можливі або наявні проблеми в системі. Програми такого типу призначені для перевірки температури певних комплектуючих (процесора, відеокарти тощо), вольтажу, перевірки версії драйверів, завантаженості системних папок та наявності непотрібного софту. Деякі з подібних програм можуть давати свою оцінну думку про стан системи на основі всієї отриманої інформації. Також деякі програми мають власні алгоритми тестування системи, що дозволяють подивитися як вона поведеться в різних сценаріях використання. Додатково в цій категорії можна виділити вузькоспрямовані програми, завдання яких виконати докладну діагностику якогось одного системного компонента або групи таких компонентів, наприклад оперативної пам'яті, процесора, відеоадаптерів тощо.

Список літератури

1. Данилевич Р.І. Моделювання алгоритмів планування процесорного часу для багатопроцесорних систем / Р.І.Данилевич, В.І.Панченко // Інформаційні технології: наука, техніка, технологія, освіта, здоров’я: тези доповідей XXIX міжнародної науково-практичної конференції MicroCAD-2021, 18-20 травня 2021р.: у 5 ч. Ч. IV –Харків: НТУ «ХПІ», 2021. –С. 91.

СЕКЦІЯ 3
БЕЗПЕКА ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н., проф. О. А. Смірнов, ЦНТУ, Кропивницький
Секретар секції: к.т.н., доц. О. В. Сєвєрінов, ХНУРЕ, Харків

ANALYSIS OF SECURITY THREATS AND PROTECTION METHODS FOR MODERN BANKING PAYMENT SYSTEMS

Koshman S., Krasnobayev V., Rossomakha M.
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine

In today's world, electronic payment systems are an integral part of the financial infrastructure. However, the increasing number of cyberattacks and criminal activity in this sector emphasizes the need to strengthen security measures. One of the most common threats is cyberattacks on Visa and MasterCard systems. Cybercriminals can use various methods to break through the systems' security, such as phishing, viruses, trojans, DDoS attacks, and others [1, 2]. This can result in the loss of data, breaches of confidentiality, theft of money from user accounts, spread of fraud, loss of customer trust and bank reputation, and more. However, Visa and MasterCard are making significant efforts to prevent such security threats [3, 4].

The purpose of the report is to identify vulnerabilities, prevent different types of attacks, eliminate their consequences on banking payment systems, and prevent the possibility of their being hacked.

Research and analysis of literature, information on real cases of attacks on banking payment systems, have shown that to achieve the goal, the most widespread is the use of modern methods of data encryption. Data encryption provides confidentiality and protection against unauthorized access. Modern cryptographic algorithms (such as AES, RSA), the SSL/TLS secure connection protocol, and tokenization methods are used in banking payment systems to protect against hacks and ensure transaction security. Also, Visa and MasterCard use two-factor authentication (2FA), which appears in the form of a request for additional code or other information after entering the main password. This significantly increases the level of security because even if hackers break the user's password, they still cannot access the account without an additional authentication factor. The results of the work can be useful for developing proposals to increase the security of banking payment systems and prevent possible threats. The report emphasizes the need for continuous updating of protection methods and improving security measures in the world of electronic payment systems to ensure protection against potential threats.

References

1. "The security of payment systems: A survey of issues and solutions" by Ross Anderson and Steven Murdoch. (https://www.cl.cam.ac.uk/~rja14/Papers/SE-06.pdf).

2. Security Threats to Electronic Payment Systems - A Review" by S. Chandrakala and N. Kavitha. (https://www.researchgate.net/publication/322890945_Security_...)

3. "Analysis of Security Threats and Vulnerabilities in Payment Systems" by Jong-Hyuk Park, Yunsik Son, and HwaMin Lee.
(https://www.sciencedirect.com/science/article/pii/S2212017313005793)

4. "Card payment frauds in the UK and Europe" by Matteo Crippa and Francesco Saita. (https://www.sciencedirect.com/science/article/pii/S0167923604000876

IMPLEMENTATION OF THE RSA CRYPTO-ALGORITHM BASED ON A SPECIALIZED DATA PROCESSING TOOL IN THE SYSTEM OF RESIDUAL CLASSES

Koshman S., Krasnobayev V., Kinchyk A.
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine

The RSA (Rivest-Shamir-Adleman) algorithm is one of the most popular cryptographic algorithms used to ensure the security of data transmission in information systems. The conducted analysis showed that the implementation of this algorithm requires significant computing resources, therefore reducing the time of its implementation is an urgent and important task. The implementation of this task is carried out by optimizing the use of memory, using specialized processors or dividing the computing work between several devices. Various methods are used as a mathematical apparatus for the implementation of the RSA algorithm, including Montgomery's fast arithmetic and Tom and Rivest's recursive formulas. For the technical implementation of the RSA algorithm, there are specialized processors that are specifically designed to perform cryptographic operations. For example, Intel AES-NI processors that support a hardware implementation of the RSA algorithm. They speed up calculations by reducing the time required for encryption and decryption operations. But it should be noted that all these tools process data presented in the positional numbering system, which in turn does not allow parallelizing the above-mentioned algorithms at the level of microoperations [1, 2].

The purpose of the report is to reduce the implementation time of the RSA crypto-algorithm when using specialized tools for processing integer data in the system of residual classes.

The report presents specialized tools for processing integer data (STPID), which are based on the use of a non-positional system of residual classes (SRC). It is noted that the use of such STPID ensures a significant acceleration of cryptographic data processing algorithms, in particular RSA, which in turn positively affects the speed of data processing systems. It is shown that the efficiency of using SRC is conditioned by such properties as independence, low-bit and equality of residues. At the same time, the representation of input data in the form of low-bit residues ensures an increase in the performance of the RSA algorithm implementation based on the use of existing methods. The conducted research showed that this approach to the construction of STPID allows to increase the efficiency of the RSA algorithm implementation.

References

1. Frank M. Groom, Kevin Groom, Stephan S. Jones Network and Data Security for Non-Engineers. 2016, p. 81-86. DOI: 10.1201/9781315381138

2. Bushra S., Farheen S. Comparison Between RSA Algorithm and Modified RSA Algorithm Used in Cloud Computing 2019, p. 218-224. DOI: 10.1007/978-3-030-33846-6_24

ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ТА АВТОРИЗАЦІЯ КОРИСТУВАЧА У ВЕБ-ДОДАТКУ

Птащенко Т.В., Олешко І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В даний час автентифікація є важливою процедурою для забезпечення захисту інформації користувачів у будь-яких системах. Механізми автентифікації та авторизації широко використовуються для захисту мережевих аккаунтів, у системах електронного документообігу, банківських картках та у різноманітних веб-додатках. Для забезпечення більш надійного рівня безпеки у веб-додатках з критичною інформацією може використовуватись багатофакторна автентифікація, яка вимагає від користувача надання двох або більше факторів для підтвердження особистості [1, 2].

Метою доповіді є реалізація процедури двофакторної автентифікації користувача у веб-додатку. Були розглянуті питання щодо управління доступом користувачів до різних функцій додатку за допомогою використання процедури авторизації. В доповіді також наводяться принципи роботи двофакторної автентифікації на основі пароля та одноразового коду, який генерується мобільним додатком. Під час реалізації використовувалась мова програмування TypeScript/JavaScript в середовищі виконання NodeJS.

Результати дослідження показали, що використання двофакторної автентифікації та авторизація є ефективними заходами для забезпечення безпеки веб-додатків та захисту користувачів від кібератак [3, 4].

У роботі було розроблено веб-додаток з двофакторною автентифікацією та авторизацією. Такі механізми захисту використовуються у веб-додатках, які містять конфіденційні дані та особливо критичну інформацію.

Список літератури

1. O. Ayoade, A. S. Afolabi, A. T. Awelewa, "A Review of Two Factor Authentication", International Journal of Computer Science and Information Security, vol. 16, no. 6, pp. 35-42, 2018.

2. Сєвєрінов О.В., Кліпоносова В.С. Автентифікації користувачів веб-ресурсів, НТУ «ХПІ», 2022.

3. T. Upadhyay, N. L. Kumar, "Two Factor Authentication: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 8, no. 3, pp. 38-44, 2018.

4. M. H. Hamza, "Design and Implementation of Web-based Role-based Access Control System", Int. Journal of Computer Applications, vol. 67, no. 11, pp. 26-30, 2013.

АЛГОРИТМ ЦИФРОВОГО ПІДПИСУ НА БАЗІ ТРИВИМІРНИХ ЕЛІПТИЧНИХ КРИВИХ

Щербакова Ю.А.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

У 21 сторіччі інформаційні технології опанували майже всі сфери життєдіяльності. Захист інформації є необхідною складовою цього процесу. Одним з головних методів аутентифікації є ЕЦП (електронний цифровий підпис) [1]. У даний час стандартом ЕЦП є алгоритм ECDSA [2], який базується на еліптичних кривих [3]. NIST рекомендує 15 еліптичних кривих. Ці еліптичні криві обрані, не лише завдяки високому рівню безпеки, але й з урахуванням ефективності програмної реалізації. 25 років тому реалізація алгоритму DSA на базі еліптичних кривих збільшила криптостійкість цього алгоритму вдвічі, що дозволило вдвічі зменшити довжину секретного ключа (з 256 до 128 біт). Швидкість реалізації алгоритму при цьому зменшилась майже у тричі, а рівень безпеки не змінився. За минулий час швидкодія обладнання зросла і, відповідно, зросла необхідність подовжити ключ до 256 біт та більше.

В доповіді розглянуто наступний крок для удосконалення алгоритму ECDSA. А саме, його реалізація на багатовимірних еліптичних кривих. Як відомо, еліптична крива у полі Галуа має вигляд скінченного набору точок.

Для визначення цих точок кожного елементу декартового добутку $x_1 \times x_2 \times ... \times x_n$ обчислимо

$$y^2 = (X^3 + BX + C) \bmod p,$$

де $X = [x_1\ x_2\ ...\ x_n]$; $B = [b_1\ b_2\ ...\ b_n]$; $C = [c_1\ c_2\ ...\ c_n]$; **p** – порядок поля Галуа точок відповідної еліптичної кривої, та визначимо $\forall y \in [0, p-1]$, чи є вони квадратичними лишками по модулю **p.**

По розрахунках, для двох- та трьох-вимірних кривих отримаємо кількість точок за різних значень порядку **p**:

p	**n = 2**	**n = 3**
17	13	272
97	100	9507
997	982	15707

Отже, криптостійкість істотно збільшилась. Для подальшого впровадження цих кривих.

Список літератури

1. Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису. URL: https://regulation.gov.ua/documents/id29825

2. ДСТУ ETSI TS 119 102-2:2022 Електронні підписи та інфраструктури (ESI). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=98923

3. Koblitz N. Introduction to Elliptic Curves and Modular Forms. Springer, New York, NY, 1993. 252 p. DOI: 10.1007/978-1-4612-0909-6.

ANTIVIRUS SOLUTIONS AND THEIR VARIATIONS: EDR, MDM, SIEM

Yevheniev A.M., Shulika K.M.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Antivirus solutions have long become an integral part of the modern cyber world. They help protect computers and networks from malicious software and other threats. However, with the development of technologies, many variations of antivirus protection have emerged, including EDR, MDM, and SIEM [1, 2].

The purpose of the report is to analyze each of these options, their features, and benefits.

EDR is an endpoint protection technology that includes monitoring, detection, response to threats, and recovery after incidents. It extends the capabilities of traditional antivirus products by adding advanced analysis and tracking of anomalous behavior on user devices. EDR provides companies with the ability to detect new attacks that have bypassed traditional antivirus products and quickly respond to security incidents [1].

MDM is a mobile device management system that allows organizations to control access to corporate resources, security settings, installation of antivirus programs, and updates on employees' mobile devices. Using MDM helps to increase the level of protection for mobile devices and reduce the risk of data loss or theft.

SIEM is a comprehensive solution for monitoring, analyzing, and managing IT infrastructure security. It collects and analyzes data from various sources, such as antivirus programs, firewalls, intrusion detection systems, and other security tools. SIEM is used to detect anomalies, track changes in the network, and correlate events for early detection and response to cyberattacks.

Modern antivirus solutions and their variations, such as EDR, MDM, and SIEM, provide different levels of protection against cyber threats. Using these technologies helps organizations protect their infrastructure, data, and users from malicious software and other malicious actions. However, it is important to understand that there is no universal solution that would provide complete protection against all types of threats [3, 4]. Therefore, it is essential to use a comprehensive approach to security, which includes various technologies, products, and practices to adequately respond to constantly changing threats in cyberspace.

References

1. Antonishchev, V. V., & Kravchenko, A. V. (2020). Analysis of antivirus technologies for corporate networks. Bulletin of V. N. Karazin Kharkiv National University. Series "Radiophysics and Computer Systems", (22), 101-106.

2. Gerasimov, V. O. (2019). Methods and technologies for protection against malicious software. Cybersecurity: education, science, technology, 2(6), 36-46.

3. Rostyslav G., Martovytskyi V., Sievierinov O., Sukhoteplyj V., Soloviova O., Kortyak Y. (2020). A Method for Identifying and Countering HID Attacks-Virus Detection in BMP Images. International Journal of Emerging Trends in Engineering Research, Volume 8, (7).

4. Sievierinov O., Ovcharenko M., Vlasov A. (2021). Enterprise Security Operations Center. COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES.

АНАЛІЗ І ПОРІВНЯННЯ ІДЕНТИФІКАЦІЇ ОСОБИ ЗА РАЙДУЖНОЮ ОБОЛОНКОЮ ОКА

Євгеньєв А.М., Єнальєва Г.С., Тельнова А.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Автентифікація є процесом верифікації особистості з метою надання доступу до тієї чи іншої інформації, її носіїв та джерел. У наш час виділяють три основні фактори автентифікації: володіння, знання та властивості. Фактор властивості також носить назву біометричного фактору автентифікації. Таким чином, до даного фактору можна віднести такі унікальні характеристики людини, як ДНК, геометрія руки, відбиток пальця чи долоні, голос, сітківка очей та їх райдужна оболонка [1].

Об'єктом проведеного дослідження є автентифікація людини за райдужною оболонкою ока.

У ході проведеного аналізу і порівняння було виявлено, що системи біометричної автентифікації, які побудовані за принципом сканування райдужної оболонки ока, мають найнижчий показник помилкових спрацьовувань серед усіх способів біометричної автентифікації. Цей показник становить лише 1,8% від усіх випробувань, з чого можна зробити висновок, що даний метод автентифікації має високу точність. Також, очевидним виявився факт, що даний метод автентифікації має характеристики стабільності і відносної безпечності, оскільки оболонка ока є унікальною і протягом повного життєвого циклу не змінюється.

Результатом порівняння способів біометричної автентифікації став висновок, що, на відміну від автентифікації за допомогою сканування відбитків пальців, долоні чи руки в цілому, автентифікація за скануванням райдужної оболонки є гігієнічним методом, бо не потребує прямого або близького контакту для ідентифікації, та здатна попереджати шахрайство, завдяки особливості розпізнавання руху ока [3].

Це означає, що у разі, якщо людина знаходиться у безсвідомому стані, ідентифікація не підтвердиться. Головним, і єдиним виявленим у ході проведеного дослідження, недоліком виявилася висока вартість приладів, що здатні здійснювати автентифікацію особи за райдужною оболонкою ока.

Список літератури

1. Коваль Л.Г, Злепко С.М., Новіцький Г.М., Крекотень Є.Г. Вчені записки ТНУ імені В.І. Вернадського. 2019. Т. 30(69), № 2. С. 104. https://www.tech.vernadskyjournals.in.ua-/journals/2019/2_2019/part_1/19.pdf

2. Кліпоносова В.С., Сєвєрінов О.В. Сучасні методи біометричної ідентифікації та автентифікації користувачів. ВА ЗС АР; НТУ" ХПІ"; НАУ, ДП" ПДПРОНДІАВІАПРОМ"; УмЖ, 2021.

3. Daugman, J. G. How iris recognition works. IEEE transactions on circuits and systems for video technology. 2004. Т. 14, №1. С. 21-30.

ФІШИНГОВІ АТАКИ І МЕТОДИ ЗАХИСТУ ВІД НИХ

Євгеньєв А.М., Гальченко А.І., Риков Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

На даний час кількість інформації, що циркулює в інформаційних мережах постійно зростає. Також зростає й кількість атак, що здійснюються на системи захисту інформації цих мереж [1].

Фішингові атаки залишаються досить актуальними і складними для боротьби з ними. Шахраї постійно змінюють свої методи та підходи, щоб обійти заходи захисту.

Метою доповіді є дослідження ефективності існуючих методів захисту від фішингових атак.

В доповіді наводяться основні методи фішингових атак [2].

Спілкування з вимогами. Шахраї можуть вимагати надіслати гроші або іншу конфіденційну інформацію, погрожуючи певними наслідками, якщо не підкоритися їх вимогам.

Атаки "від імені офіційних осіб". Шахраї можуть використовувати фальшиві електронні адреси або імена відомих компаній або осіб, щоб виглядати більш довірливо та переконати жертву надіслати конфіденційну інформацію.

Соціальний інжиніринг**.** Шахраї можуть використовувати персональну інформацію жертви.

Основними методами захисту від атак такого типу можна виділити наступні [3]:

- ніколи не надсилати конфіденційну інформацію, якщо не впевнені, що отримувач є довіреною особою;
- перевіряти електронну адресу, від якої прийшло повідомлення. Якщо вона виглядає підозріло, не відкривати повідомлення;
- ніколи не відкривати посилання в електронних повідомленнях або соціальних мережах, якщо вони виглядають підозріло;
- необхідно використовувати програмне забезпечення для захисту від шахрайства, таке як антивірус та антишпигунська програма.

Фішингові атаки залишаються досить актуальними і складними для боротьби з ними. Тому важливо постійно оновлювати свої знання про фішинг та використовувати заходи захисту від шахрайства, щоб зменшити ризик стати жертвою фішингової атаки.

Список літератури

1. Голубничий Д.Ю., Сєвєрінов О.В., Коломійцев О.В., Місюра О.М., Третяк В.Ф., Власов А.В., Крук Б.М. Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації, 2021.

2. М. Ліндстрем, Я. Стрікер. "Фішингові атаки: підходи та методи боротьби". Видавництво "Логос", 2018 рік.

3. Jakobsson, M., & Myers, S. (2016). "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft". Wiley.

ДОКАЗИ ІЗ НУЛЬОВИМИ ЗНАННЯМИ НА БАЗІ ДЕРЕВ МЕРКЛА

Гаража Р.Ю., Мельникова О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Доказ із нульовими знаннями (з нульовим розголошенням) — тип доказу, який дозволяє одній стороні довести істинність певного твердження іншій стороні без розкриття будь-якої іншої інформації, крім істинності цього твердження. Можливими способами застосування доказів із нульовими знаннями є анонімні онлайн-голосування, цифрові ідентифікаційні документи, блокчейн, тощо.

Метою доповіді є аналіз можливостей застосування дерев Меркла для забезпечення надійності доказів із нульовими знаннями. В доповіді розглянуто структуру та механізм побудови дерева Меркла та проаналізовано його властивості, корисні для реалізації саме протоколів доказу з нульовими знаннями. Аналізуються різні групи доказів із нульовими знаннями (інтерактивні та неінтерактивні).

У випадку з онлайн-голосуваннями дерево Меркла може бути утвореним списком користувачів, що мають право голосувати. Дерево Меркла цифрового ідентифікаційного документу, в свою чергу, може включати ім'я та прізвище, дату народження, стать, особистий податковий номер, тощо. Блокчейн може бути використаний у якості довіреної сторони, що зберігає корені дерев Меркла розподіленим чином, гарантуючи доступність цих даних для сторони, що перевіряє, тобто для безпосереднього залучення у конкретних випадках застосування доказів із нульовими знаннями на базі дерев Меркла.

Щоб підтвердити факт входження певного блоку даних до дерева Меркла або факт володіння даними, що утворюють дерево Меркла, як такий, сторона, що доводить, має надати стороні, що перевіряє, листок (або певний блок даних, якщо це необхідно) та ті мінімально необхідні вузли дерева, що потрібні для розрахунку кореня дерева. Дерево Меркла для такої перевірки зазвичай доступне публічно або надається третьою довіреною стороною (trusted third party).

Проведений аналіз показав, що дерево Меркла є надійним засобом реалізації доказів із нульовими знаннями як таких, що гарантує нерозголошення зайвої інформації, високу масштабованість, невеликий час перевірки та розмір доказу. Дерево Меркла знайшло своє застосування для перевірки справжності й цілісності даних, що зберігаються, обробляються та передаються у peer-to-peer мережах (наприклад, BitTorrent та IPFS).

Список літератури

1. What is a zero-knowledge proof and why is it useful? [Електронний ресурс] / Режим доступу: https://www.expressvpn.com/blog/zero-knowledge-proofs-explained/;
2. Merkle tree patent. [Електронний ресурс] / Режим доступу: https://patents.google.com/patent/US4309569.

ПРИШВИДШЕННЯ ЛІНІЙНИХ ПЕРЕТВОРЕНЬ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУ "КАЛИНА"

Мельникова О.А., Стефаниць Е.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні симетричні шифри мають забезпечувати високу швидкість обробки великих обсягів інформації в режимі реального часу. Тому важливим завданням є зменшення обчислювальної складності як базових перетворень шифру (прямого та зворотного) в цілому, так і окремих елементарних перетворень.

Метою доповіді є аналіз можливостей зменшення обчислювальної складності прямого та зворотного лінійних перетворень (перемішувань) змісту стовпців матриці внутрішнього стану для вітчизняного блокового симетричного шифру “Калина” [1, 2].

У доповіді розглянуто як варіанти швидкого виконання базової для вищезгаданих лінійних перетворень операції множення за модулем елементів поля $GF(2^m)$, побудованого за модулем $f(t) = t^8 + t^4 + t^3 + t^2 + 1$, так і різні варіанти реалізації лінійних перетворень в цілому. Зокрема, пропонується використання індексованих таблиць підстановок замість операції множення за модулем елементів поля $GF(2^8)$ та аналізується обчислювальна складність таких варіантів реалізації лінійних перетворень.

Для досягнення максимальної швидкості виконання прямого лінійного перетворення необхідне попереднє обчислення та зберігання таблиці підстановок із 1536 елементів поля, а також використання додаткового індексного масиву із 64 елементів. А для зворотного лінійного перетворення необхідно сформувати таблицю підстановок із 2048 елементів поля та використовувати додатковий індексний масив із 64 елементів.

В доповіді аналізується обчислювальна складність розглянутих варіантів реалізації прямого та зворотного лінійних перетворень і наводяться результати експериментальних вимірювань обчислювальної складності (часу виконання, в тактах процесора). Проведені дослідження показали, що використання запропонованого варіанту індексованих таблиць підстановок дозволяє значно зменшити обчислювальну складність прямого та зворотного лінійних перетворень.

Список літератури

1. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Текст]. — Введ. 01-07-2015. — К. : Мінекономрозвитку України, 2015.

2. Горбенко І. Д. Симетричний блоковий шифр "Калина” — новий національний стандарт України / І. Д. Горбенко, Р. В. Олійников, О. В. Казимиров, В. І. Руженцев, О. О. Кузнєцов, Ю. І. Горбенко, О. В. Дирда, В. І. Долгов, А. І. Пушкарьов, Р. І. Мордвінов // Радіотехніка. - 2015. - Вип. 181. - С. 5-22. - Режим доступу: http://nbuv.gov.ua/UJRN/rvmnts_2015_181_3.

ВИКОРИСТАННЯ ПРЕДСТАВЛЕНЬ ПО МНОЖИННИМ ОСНОВАМ В ЕЛІПТИЧНІЙ КРИПТОГРАФІЇ

Кузнецов О.В., Гапіченко А.М., Мельникова О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Системи захисту інформації зазвичай мають функціонувати в режимі реального часу. При застосуванні криптографічних алгоритмів, які використовують перетворення в групах точок еліптичних кривих (ЕК), найбільший час витрачається на операції еліптичного скалярного множення (однократного або одночасного двократного). Тому важливим питанням є зменшення обчислювальної складності саме цих операцій. Одним із підходів до зменшення обчислювальної складності криптографічних алгоритмів, які використовують багаторозрядні значення, є застосування нестандартних форм їх представлення. **Метою доповіді є** аналіз методів еліптичного скалярного множення з використанням представлень багаторозрядних значень по множинним основам (зокрема, по подвійним). Більш детально розглянуто метод представлення по подвійним основам із використанням направленого ациклічного графу.

Направлений (орієнтований) ациклічний граф (DAG) — випадок орієнтованого графу, в якому відсутні орієнтовані цикли. Тобто відсутні шляхи, що починаються і закінчуються в одній і тій самій вершині. В роботі [1] було запропоновано метод, заснований на DAG, для представлення чисел по подвійним основам. Основною метою цього методу є пошук ланцюга, оптимального за вагою. Ідея методу на основі DAG полягає в тому, щоб створити таблицю зі стовпцями й рядками, які містять значення основ.

Однією з переваг є нижча оцінка обчислювальної складності у порівнянні з іншими методами представлення чисел, а саме $O = (\log n)^{2.5+o(1)}$, де n — ціле додатне число. Наприклад, алгоритм представлення запропонований у [2], має обчислювальну складність $O = (\log n)^{4+o(1)}$. Для стандартного алгоритму [3], вказано обчислювальну складність $O = (\log n)^{5+o(1)}$.

Проведений аналіз показав, що методи формування представлень багаторозрядних чисел по подвійним основам, у яких використовуються графи, є перспективним напрямком, але для отримання практичних реалізацій потребують значного обсягу додаткових експериментальних досліджень.

Список літератури

1.Bernstein D. Double-base scalar multiplication revisited / D. Bernstein, C. Chuengsatiansup, T. Lange. // Cryptology ePrint Archive. — 2017. — № 37.

2.Alex Capunay, Nicolas Th´eriault / Computing optimal 2-3 chains for pairings, Latincrypt. —2015. — pp. 225 - 244.

3.Dimitrov V. S. The Double-Base Number System And Its Application to Elliptic Curve Cryptography / V. S. Dimitrov, L. Imbert, P. K. Mishra. // Mathematics of Computation. — 2008. — № 262. — pp. 1075 - 1104.

ПОСТКВАНТОВІ АЛГОРИТМИ НА АЛГЕБРАГІЧНИХ РЕШІТКАХ. АЛГОРИТМ CRYSTALS-KYBER

Скибенко М.С., Долинський В.М.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасному світі швидкістю та ефективністю обчислювання традиційних криптографічних алгоритмів, квантові комп'ютери значно перевищують класичні комп'ютерні архітектури, в результаті чого, криптографічні системи стають потенційно вразливими для криптографічних атак. Постквантові конструкції здатні врятувати криптографічний світ від квантових нападів.

Метою доповіді є розгляд алгоритму Crystals-Kyber, його властивостей та постквантових алгоритмів на алгебраїчних решітках в цілому, аналіз Kyber, як механізму захисту CPS (Cyber-Physical Systems) [1].

Kyber - це захищений є від IND-CCA2 (негнучкості для адаптивних атак на основі підібраного шифротексту) механізм інкапсуляції ключів, захист якого базується на складності вирішення проблеми навчання з помилками (LWE - Learning With Errors) над решітчастими модулями. Kyber є кандидатом на стандартизацію Національним інститутом стандартів і технологій (NIST).

В роботі проведені дослідження алгебрагічних решіток [2]. Решітка складається з набору точок у n-вимірному просторі з періодичною структурою. За допомогою n-лінійно незалежних векторів будь-яка точка цієї структури може бути відтворена. Безпека криптографічних примітивів на основі решітки базуються на NP-складних проблемах високовимірних решіток, наприклад, проблема найкоротшого вектора (SVP).

В ході досліджень як механізму захисту CPS Kyber показав дуже високу продуктивність на всіх оцінених рівнях безпеки CPS [2, 3]. Оскільки промислові кіберфізичні системи (CPS) зазвичай розгортаються десятиліттями, захист від довгострокових загроз є необхідністю [4].

Таким чином, Crystals-Kyber – побудований за допомогою алгебраїчних решіток механізм інкапсуляції ключів, що демонструє себе як ефективний механізм захисту CPS.

Список літератури

1. Roberto Avanzi, Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schank, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber. NIST PQC Standardization: Round 2., 2019

2. Sebastian Paul, Patrik Scheible, Friedrich Wiemer. Towards Post-Quantum Security for Cyber-Physical Systems: Integrating PQC into Industrial M2M Communication. Paul, Scheible, and Wiemer, 2021.

3. Petrenko, O. E., Petrenko, O. S., Sievierinov, O. V., Fiediushyn, O. I., Zubrych, A. V., & Shcherbina, D. V. (2021). Аналіз шляхів підвищення стійкості криптоалгоритмів на алгебраїчних решітках щодо часових атак. Radiotekhnika, (207), 59-65.

4. Edward A. Lee, Sanjit A. Seshia. An Introductory Textbook on Cyber-Physical Systems. University of California, Berkeley, USA. 2010.

БЕЗПЕЧНЕ ПІДКЛЮЧЕННЯ МОБІЛЬНИХ ПРИСТРОЇВ ДО КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТУНЕЛЮ VPN

Сердюков Д.В., Сєвєрінов О.В., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Останнім часом все більше мобільні пристрої використовуються не тільки для повсякденних цілей, а і для виконання професійних завдань організацій та підприємств. Залежно від того, як організація використовує пристрої, несанкціонований доступ до смартфону, планшета або іншого пристрою може призвести до кіберінциденту, пов'язаного зі всією інформаційною системою організації [1, 2].

Метою доповіді є аналіз можливостей використання тунелю VPN для захисту корпоративної інформації на мобільних пристроях, які використовуються для доступу до комп'ютерної мережі установи.

Проведений аналіз основних методів захисту мобільних пристроїв. Одним з найбільш ефективних способів захисту інформації від несанкціонованого доступу є використання тунелю VPN. Співробітники підключаються до VPN щоразу з отриманням доступу до корпоративних даних. Цей тунель дозволяє захистити трафік від несанкціонованого доступу та прослуховування.

В доповіді розглянуті обмеження та недоліки сервісу VPN. А також виконана оцінка ризиків щодо інформаційної безпеки та заходи щодо обробки їх [2]. Однак, VPN не є панацеєю в усіх випадках. Крім того, при низькій пропускній здатності або ненадійному зв'язку у мережі, можуть виникати складності з обробкою даних через VPN канал. Іншим недоліком є можливість злому системи безпеки, що відбувається, якщо зловмисники отримають доступ до тунелю VPN. Тому, для забезпечення максимального рівня безпеки, пропонується використовувати VPN-системи з багатофакторною автентифікацією, які вимагають від користувачів введення додаткового пароля, або використання біометричних методів ідентифікації.

Загалом, використання тунелю VPN для підключення мобільних пристроїв до інформаційної системи організації дозволяє забезпечити захист даних та знизити ризики інформаційної системи.

Варто пам'ятати, що це не є єдиним засобом забезпечення безпеки і вимагає постійного контролю і підтримки.

Список літератури

1. Сєвєрінов О., Федорченко В., Перепадя В. Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків. Системи озброєння і військова техніка 4 (2016): 42-45.

2. Северинов А.В., Черныш, В.И. Анализ угроз и рисков безопасности информации в беспроводных сетях. // Системи управління, навігації та зв'язку.– Вип, 1, 229-232.

3. Why VPNs on mobile devices are a crucial part of securing access to corporate data - ManageEngine Blog. ManageEngine Blog. DOI: https://cutt.ly/V41SZjN (date of access: 30.03.2023).

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД ЗАГРОЗИ CVE-2020-1472

Сєвєрінов О.В., Федоров І.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Використання служби каталогів Active Directory (AD) має вирішальне значення для безпеки інформаційних систем багатьох підприємств. Можливі атаки на вразливості AD можуть мати серйозні наслідки для безпеки організації [1].

Одна з таких вразливостей - CVE-2020-1472, також відома як Zerologon, дозволяє зловмиснику зламати механізм автентифікації в службі AD [2]. Тому актуальним напрямом є розгляд методів захисту від атак через вразливість CVE-2020-1472.

Метою доповіді є аналіз методів захисту від вразливості CVE-2020-1472, які допоможуть знизити ризик зламу контролера домену Active Directory.

Проведений аналіз показав, що одним з методів захисту є використання надійних паролів, чітка політика безпеки стосовно паролів в організації. Другим засобом є використання багатофакторних методів автентифікації для підвищення рівня захисту. Необхідно також своєчасно встановлювати патчі Microsoft для оновлення безпеки.

Одним з основних методів захисту є застосування систем виявлення вторгнень (IDS) для протидії та повідомлення про системні атаки [3, 4]. Необхідно використовувати рішення для моніторингу подій, які дозволяють відстежувати й аналізувати системні журнали, щоб своєчасно виявляти незвичні події та підозрілі дії. Детектори вторгнень забезпечать захист від відомих атак, а також дозволять виявляти аномалії, які можуть бути пов'язані з новими атаками, про які можуть знати лише експерти з безпеки.

Регулярні перевірки безпеки в інформаційній системі організації дозволить виявити потенційні слабкі місця в системі захисту.

Таким чином, використання інструментів моніторингу подій і детекторів вторгнень може допомогти виявити атаки на контролер домену та зменшити ризики. Однак для ефективного використання цих інструментів необхідні правильні налаштування та належна підтримка експертів інформаційної безпеки.

Список літератури

1. Сєвєрінов О. В., Хрєнов А. Г. Аналіз сучасних систем виявлення вторгнень //Системи обробки інформації. – 2014. – №. 6. – С. 122-124.

2. Netlogon Elevation of Privilege Vulnerability CVE-2020-1472 [Електронний ресурс] – Режим доступу: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472.

3. Intrusion Detection System (IDS) [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/intrusion-detection-system-ids.

4. Федоров І.А., Сєвєрінов О.В. Виявлення загрози CVE-2020-1472 за допомогою IDS/IPS SNORT, НТУ «ХПІ», 2022.

РЕАЛІЗАЦІЯ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ФАЙЛУ-КЛЮЧА ДЛЯ СИСТЕМИ КЕРУВАННЯ ВЕБСАЙТАМИ WORDPRESS

Коломійцев С.О., Сєвєрінов О.В., Власов А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

З кожним роком зростає популярність та кількість веб-ресурсів, а тому кількість інформації з якою вони взаємодіють стає все більшою. Також все збільшується кількість систем управління контентом веб-ресурсів.

За даними компанії W3Techs, що займається веденням статистики різних технологій в мережі Інтернет, станом на початок 2023 року, на системі WordPress працює 43% всіх сайтів в інтернеті. Цей відсоток постійно зростає. Найближчий конкурент Shopify має долю лише в 3.8% [1].

Зважаючи на цю популярність, зловмисники приділяють WordPress особливу увагу. Існує безліч програм орієнтованих на злам таких сайтів. Враховуючи відносну простоту реалізації та ефективність, одні з популярних типів атак на дану систему – це атака грубої сили і атака зі словником [2, 3]. Без використання на сайті додаткового програмного забезпечення (плагінів), успішність атак даного типу у більшості випадків залишається питанням часу.

Для системи WordPress реалізовано безліч плагінів, що надають типові методи двофакторної автентифікації [4]. Але вони мають певні недоліки та незручності, найбільші з яких – це необхідність у наявності під рукою мобільного пристрою зі стабільним рівнем сигналу мережі або мобільного інтернету. А також залежність від сторонніх сервісів.

Метою роботи було реалізувати досі не існуючого для WordPress методу двофакторної автентифікації, який зможе поєднати в собі такі властивості як зручність та ефективність.

Розроблений плагін надає власнику вебсайта можливість обрати будь який файл на своєму комп'ютері і перетворити його у персональний ключ, завдяки якому і буде здійснюватись додаткова ідентифікація користувача в системі. В основі лежить використання криптографічних геш-функцій, отримання геш-значення файлу і порівняння його з еталоним геш-значенням що зберігається на сайті.

Список літератури

1. W3Techs statistic URL: https://w3techs.com/technologies/details/cm-wordpress (дата звернення: 31.03.2023).
2. Д'якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних веб-ресурсів, НТУ «ХПІ», 2022.
3. Brute Force Attac URL: https://crashtest-security.com/brute-force-attacks/ (дата звернення: 31.03.2023).
4. Authentication. URL: http://www.webopedia.com/TERM/A/authentication.html (дата звернення: 31.03.2023).

ЗАХИСТ МЕРЕЖІ НА ОСНОВІ БРАНДМАУЕРІВ NGFW

Москвін К.С., Севєрінов О.В., Федоров І.А.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі, де технології стають все більш складними та розповсюдженими, захист мережі стає вкрай важливим завданням для будь-якої компанії або організації. Кількість атак на інформацію, що зберігається, обробляється та передається у мережах постійно зростає [1].

Наступне покоління брандмауерів, так звані NGFW, забезпечують високий рівень безпеки та мають декілька переваг порівняно з традиційними рішеннями [2]. **Метою доповіді є** аналіз принципів роботи засобів NGFW, їх переваги порівняно з традиційними брандмауерами та іншими рішеннями, а також недоліки, які слід враховувати при розгляді вибору захисту мережі.

NGFW працює на основі пакетного аналізу та застосовує цілу низку технологій, таких як DPI (глибокий пакетний інспектор), IPS (система запобігання вторгнень) та VPN (віртуальні приватні мережі), для забезпечення безпеки мережі [3].

Проведений аналіз показав, що NGFW має декілька переваг порівняно з іншими рішеннями захисту мережі. NGFW забезпечує більш високий рівень безпеки мережі, оскільки використовує більш складні технології, щоб виявляти й блокувати небезпечний трафік. По-друге, NGFW має більш широкий функціонал, який дозволяє забезпечити не тільки захист від вторгнень, а й захист від шкідливих застосунків, сайтів та фішингових атак. Також NGFW може обробляти більш великі обсяги трафіку, що дозволяє забезпечити більш високу продуктивність мережі, що в свою чергу забезпечує кращий досвід користувача. NGFW має більш гнучкі настройки, що дозволяє адміністраторам мережі налаштувати правила захисту мережі залежно від потреб організації.

Таким чином, використання брандмауерів NGFW може забезпечити більш глибокий та розширений захист за рахунок використання функцій, таких як контроль доступу до додатків, захист від загроз інтелектуальних атак та більш точні фільтри. NGFW також може бути більш ефективним у виявленні і запобіганні атакам через використання аналізу пакетів та поведінки користувачів.

Список літератури

1. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі // Системи обробки інформації, 9 (2015). – С. 101-104.

2. Терентьєв О., Горбатюк Є., Лященко Т., Кузьмінський О. Брандмауери нового покоління: дослідження історії розвитку // Управління розвитком складних систем, (45), 2021. – С. 102-106.

3. Гура Д.Ю. Програмний комплекс захисту мережевого периметру інформаційно-комунікаційної системи підприємства, 2021.

ГОМОМОРФНЕ ШИФРУВАННЯ В ХМАРНИХ ОБЧИСЛЕННЯХ

Азаренко А.П., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Хмарні обчислення стали невід'ємною складовою сучасного світу і дозволяють користувачам зберігати та обробляти великі обсяги даних без необхідності у власних комп'ютерах [1]. **Метою доповіді** є дослідження можливостей використання гомоморфних методів шифрування з метою покращення надійності захисту конфіденційних даних у хмарному середовищі, а саме: аналіз існуючих алгоритмів повністю гомоморфного шифрування; визначення поняття криптостійкості, коректності та компактності для гомоморфних систем; оцінка криптостійкості повних гомоморфних систем; визначення перспектив використання гомоморфного шифрування в хмарних обчисленнях.

Гомоморфне шифрування є методом шифрування даних, який дозволяє проводити операції з зашифрованими даними не розшифровуючи їх. Це дозволяє зберігати конфіденційні дані в безпеці, навіть коли вони перебувають в публічному хмарному середовищі [2]. В доповіді наведені результати дослідження різних методів гомоморфного шифрування, таких як повне гомоморфне шифрування та часткове гомоморфне шифрування, результати порівняльного аналізу ефективності застосування цих методів в хмарних обчисленнях.

Повні гомоморфні системи в хмарних обчисленнях повинні забезпечувати високий рівень криптографічної стійкості за допомогою криптографічних методів та протоколів, які забезпечують захист від різних видів атак, таких як: атаки типу залежність від контексту, атаки на основі розкриття ключів, атаки на основі перехоплення інформації та інших. Гомоморфне шифрування має кілька переваг для хмарних обчислень, зокрема, збереження конфіденційності, зменшення ризику витоку даних, менша потреба в пропускній здатності та забезпечення безпеки даних [3]. Попри потенційні переваги, гомоморфне шифрування все ще є відносно новою технологією і має обмеження. Також воно може бути повільним і вимогливим до ресурсів, що може бути проблемою обробки великих обсягів даних.

Список літератури

1. Carlin, S., Curran, K. Cloud Computing Security. International Journal of Ambient Computing and Intelligence. 2011. Vol. 3, No. 1. P. 14-19. DOI: https://doi.org/10.4018/jaci.2011010102.

2. Gentry C. A fully homomorphic encryption scheme. Ph.D. Thesis. 2009. 199 p.

3. Lauter, K., Naehrig, M., Vaikuntanathan, V. Can Homomorphic Encryption be Practical? CCSW'11, Chicago, USA. 2011. P. 113-124. Available at: https://eprint.iacr.org/2011/405.pdf (accessed 23.03.2023).

СИСТЕМИ УПРАВЛІННЯ НА ОСНОВІ БЕЗДРОТОВИХ МЕРЕЖ ТА АНАЛІЗ ЇХ ВРАЗЛИВОСТЕЙ

Соболь Д.Ю., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Існує безліч бездротових технологій, найчастіше відомих за назвами, такими як Wi-Fi, Near Field Communication (NFC), Bluetooth, супутниковий зв'язок [1, 2]. Кожна технологія має певні характеристики, які визначаються її сферою застосування. Незважаючи на свій постійний розвиток, дані мережі мають безліч прогалин у системі безпеки, що дозволяє зловмисникам здійснювати перехоплення інформації. **Метою доповіді** є дослідження та аналіз використання бездротових мереж у глобальному суспільстві.

Однією з найпопулярніших бездротових мереж є Wi-Fi. Wi-Fi використовується для передачі даних на короткі відстані та забезпечення доступу до Інтернету. Ще однією поширеною технологією бездротового зв'язку є NFC. NFC використовується для передачі даних на дуже короткі відстані, зазвичай менше 10 см. Супутниковий зв'язок – це технологія передачі даних, яка використовує супутники у космосі для зв'язку із наземною станцією. Супутниковий зв'язок використовується для передачі даних на великі відстані й у місцях, де немає доступу до проводового зв'язку. Кожна з цих бездротових технологій використовується в різних сферах життя та має свої переваги. Також кожна з цих систем має свої вразливості та недоліки, які потрібно враховувати при використанні цих технологій. В доповіді наводяться результати дослідження та аналізу всіх видів вразливостей різних типів бездротових мереж, їх протоколів безпеки. Наводяться та порівняльного аналізу криптостійкості та ефективності захисту інформації від загроз.

Аналіз публікацій за темою дослідження дає розуміння про необхідність захисту бездротових мереж, що є важливим аспектом кібербезпеки, оскільки дані, що надходять через бездротові мережі, можуть бути викрадені або пошкоджені несанкціонованим користувачем [3]. Кожен тип бездротової мережі має свої унікальні методи захисту, такі як шифрування, автентифікація та керування доступом. В результаті дослідження були запропоновані методи захисту систем управління для забезпечення захисту від таких атак як перехват трафіку, модифікація трафіку, злам та крадіжка особистих даних.

Список літератури

1. Pavur, J., Martinovic, I. Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight. *Journal of Cybersecurity*. 2022. Vol.8, Issue 1. P. 6-13. DOI: https://doi.org/10.1093/cybsec/tyac008.

2. Zbigniew Piotrowski. Will WPA3 really provide Wi-Fi security at a higher level? *Proceedings SPIE*. 2019. P. 2-11. DOI: https://doi.org/10.1117/12.2525020.

3. Северинов А.В., Черныш, В.И. Анализ угроз и рисков безопасности информации в беспроводных сетях. // Системи управління, навігації та зв'язку.– Вип, 1, 229-232.

АНАЛІЗ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ З ВИКОРИСТАННЯМ МОВИ ПРОГРАМУВАННЯ PYTHON

Євгеньєв А.М., Бичковський І.Ю., Уманець М.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Аналіз вразливостей веб-додатків є важливим етапом розробки програмного забезпечення. Він допомагає виявити потенційні недоліки та забезпечити безпеку веб-додатку [1].

Метою доповіді є аналіз сучасних методів аналізу вразливостей веб-додатків з використанням мови програмування Python.

Використання PyTesseract для аналізу CAPTCHA

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) - це тест, який розроблено для того, щоб відрізнити людей від комп'ютерів. Однак, іноді CAPTCHA може бути обійдена зловмисниками, що може призвести до вразливостей веб-додатку. PyTesseract є бібліотекою Python, яка дозволяє розпізнавати тексти на зображеннях, в тому числі і на CAPTCHA. Використовуючи PyTesseract, можна перевірити, чи може зловмисник отримати доступ до облікового запису, обійшовши CAPTCHA.

Використання Pycodestyle та Flake8 для виявлення стилевих помилок [2].

Структуроване програмування є важливим елементом розробки програмного забезпечення. Читабельний та структурований код допомагає уникнути помилок та покращує розуміння коду. Pycodestyle та Flake8 є бібліотеками Python, які дозволяють виявляти стилеві помилки в коді. Вони перевіряють стиль коду на відповідність PEP8 (Style Guide for Python Code) та надають рекомендації щодо покращення стилю коду. Використання цих бібліотек допоможе покращити якість програмного коду та забезпечити безпеку веб-додатку.

Використання бібліотеки requests для аналізу HTTP запитів [3].

HTTP запити є важливим елементом взаємодії веб-додатків. requests є бібліотекою Python, яка дозволяє виконувати HTTP запити та аналізувати їх відповіді. Використовуючи requests, можна перевірити, чи є веб-додаток вразливим до атаки, таких як SQL-ін'єкції та XSS-атаки.

Аналіз вразливостей веб-додатків є важливим етапом розробки програмного забезпечення. Використовуючи сучасні методи аналізу вразливостей з використанням Python, можна забезпечити безпеку веб-додатку та зменшити ризик вразливостей.

Список літератури

1. Д'якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних вебресурсів, НТУ «ХПІ»,. – 2022.

2. Марков, Андрій. Python для слабаків. Бібліотека пайтоніста, 2019.- Рассел, Джеймс. SQL Injection Attacks and Defense, Second Edition. Syngress, 2012.-

3. Митчелл, Стефен. Web Scraping with Python: Collecting More Data from the Modern Web. O'Reilly Media, Inc., 2018.

ЕКСПЕРИМЕНТАЛЬНЕ ВИЗНАЧЕННЯ ПРИРОДИ ДЖЕРЕЛА ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ВІДЕОТРАКТУ ЗАСОБІВ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

Євтушенко С.А., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Під час створення, модернізації та впровадження комплексів технічного захисту інформації (ТЗІ) на об'єктах електронно-обчислювальної техніки (ЕОТ) є необхідність забезпечити рівень захисту інформації встановлений вимогами нормативних документів.

Для визначення необхідних заходів захисту інформації від витоку технічними каналами проводяться спеціальні дослідження побічних електромагнітних випромінювань (ПЕМВ), при яких визначається радіус, за межами якого відношення "інформативний сигнал/шум" менше гранично допустимої величини [1]. Проводяться вимірювання і розрахунок параметрів інформативного (небезпечного) сигналу, виявляється можливість його витоку. За результатами спеціального дослідження приймається рішення про необхідність встановлення активних та/або пасивних засобів захисту [2]. Значну роль у цьому грає визначення природи джерела випромінювання ПЕМВ електричного чи магнітного. Особливо це важливо для ПЕМВ відеотракту засобів ЕОТ, як найбільш небезпечних з точки зору загроз витоку інформації.

В доповіді наводяться результати інструментальних вимірювань ПЕМВ тестових сигналів відеотрактів для різних типів моніторів дипольною та рамковою антенами.

Вимірювання проводилися на прийнятій для таких робіт відстанях (~1м). Показано, що переміщення антен вздовж лінії візування на невеликі відстані (±0,1м) достатня для впевненої реєстрації характеру зміни інтенсивності електричного і магнітного поля за законами $1/r^2$ або $1/r^3$.

Визначені закони зміни полів можуть свідчити про відповідну природу джерела ПЕМВ [3].

Список літератури

1. ТР ТЗІ – ПЕМВН-95. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93).

2. ТР ЕОТ-95. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93).

3. Пілінський В. В. Технічна електродинаміка та поширення радіохвиль: навч. пос. для студентів напряму підготовки 6.050903 «Телекомунікації» / В. В. Пілінський ; Нац. техн. ун-т України «Київ. політехн. ін-т». – Київ : Кафедра, 2014. – 336 с.

ЗАСТОСУВАННЯ МЕТОДА СТАТИСТИЧНОГО ДОСЛІДЖЕННЯ ЕНЕРГОСПОЖИВАННЯ КОМПОНЕНТА ПЕОМ У ВИЯВЛЕННІ ЗАКЛАДНИХ КОМПОНЕНТІВ У МІКРОСХЕМАХ ПЕОМ

Зайцев С.В., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Виявлення закладних пристроїв в обчислювальних компонентах ЕОМ стає все складніше з кожним поколінням чіпів, у зв'язку з ускладненням цих схем - це твердження побічно підтверджується законом Мура про збільшення кількості транзисторів, що розміщуються на кристалі інтегральної схеми, що зберігає свою працездатність [1].

Якщо розглядати стандартні для ПЕОМ центральні процесори CPU, то буде помітна очевидна деталь: їхнє енергоспоживання стає все складніше контролювати - це пов'язано з величезною, нерівномірно розподіленою за часом кількістю програмних процесів покладених на нього нинішніми неоптимізованими системами [2]. Ця деталь дозволяє зловмиснику одноразово задіяти не тільки закладену при виготовленні антену, яку ще є шанс виявити при дослідженні навколишнього середовища за допомогою радіоелектронних засобів, але й ті частини схеми чипу, що були закладені виробником. Наприклад, для її компресії, стеганографічної обробки та полегшення подальшої передачі.

Однак, подібні закладні схеми можуть значно виділятися при статистичних дослідженнях роботи ПЕОМ - на загальному графіку енергоспоживання зловмисник споживатиме помітно більше енергії в певний відрізок часу, якщо проводити порівняння поза ділянкою або з іншими користувачами зі схожими завданнями [3].

Метою доповіді є дослідження корисності статистичних спостережень над енергоспоживанням обробляючих компонентів ПЕОМ користувачів як на основі статистичних відхилень, так і на основі бази правил для виявлення зловмисника, неавторизованих чіпів та їх компонентів.

Додатковим достоїнством застосування метода статистичних спостережень є можливість досягнення позитивного результату без розборки ПЕОМ яка може знаходитися на гарантійному обслуговуванні.

Список літератури

1. Moore, Gordon E. (1965-04-19). "Cramming more components onto integrated circuits" (PDF). https://web.archive.org/web/20190327213847/ https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf (дата звернення 07.03.2023 р.).

2. List of CPU power dissipation figures. Стаття. https://en .wikipedia.org/ wiki/List_of_CPU_power_dissipation_figures(дата звернення 07.03.2023 р.).

3. Mark M. Tehranipoor. "Sensitivity Analysis to Hardware Trojans using Power Supply Transient Signals" https://www.researchgate.net/publication/4349859 (дата звернення 07.03.2023 р.).

ФОРМУЛЮВАННЯ ЕЛЕМЕНТІВ ОРГАНІЗАЦІЙНО-РОЗПОРЯДЧИХ ДОКУМЕНТІВ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Малахова А.А., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

В управлінській сфері України все більше застосовуються інформаційні технології, призначені для обробки інформації, що озвучується, візуалізується та (або) обробляється технічними засобами на об'єктах інформаційної діяльності (ОІД) в установах різних форм власності. Впровадження таких ОІД вимагає створювати комплекси технічного захисту інформації (ТЗІ). Для прискорення впровадження комплексів ТЗІ уведено в дію «Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб» [1]. Положення визначає види та умови проведення робіт з ТЗІ, встановлює відповідальність при їх проведенні.

До числа важливих складових робіт з ТЗІ є обстеження ОІД, визначення технічних каналів витоку інформації (ТКВІ) і розробка на цьому окремої моделі загроз.

Формулювання точного однозначного опису ТКВІ є важливим моментом, оскільки на цьому базується проектування ефективного комплексу ТЗІ на ОІД. В Україні національним стандартом [2] надане визначення ТКВІ, як «Сукупність носія інформації, середовища його поширення та засобу технічної розвідки». З досвіду одного з авторів, в проектах організаційно-розпорядчих документів формулювання визначених на ОІД ТКВІ інколи не відбиває усіх складових, що може привести до їх однозначних тлумачень [3].

Метою доповіді є основана на синтаксичному аналізі методика розбору визначеного на ОІД конкретного ТКВІ і його подальшому синтезі, в кінцевому документі, з урахуванням визначеної в ДСТУ структури.

Синтаксичний аналіз вимагає не плутати словосполучення та просту пропозицію. Синтаксичний розбір, покликаний виробити уміння аналізувати структуру простого, складного і ускладненого речення, розкривати характер синтаксичних зв'язків слів у словосполученні й реченні та синтаксичних відношень.

Матеріал доповіді базується на аналізі визначень ТКВІ з ДСТУ, НД ТЗІ, наукової і навчальної літератури, джерел іноземних держав.

Список літератури

1. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб, затверджене наказом ДСТСЗІ СБ України від 23.02.2002 № 9, зареєстрованим в Міністерстві юстиції України 13.03.2002 за № 245/6533.

2. ДСТУ 3396.2-97 Захист інформації Технічний захист інформації. Терміни та визначення. К.: Держстандарт України, 1997. - 16 с.

3. Заболотний В.І., Класифікація технічних каналів витоку інформації / В.І. Заболотний // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2003. Вип. 134.

АНАЛІЗ МОЖЛИВОСТІ ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ЗНАХОДЖЕННЯ ПРООБРАЗІВ ГЕШ-ФУНКЦІЙ

Іщук О.Р., Руженцев В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток обчислювальної техніки вже дійшов тієї стадії, коли є можливість створювати потужні штучні нейронні мережі. Адже на початку заснування теорії про них, вони не набрали популярність через складності з обробкою великих масивів даних.

Нейронні мережі імітують роботу невеликої частини мозку людини. Є набір нейронів поєднаних між собою, які вирішують поставлені задачі. Під час діяльності людини у неї активуються різні частини мозку, так і в нейронних мережах, тобто кожна виконує свої завдання.

Використання нейронних мереж знайшло своє місце у музичних додатках, які за сотнями параметрів рекомендують вам пісні, в комп'ютерних іграх і графічному дизайні, аби зображення на моніторі було на високому рівні при використанні недостатнього потужного обладнання, в мистецтві, де за декількома слова мережа створює зображення, яке захоплює дух.

Метою моєї роботи буде перевірка можливості використання нейронних мереж для успішного знаходження прообразів першого роду популярних геш-функцій. При побудові криптографічно стійких геш-функцій до них висуваються наступні умови: незворотність, висока складність знаходження прообразу, висока складність знаходження другого прообразу та висока складність знаходження колізій. Під другим прообразом мають на увазі, що для заданого повідомлення M має бути обчислювально неможливо підібрати інше повідомлення N, яке має таке ж геш-значення.

Для дослідження функцій буде реалізовано декілька нейронних мереж, адже не можна сказати одразу що є якийсь конкретний тип який нам підійде. Після навчання мережі даними типу «хеш-вхідне повідомлення» спробуємо дегешувати тестовий хеш. Можливо виявиться, що ми можемо отримати лише певні біти, замість цілого тексту.

Геш-функції є основою в криптографічних протоколах, цифрових підписах, відомому протоколі Bitcoin, декартових деревах, фільтрах Блума і цей список можна перелічувати ще довго. Тому ця тема є актуальною, адже має бути впевненість у стійкості та безпеці геш-функції.

Список літератури

1. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування. — Введ. 01–04–2015. — К.: Мінекономрозвитку України, 2015.

2. Євсеєв С.П. Йохов О.Ю. Король О.Г. Гешування даних в інформаційних системах: монографія. Вид. ХНЕУ, 2013. – 312 с.

АЛГОРИТМ LUFFA У ОДНОРАЗОВИХ ПОВІДОМЛЕННЯХ

Федяєв Д.В., В'юхін Д.А.
Харківський національний університет радіоелектроніки, Харків, Україна

На даний час функції гешування використовуються у багатьох застосуваннях систем захисту інформації. При цьому не всі геш-функції є криптографічно безпечними та можуть використовуватись у різних напрямках безпеки.

Метою доповіді є аналіз можливостей алгоритму Luffa для використання у одноразових повідомленнях.

Алгоритм Luffa - це сімейство криптографічних геш-функцій, який є варіантом функції губки, але на відміну від оригіналу, використовує множину паралельних перестановок та функції інжекції повідомлень [1].

У ході другого туру конкурсу SHA-3 Luffa-224 та Luffa-256 у початковому варіанті показали низьку криптостійкість, для успішної атаки знадобилося 2^{216} повідомлень. Барт Пренель (Bart Preneel) представив успішну атаку з пошуку колізій для 4 раундів крокової функції Luffa за операцій гешування та для 5-раундової, показавши тим самим межу стійкості дизайну до диференційного пошуку колізій. Після чого алгоритм був вдосконалений Даї Ватанабе і отримав назву Luffa v.2 [2, 3].

Зміни Luffa v.2:

– доданий порожній раунд функції завершення для всіх розмірів гешу;
– змінено S-блок;
– збільшено кількість повторень крокової функції з 7 до 8.

Проведений аналіз показав, що на даний час статус безпеки Luffa:

– немає доказів безпеки для з'єднання;
– відомо кілька загальних атак, але жодна з них нереалізована;
– можлива диференціальна атака, яка показала межу стійкості алгоритму;
– алгоритм здається достатньо безпечним

Таким чином проведений аналіз показав, що алгоритм Luffa не може використовуватися як довгостроковий цифровий підпис, але його особливості достатні для систем з одноразовим повідомленням.

Список літератури

1. Hisayoshi Sato, Dai Watanabe: Hash Function Luffa Supporting Document, 31 October 2008, https://ehash.iaik.tugraz.at/uploads/f/fe/Luffa_SupportingDocument.pdf

2. Shugo Mikami1 , Nagamasa Mizushima1 , Setsuko Nakamura1 , and Dai Watanabe1 https://www.hitachi.com/rd/yrl/crypto/luffa/ACompactHardwareImplementationOfSHA-3CandidateLuffa_20100810.pdf

3. Dai Watanabe Christophe De Cannière Hisayoshi Sato, 25th February 2009, https://csrc.nist.rip/groups/ST/hash/sha-3/Round1/Feb2009/documents/luffa_sha3ws1_2pp.pdf

ПРОБЛЕМИ БЕЗПЕКИ ТА МАСШТАБОВАНОСТІ В СИСТЕМІ ETHEREUM, ПОВ'ЯЗАНІ ІЗ ЗАСТОСУВАННЯМ СМАРТКОНТРАКТІВ

Юрченко А.Є., Шафоростов М.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Смартконтракти – це програми, що забезпечують автоматизоване виконання угод між сторонами, для якого посередник не потрібен [1]. Вони є наріжним елементом багатьох децентралізованих облікових систем – платформ смартконтрактів.

Смартконтракти можуть застосовуватися для розроблення похідних фінансових засобів, ідентифікаційних систем, файлових сховищ і т. ін.

Саме в межах блокчейн-платформи Ethereum смартконтракти вперше набули широкого поширення.

Основними складниками смартконтрактів Ethereum є функції, події та змінні стану. Здебільшого для їх написання використовується повна за Тьюрінгом мова Solidity.

Після компіляції код смартконтракту перетворюється на байт-код для віртуальної машини Ethereum і зберігається в блокчейні за допомогою транзакції створення контракту.

Кожний успішно збережений смартконтракт розпізнається за унікальною адресою [2].

Мета доповіді – проаналізувати вплив застосування смартконтрактів на безпеку та масштабованість системи Ethereum.

Для аналізу використовуються статистичні дані про проведення транзакцій та виконання смартконтрактів у системі Ethereum, а також інформація про відомі вразливості.

Уразливості, які розглядаються, поділяються на групи за 3 основними причинами:

«мова Solidity»,

«віртуальна машина»,

«будова блокчейна» [2].

Також пропонуються шляхи вдосконалення смартконтрактів, як-от використання різних мов програмування, розробляння бібліотек безпечних контрактів та вдосконалення механізмів передзапускної верифікації контрактів.

Список літератури

1. Buterin V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2014. URL: https://ethereum.org /669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf.

2. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract / S. S. Kushwaha та ін. *IEEE Access*. 2022. Т. 10. С. 6605–6621.

КРИПТОГРАФІЧНА БЕЗПЕЧНІСТЬ СХЕМИ АВТЕНТИФІКАЦІЇ ШНОРРА

Оболоник Д.В., Шафоростов М.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У час, коли майже кожна комп'ютерна система передбачає налаштовування доступу до неї для мережних користувачів, автентифікація суб'єктів – невід'ємний процес комп'ютерної системи. Автентифікація – це процес підтвердження того, що користувач є тим, ким себе видає. На даний час існує багато методів та протоколів автентифікації користувачів у комп'ютерних та інформаційних системах [1, 2].

Одним із протоколів, які реалізують автентифікацію, є схема Шнорра. Її особливість із погляду швидкодії – попереднє обробляння операції піднесення до степеня за модулем, для якої випадкове число добирається як показник степеня.

Похідною до цієї схеми є однойменна схема цифрового підпису, яка поєднує ідеї схеми Ель-Ґамаля та схеми Фіата–Шаміра [3].

Криптографічна безпечність схеми Шнорра математично ґрунтується на складності задачі знаходження дискретного логарифма. Таке саме підґрунтя характерне, наприклад, для протоколу Діффі–Геллмана в кінцевих полях.

Мета доповіді – розглянути можливі значення параметра безпеки t для використання схеми саме в контексті автентифікації.

Розкривається суть показника складності зламу 2^t. Пояснюється розбіжність мінімального необхідного значення t для схеми автентифікації та для схеми підпису.

Також пропонуються обмеження на значення відкритих параметрів схеми p та q з огляду на останні досягнення щодо знаходження дискретного логарифма за допомогою класичного комп'ютера.

Дослідний розрахунок, який розглядається, було виконано над 795-бітним простим числом. Він показав, що, зокрема, складність задачі знаходження дискретного логарифма лише в 3 рази (за грубою оцінкою) вища, ніж складність задачі розкладення на множники [4].

Список літератури

1. Сєвєрінов О.В., Кліпоносова В.С. Автентифікації користувачів веб-ресурсів, НТУ «ХПІ», 2022.

2. Власов А.В., Сєвєрінов О.В., Слиш О.В. Впровадження децентралізованої системи ідентифікації. НТУ «ХПІ», 2020.

3. Schorr C. P. Efficient Signature Generation by Smart Cards. *Journal of cryptology*. 1991. Т. 4, № 3. С. 161–174.

4. Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment / F. Boudot та ін. *Advances in Cryptology – CRYPTO 2020*. Springer, 2020. С. 62–91.

ВИКОРИСТАННЯ МЕТОДІВ ГЛИБОКОГО НАВЧАННЯ ДЛЯ ВІЗУАЛІЗАЦІЇ ТА ВИЯВЛЕННЯ MALWARE

Федюшин О. І., Хижняк К.М.
Харківський національний університет радіоелектроніки, Харків, Україна

В останні роки атаки за допомогою зловмисного програмного забезпечення стали серйозною загрозою безпеці та продовжують завдавати величезних збитків бізнесу. Через швидке зростання кількості варіантів шкідливих програм, їх миттєва й точна класифікація має вирішальне значення для кібербезпеки.

Оскільки традиційні методи, засновані на машинному навчанні, обмежені в швидкості обробки величезної кількісті зловмисного програмного забезпечення, класифікація зловмисного програмного забезпечення на основі зображень [1] - візуалізації вихідного коду malware - та глибокого навчання може стати ефективним рішенням цього завдання.

Згорточні нейронні мережі швидко стали найсучаснішими фреймворками для різноманітних додатків, які використовуються в класифікації зображень [2, 3]. На відміну від більш традиційних методів машинного навчання, класифікатори глибокого навчання навчаються за допомогою вивчення характеристик, а не за допомогою алгоритмів для конкретних завдань. Це означає, що машина вивчатиме шаблони в зображеннях, які їй представлені, замість того, щоб вимагати від людини-оператора визначати шаблони, які машина повинна шукати на зображенні.

Тож методи глибокого навчання можуть застосовуватися до згенерованих зображень, щоб класифікувати їх як зловмисне або ж безпечне програмне забезпечення.

Метою доповіді є дослідження методів глибокого навчання та отримання результатів щодо їх ефективності при виявленні шкідливого програмного забезпечення у вигляді метрик. В доповіді також надається аналіз результатів роботи отриманих моделей.

Список літератури

1. G. Sun and Q. Qian, “Deep Learning and Visualization for Identifying Malware Families,” IEEE Trans. Dependable Secur. Comput., vol. 18, no. 1, pp. 283–295, 2021, doi: 10.1109/TDSC.2018.2884928.

2. A. Patil and M. Rane, “Convolutional Neural Networks: An Overview and Its Applications in Pattern Recognition,” Smart Innov. Syst. Tech-nol., vol. 195, pp. 21–30, 2021, doi: 10.1007/978-981-15-7078-0_3.

3. Федюшин О. І., Хижняк К. М. Методи виявлення та блокування Ransomware загроз / Матеріали Дванадцятої міжнародної науково-технічної конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління», м. Харків, 27-28 квітня 2022р. – С. 152.

БЕЗПЕКА ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ НА ОСНОВІ МОДЕЛЕЙ ВИЯВЛЕННЯ АНОМАЛІЙ

Федюшин О.І., Кавецький М.С.
Харківський національний університет радіоелектроніки, Харків, Україна

З кожним днем, комп'ютерні системи та мережі стають все більш важливими для нашого повсякденного життя. Вони забезпечують доступ до інформації, зручність та швидкість взаємодії з іншими людьми та системами. Але разом зі зростанням їх важливості, збільшується також ризик їхнього некоректного функціонування та зловмисного втручання. Тому безпека комп'ютерних систем є дуже важливою.

Одним з підходів до розв'язання цієї проблеми є використання методів машинного навчання на основі виявлення аномалій.

Завдяки цим технологіям, можна виявити відхилення в поведінці комп'ютерної системи або мережі та вчасно вжити необхідні заходи для захисту від потенційних загроз.

Для виявлення загроз комп'ютерним мережам використовують багато методів машинного навчання з вчителем та без нього. Аналіз відповідних робіт показав, що зараз фокус досліджень змістився в бік використання глибоких нейронних мереж для виявлення аномалій [1, 2].

Традиційні методи машинного навчання, як правило, неефективні при обробці великомасштабних даних і нерівномірно розподілених вибірок. Моделі глибокого навчання більш продуктивні при аналізі таких даних.

Отже, оскільки обраним напрямом є моделі глибокого навчання для побудови таких систем потрібно мати багато даних, але це цілком виправдано, бо модель зможе мати більший простір для тренування, що якісно вплине на її точність виявлення аномалій.

Метою доповіді є ознайомлення з потенційними методами забезпечення функціонування комп'ютерних систем та мереж на основі побудови моделі штучного інтелекту для виявлення аномалій.

Результати досліджень показали, що ефективним способом для вирішення завдання є використання моделей глибокого навчання, які приймають дані наперед записаної активності мережі та будують модель, яка найкращим чином може узагальнити всі процеси у комп'ютерній системі та класифікувати активність як нормальну чи шкідливу.

Список літератури

1. Tushkanova, O.; Levshun, D.; Branitskiy, A.; Fedorchenko, E.; Novikova, E.; Kotenko, I. Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation. *Algorithms* 2023, *16*, 85. https://doi.org/10.3390/a16020085

2. Lee, K.-M.; Cho, M.-Y.; Kim, J.-G.; Lee, K.-H. Anomaly Detection Method for Unknown Protocols in a Power Plant ICS Network with Decision Tree. *Appl. Sci.* 2023, *13*, 4203. https://doi.org/10.3390/app13074203

ОЦІНКИ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ У ПРОЦЕСІ ФУНКЦІОНУВАННЯ ЄДИНОЇ ДЕРЖАВНОЇ СИСТЕМИ ЦИВІЛЬНОГО ЗАХИСТУ

Тютюник В.В.
Національний університет цивільного захисту України, Харків, Україна
Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, України
Тютюник О.О.
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна

В Україні для забезпечення реалізації державної політики у сфері цивільного захисту функціонує Єдина державна система цивільного захисту (ЄДСЦЗ), яка складається з функціональних і територіальних підсистем та повинна забезпечувати необхідний рівень безпеки життєдіяльності в умовах надзвичайних ситуацій різної природи [1–3].

У процесі функціонування ЄДСЦЗ являє собою систему з рознесеними у просторі та часі складовими, які пов'язані між собою великими потоками різного роді інформації [4].

В роботі [5] представлено результати розповсюдження ризико-орієнтованого підходу для оцінки виникнення загроз для інформації, що циркулює у процесі функціонування ЄДСЦЗ, як системи з рознесеними у просторі та часі складовими, які пов'язані між собою великими потоками різного роді інформації.

Представлені у доповіді результати є однією з складових комплексного підходу щодо розвитку наукових основ формування системи національної безпеки держави.

Список літератури

1. Кодекс цивільного захисту України від 2 жовтня 2012 року № 5403-VI // Голос України. – 2012.– листопад (№ 220(5470)). – С. 4 – 20.

2. Постанова Кабінету Міністрів України від 9 січня 2014 року № 11 «Про затвердження Положення про Єдину державну систему цивільного захисту» [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/11-2014-%D0%BF

3. Розпорядження Кабінету Міністрів України від 25 січня 2017 року № 61-р. «Про схвалення Стратегії реформування системи Державної служби України з надзвичайних ситуацій» [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/61-2017-%D1%80

4. Наказ ДСНС від 01 жовтня 2020 року № 533 «Про затвердження Положення з організації заходів забезпечення кібербезпеки ДСНС».

5. Рубан І.В., Тютюник В.В., Заболотний В.І., Тютюник О.О. Особливості розповсюдження ризико-орієнтованого підходу до оцінки вразливості об'єктів кіберзахисту. Науковий журнал "Безпека інформації". Київ: Національний авіаційний університет, 2020. Т.26. №3. С. 145–155.

ПОРІВНЯННЯ ПОШИРЕНИХ ХМАРНИХ СХОВИЩ ЗА КРИТЕРІЄМ БЕЗПЕКИ

Чепенко Д.О., Олешко І.В.
Харківський національний університет радіоелектроніки , Харків, Україна

Хмарне зберігання даних стає все більш актуальним у сучасну епоху цифрових технологій. Це можна пояснити наступним: хмарні сховища доступні в будь-який час і в будь-якому місці, хмарне сховище усуває потребу у дорогому апаратному забезпеченні, користувачі можуть легко збільшувати або зменшувати обсяги свого сховища за потреби. Це дозволяє компаніям масштабувати свої рішення для зберігання в міру зміни потреб, робити резервне копіювання даних і аварійне відновлення.

Метою даної роботи є порівняльний аналіз хмарних сховищ Dropbox і Google Drive. Безпека є одним із найважливіших критеріїв при виборі хмарного сховища [1, 2].

Обидві платформи використовують шифрування для захисту користувачів, однак є деякі відмінності в механізмах захисту даних.

Dropbox використовує шифрування AES 256-bit для захисту даних при транспортуванні та зберіганні.

Dropbox надає можливість використовувати двофакторну автентифікацію для підвищення безпеки облікового запису. Dropbox Business також дозволяє налаштовувати права доступу та переглядати журнали активності.

Google Drive так само використовує шифрування AES 128-bit для захисту даних. При цьому протокол HTTPS використовується для безпечного транспортування даних [3].

Google Drive надає можливість двофакторної автентифікації та налаштування прав доступу. Google Drive також надає інструменти захисту конфіденційних даних такі, як вбудовані засоби контролю прав доступу та можливість встановлення обмежень на поширення файлів.

Таким чином, обидві платформи, Dropbox та Google Drive, надають користувачеві широкий спектр функцій та можливостей, але рекомендуємо використовувати саме Dropbox тому, що він має більш простий інтерфейс користувача і більш високий рівень безпеки для бізнес-користувачів. Перевагами Google Drive можна вважати безкоштовне сховище та інтеграцію з іншими продуктами Google.

Список літератури

1. І.Ф. Абулов І.Д. Горбенко, “Хмарні обчислення та аналіз питань інформаційної безпеки в хмарі”, Прикладна радіоелектроніка, т. 12, №2. с. 194-201, 2013.

2. Рудий С.В., Сєвєрінов О.В. Дослідження моделі безпеки при використанні хмарних сервісів, НТУ «ХПІ», 2022.

3. Instructor Textbook «Designing & Deploying Cloud Solutions for Small and Medium Business», Hewlett-Packard Company, L.P., 2013. - 893p.

ВИКОРИСТАННЯ ДИФРАКЦІЙНО ВІДБИВНОГО ПОКРИТТЯ ДЛЯ БЕЗПЕКИ ФУНКЦІОНУВАННЯ ПУНКТІВ УПРАВЛІННЯ

Коломійцев О.В.
Національний технічний університет "ХПІ", Харків, Україна
Катунін А.М.
Національний університет цивільного захисту України, Харків, Україна
Пустоваров В.В.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна

Активне застосування комплексів високоточної зброї, зокрема систем із напівактивним лазерним наведенням, для знищення, у тому числі, пунктів управляння (ПУ), робить розробку методів протидії цієї зброї актуальною.

Метою доповіді є представлення наукового матеріалу щодо формування оптичних перешкод на основі використання дифракційно відбивного покриття для безпеки функціонування ПУ.

В доповіді розкрито сутність дифракційно відбивного покриття, яка полягає у наступному у тому, що при підсвічуванні ПУ лазерною станцією підсвічування цілей система попередження визначає напрям на станцію.

На основі отриманих даних здійснюється орієнтація екрану з дифракційно відбивним покриттям таким чином, щоб напрями розповсюдження головних дифракційних максимумів діаграми розсіювання збігалися з напрямом на підстилаючу поверхню і формування світлових плям – оптичних перешкод відбувалося на відстанях, що забезпечують попадання оптичних перешкод у полі зору системи наведення високоточної зброї. Відстань від ПУ до світлових плям – оптичних перешкод повинна перевищувати радіус ураження боєприпасів. В кутових секторах, відмінних від напрямів розповсюдження головних дифракційних максимумів діаграми розсіювання дифракційно відбивного покриття, спостерігатиметься значне зниження інтенсивності відбитого лазерного випромінювання.

Таким чином, за зміною значення періоду дифракційно відбивного покриття можливо керувати положенням світлових плям – оптичних перешкод на підстилаючої поверхні та виведення з робочого стану системи керування високоточної зброї.

Список літератури

1. Катунін А.М., Коломійцев О.В. Пропозиції щодо використання акустооптичного методу керування дифракцією оптичного випромінювання на відбивних покриттях для захисту озброєння та військової техніки. II Всеукраїнська науково-технічна інтернет-конференція «Актуальні проблеми бойового застосування та експлуатації і ремонту зразків озброєння та військової техніки». 17-18 листопада 2022 року. – Вінниця: ВНТУ, 2022. – С. 192-193. http://repositsc.nuczu.edu.ua/handle/123456789/16197.

ОБФУСКАЦІЯ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ ЗА ДОПОМОГОЮ АГРЕГАЦІЇ ВИСОКОГО РІВНЯ

Горбачов В.О., Пономаренко О.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Обфускація апаратного забезпечення [1] – це техніка, за допомогою якої опис або структура електронного апаратного забезпечення змінюється, щоб навмисно приховати його функціональність для захисту від різних форм атак. Іншими словами, апаратна обфускація модифікує дизайн таким чином, що результуюча архітектура стає неочевидною для зловмисника.

Зменшення контролю над життєвим циклом мікросхем підкреслює різні проблеми безпеки, пов'язані з мікросхемами. Таким чином, безпека апаратних мікросхем стала основною проблемою при проектуванні та тестуванні інтегральних мікросхем (ICs).

Основною метою дослідження є розробка методів проектування, які можуть ефективно протистояти загрозам безпеці на ненадійних етапах життєвого циклу ІС або пом'якшувати їх. Основним принципом запропонованих методів є метод обфускації дизайну для досягнення апаратної безпеки. У роботі розглядається обфускація на основі реконфігурації на етапі постфабрикації ІС. Розглядається необхідність додавання етапу реконфігурованої логіки до циклу розробки. Цю техніку можна розглядати як профілактичний захід, який приховує частину дизайну від зловмисника. Іншими словами, метод приховує точні функції та структуру мікросхеми до тих пір, поки не буде запрограмована реконфігурована логіка.

У роботі розглядається концепція багаторівневої архітектури безпеки на основі ядра. Реконфігурована техніка обфускації на основі логіки використовує функції реконфігурації для обфускації дизайну. Пропонується зробити невеликий компонент дизайну еталонного монітора (reference monitor) реконфігурованим у ІС. Цей підхід приховує функціональні та/або схемні деталі на ненадійних етапах циклу розробки проекту.

Метод застосування реконфігурованої обфускації еталонного монітора виконується за допомогою багаторівневого алгоритму агрегації структурної моделі SoC [2]. Цей метод реалізовано в рамках платформи FPGA. Робота ілюструє використання функції реконфігурації Xilinx Vivado Design Suite і плати Nexys4-DDR для обфускації еталонного монітора SoC.

Список літератури

1. Sengupta A., Roy D., Mohanty S., Corcoran P., "DSP design protection in CE through algorithmic transformation based structural obfuscation", IEEE Transactions on Consumer Electronics, 2017, vol. 63, no. 4, pp. 467–476.

2. Gorbachov V., Sytnikov D., Ryabov O., Batiaa A. K., Ponomarenko O., "Dimension Reduction for Network Systems Using Structure Model Aggregation", International Journal of Design & Nature and Ecodynamics, 2020, vol. 15, no. 1, pp. 13–23.

СЕКЦІЯ 4
ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У РІЗНИХ ГАЛУЗЯХ

Керівник секції: д.т.н., проф. В. В. Косенко, НУ «ПП», Полтава
Секретарка секції: к.т.н. Бельорін-Еррера О.М., НТУ «ХПІ», Харків

Підсекція 4.1. Сучасні інформаційно-вимірювальні системи

DIAGNOSTIC SOFTWARE OF INFORMATION-MEASURING SYSTEMS

Dotsenko M.I.
V. N. Karazin Kharkiv national university, Kharkiv, Ukraine

The current stage of development of measurement technology for diagnosis and condition monitoring of objects of different nature is characterized by an increasing complexity of tasks and intensive implementation of intelligent technologies in the measurement process [1]. The growth of complexity and high rates of development of computer systems, their introduction into all areas of activity determine the urgency of the problem of increasing their fault tolerance and survivability. To reduce the time for determining the working capacity of technical objects and finding the place of failure in them, it is necessary to develop diagnostic support - a set of interrelated rules, methods, algorithms and tools necessary for diagnosing at all stages of the object's life cycle [2, 3].

The purpose of the report is to analyze the methods for developing diagnostic support for automated control systems. The report discusses the features of the problem under consideration. It is shown that the development of diagnostic software is a difficult task, since the means of control and diagnostics must satisfy a number of most often conflicting requirements for speed, hardware costs, reliability of operation, etc. Many problems: finding minimal tests, choosing the optimal composition of checks, etc. are logical-combinatorial problems. The complexity of classical algorithms and methods for solving these problems makes us look for new approaches and develop more efficient methods.

To reduce the complexity of developing diagnostic software, reduce the duration of the process, improve the quality of design, and reduce the cost of its development, the TEST program [4] has been developed, which allows you to automate the process of developing diagnostic software, reduce development time and improve its quality by generating minimal test sequences and simplifying control schemes.

References

1. Babak V. P. et al. Principles of construction of systems for diagnosing the energy equipment //Diagnostic Systems for Energy Equipments. – 2020. – С. 1-22.

2. Nikitaev V. G. et al. Approach to building knowledge bases in information-measuring systems diagnostics of acute leukemias // Journal of Physics: Conference Series. – IOP Publishing, 2018. – Т. 945. – №. 1. – С. 1 – 5.

3. Peleska J. Industrial–Strength Model–Based Testing–State of the Art and Current Challenges / J. Peleska // EPTCS 111, 2013. – P. 3 – 28.

4. Computer program "TEST" / Dotsenko M.I. et al. Registered in UNOIPI on 30.03.2023.

DOELIB - DESIGN OF EXPERIMENTS PROBLEM LIBRARY

Pavlik G.V.
National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine
Dotsenko N.V.
O.M. Beketov National University, Kharkiv, Ukraine

To improve the efficiency of experimental studies, it is of great importance to develop a strategy for optimal planning of the experiment. The modern method of planning an experiment is intended to expand the technology of industrial planning of an experiment, and consists of integrated methods and tools for planning, performing and analyzing an experiment [1, 2]. The task of planning an experiment is to find the optimal combination by enumeration of options. The use of combinatorial plans makes it possible to optimally reduce and significantly reduce the cost of computer time. The construction of combinatorial schemes belongs to combinatorial analysis, and their application in real experimental studies is an application of combinatorial analysis in experiment planning [3].

The problem under consideration belongs to NP-complete problems. The traditional directions for solving this class of problems are as follows: devising exact algorithms, which work reasonably fast only for small problem sizes; devising "suboptimal" or heuristic algorithms, i.e., algorithms that deliver approximated solutions in a reasonable time; finding special cases for the problem for which either better or exact heuristics are possible. Various heuristics and approximation algorithms, which quickly yield good solutions, have been devised.

The purpose of the report is to develop a set of test problems for evaluating the effectiveness of approximate methods for constructing optimal plans for a multifactorial experiment.

This paper contains the description of a Design of Experiments problem library (DOELIB) which is meant to provide researchers with a broad set of test problems with various properties. For every problem a short description is given along with known lower and upper bounds.

References

1. Weissman S. A., Anderson N. G. Design of experiments (DoE) and process optimization. A review of recent publications //Organic Process Research & Development. – 2015. – Т. 19. – №. 11. – С. 1605-1633.

2. Ranga S. et al. A review on Design of Experiments (DOE) //Int. J. Pharm. Chem. Sci. – 2014. – Т. 3. – №. 1. – С. 216-24.

3. Методология оптимального по стоимостным и временным затратам планирования эксперимента: монография / Н. Д. Кошевой, Е. М. Костенко, А. В. Павлик, Н. В. Доценко. – Полтава: Полтавская государственная аграрная академия, 2017. – 232 с.

КОНСТРУКТИВНЕ ПЕРЕРАХУВАННЯ ДІАГНОСТИЧНИХ МОДЕЛЕЙ

Павлик Г.В.
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

У сфері виробництва та експлуатації комп'ютерних систем значну роль відіграє технічна діагностика. Інформація, що одержується за допомогою засобів діагностики про справність пристроїв, місце та причини відмов дозволяє встановити прямі й зворотні зв'язки керування якістю та надійністю технічної системи, що експлуатується [1].

Для скорочення строків проектування засобів діагностування бажано мати стандартні рішення з організації ефективних процесів перевірки комп'ютерних систем і їхніх компонентів.

Сучасні методи діагностування орієнтовані на порівняно вузькі класи дискретних пристроїв [2, 3].

Метою доповіді є розгляд актуальної проблеми розробки нових методів й засобів забезпечення ефективності, надійності, контролю, діагностики.

В доповіді розглянуто метод функціонального контролю дискретних пристроїв, заснований на комбінаторному підході до класифікації об'єктів. Пошук оптимального рішення серед заданої множини варіантів надзвичайно складний і вирішується шляхом перебору, однак у більшості задач такий повний перебір нездійсненний.

Для зменшення кількості варіантів, що розглядаються, на множині всіх об'єктів вводяться відношення еквівалентності й множина всіх об'єктів розбивається на класи еквівалентності. Будь-який об'єкт із класу еквівалентності за допомогою заданих перетворень переходить в інший об'єкт із цього ж класу еквівалентності.

Для одержання інформації про множину всіх об'єктів достатньо вибрати типового представника від кожного класу еквівалентності.

За допомогою розробленого методу конструктивного перерахування діагностичних моделей сформовані каталоги типових ДМ, необхідні при побудові засобів контролю.

Список літератури

1. Peleska J. Industrial–Strength Model–Based Testing–State of the Art and Current Challenges / J. Peleska // EPTCS 111, 2013. – P. 3 – 28.

2. Knuppel T. Fault Diagnosis for Electrical Distribution Systems using Structural Analysis / T. Knuppel, M. Blanke, J. Stergaard // International Journal of Robust and Nonlinear Control, 2014. – V. 24. – P. 1446 – 1465.

3. Babak V. P. et al. Principles of construction of systems for diagnosing the energy equipment //Diagnostic Systems for Energy Equipments. – 2020. – С. 1-22.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ВИЗНАЧЕННЯ ВАГИ ТІЛА КОСМОНАВТА І МАЛОЇ ВАГИ ОБ'ЄКТІВ В УМОВАХ НЕВАГОМОСТІ

Коломійцев О.В.
Національний технічний університет "ХПІ", Харків, Україна
Комаров В.О.
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

Бурхливий розвиток космічних технологій та прагнення підкорення космосу відкриває нові широкі перспективи щодо подальшого вивчення та використання космічного простору на користь науки. Тому, головним завданням, при використанні космічних комплексів та транспортних засобів, є доставка на орбіту та повернення з неї корисних вантажів малої ваги. Такі транспортні засоби дозволяють повертати з орбіти на Землю з автоматичних апаратів космонавтів, матеріали наукових досліджень і експериментів, а також обладнання, що вийшло з ладу тощо.

Таким чином, визначенням ваги тіла космонавта і малої ваги об'єктів в умовах невагомості є актуальною науковою задачею.

Метою доповіді є створення пристрою для високоточного визначення ваги тіла космонавтів і малої ваги об'єктів в умовах невагомості.

В доповіді розглянуто найбільш зручні і перспективні методи визначення інерціальної ваги тіла в умовах невагомості, які використовують різного роду осцилятори та прилади, що дозволяють вимірювати параметри тіла, яке коливається, а також – різноманітні завдання, які пов'язані з визначенням ваги об'єктів малої ваги.

Запропоновано використання інформаційних технологій для визначення ваги тіла космонавтів і малої ваги об'єктів в умовах невагомості. При цьому контролюється зміна частоти власних коливань динамічної системи, до якої жорстко закріплено об'єкт контролю.

Представлено технічні розробки пружно-вагового пристрою для проведення вимірювань ваги об'єкта контролю.

Наведено схемо-технічне рішення пристрою, як одноступеневого осцилятора, стосовно якого можуть бути записані відповідні рівняння динаміки зміни ваги об'єкта контролю за часом. Розкрито принцип дії пристрою.

Список літератури

1. Метод контролю частоти власних коливань для визначення ваги тіла космонавта і малої ваги в умовах невагомості / О. В. Коломійцев, В. О. Комаров, О. М. Дмітрієв, В. В. Пустоваров, Р. М. Олійник // Сучасні інформаційні системи = Advanced Information Systems. – 2022. – Т. 6, № 2. – С. 74-81. URI:https://repository.kpi.kharkov.ua/handle/KhPI-Press/63163.

СУЧАСНА МОБІЛЬНА ОДНОПУНКТНА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНА СИСТЕМА

Коломійцев О.В.
Національний технічний університет "ХПІ", Харків, Україна
Калачова В.В., Балабуха О.С., Беспалько О.В.
Харківський національний університет Повітряних Сил імені І. Кожедуба, Харків, Україна

Відома, велика низка методів щодо побудови (оптимального синтезу) інформаційно-вимірювальних систем (ІВС) різних за діапазонами хвиль та призначенням. Такі методи базуються на математичному апараті перетворення вимірювальних сигналів, технологіях вимірювань, передавання та опрацювання сигналів і даних, використанні сучасних інформаційно-комунікаційних каналів передавання інформації, методах досліджень метрологічних характеристик тощо. Теоретичні основи ІВС умовно можна розділити на два великі напрями: основи розроблення і створення ІВС (як технічної системи) та – основи функціонування ІВС (як апаратно-програмних засобів вимірювання, що відображають характерні специфіку та особливості спільності і конкретики проведення процесів вимірювання).

Метою доповіді є доведення наукових підходів щодо синтезу сучасної мобільної однопунктної інформаційно-вимірювальної системи (МОІВС) для забезпечення траєкторних вимірювань літальних апаратів (ЛА) на полігонних випробувально-обчислювальних комплексах.

В доповіді проведено аналіз особливостей оптимального синтезу ІВС різних за діапазонами хвиль.

Розглянуто процес вимірювання параметрів руху ЛА, який характеризується послідовним застосуванням двох мір: фізичної міри (одиниці або шкали) при експериментальному її порівнянні зі значенням вимірюваної величини, а також нормованої ймовірнісної міри для статистичного оцінювання результату вимірювання і його якості (характеристики точності).

Запропоновано МОІВС, яка забезпечить виявлення ЛА, його захват, стійке кутове автоматичне супроводження, високоточне вимірювання кутів азимута і місця, похилої дальності, радіальної і кутових швидкостей у широкому діапазоні дальностей, у будь-який час року, доби і за будь-якої погоди, у будь-якій точці і за будь-яким рельєфом місцевості полігону та багатоканальну передачу команд керування на ЛА.

Список літератури

1.Альошин Г.В., Коломійцев О.В., Акулінін Г.В., Клівець С.І. Параметричний та структурний оптимальний синтез багатошкальних радіотехнічних інформаційно-вимірювальних систем. *Системи обробки інформації*. 2020. № 2(161). С. 114-21. https://doi.org/10.30748/soi.2020.161.13.

Підсекція 4.2. Інформаційні технології у цивільній безпеці

BLOCKCHAIN TECHNOLOGY IN CIVILIAN SECURITY

Buslov P.V., Yevheniev A.M., Kireieva S.O.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

The adoption of blockchain technology in civil security represents an important step towards increasing citizen security and protecting citizens' rights and freedoms. Blockchain technology is a secure, decentralised system that can be used to exchange and store data without the possibility of tampering [1]. This makes it an ideal tool to improve law enforcement and provide a more reliable system of civil security.

The purpose of this paper is to explore the applicability of blockchain technology to civil security in Ukraine, in order to identify the main benefits and potential challenges of using this technology to improve the security of citizens, and therefore the entire country [2].

The report focuses on the main benefits of using blockchain technology in civil security, as well as the possible problems and challenges associated with its implementation. Initially, the paper discusses the theoretical background of blockchain technology and how it works [3]. It then explores the main benefits of blockchain technology in civil security, such as transparency, reliability, security and the ability to create decentralized systems. Then, the potential challenges and problems in the implementation of blockchain technology in civil security in Ukraine are discussed, such as limited access to the technology, the high cost of implementation, legislative and regulatory issues [4].

As a result, based on the analyzed information, it is concluded that blockchain technology can be an important tool to improve civil security in Ukraine. It allows the creation of secure, transparent and reliable data management systems that can help improve the efficiency of law enforcement, protect citizens' personal data and combat corruption and smuggling. However, successful implementation of blockchain technology requires sufficient effort on the part of government agencies and professionals to address the potential problems associated with its use. It is therefore proposed to draw attention to the potential of blockchain technology to improve civil security, and to insist on additional research for its subsequent implementation.

References

1. Zohar A. Bitcoin: Under the Hood. Communications of the ACM, vol. 58, pp. 104-113, 2015.
2. Kshetri N. Blockchain's Roles in Meeting Key Supply Chain Management Objectives. International Journal of Information Management, vol. 39, pp. 80-89, 2018.
3. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton Uni Press, 2016.
4. Crosby M., Pattanayak P., Verma S., Kalyanaraman V. Blockchain Technology: Beyond Bitcoin. Applied Innovation, vol. 2, pp. 6-10, 2016.

РОЗРОБКА ВЕБ-ДОДАТКА ДЛЯ ТРАНСПОРТНО-ЛОГІСТИЧНОЇ КОМПАНІЇ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ INTERSYSTEMS IRIS

Лещенко О.Б., Анікін А.М.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Ефективне керування перевезеннями будь-яких підприємств можливо за допомогою удосконалення процесів в такої галузі як логістика. Велика кількість проблем логістичних компаній пов'язані з оптимізацією роботи транспорту у ланцюзі логістичних систем, особливо якщо це пов'язано з воєнним станом [1]. Зниження собівартості перевезень та їх оптимізацію можливо за допомогою якісного планування та організацію перевезення.

Метою доповіді є використання інформаційних технологій InterSystems IRIS для розробки веб-додатка для транспортно-логістичної компанії. При використанні запропонованих технологій з'являється можливість зберігати великі об'єми даних, аналізувати їх та застосовувати їх для подальшого прогнозування діяльності компанії.

В доповіді наводяться особливості організації перевезення вантажу транспортом, а також структура створюваного рішення. Наведені дані показують, що на ефективність перевезення вантажу та вартість впливають багато чинників, такі як: тип вантажу, вага вантажу, вага причепу, стан доріг, витрати пального транспортом, відстань між двома точками трансферу тощо [1].

Розробка веб-додатка виконана на основі трирівневої технології клієнт-сервер. Інтерфейс кінцевого користувача розроблений за допомогою сучасних методів та інформаційних технологій, таких як: HTML, CSS, JavaScript, InterSystems ZEN та API інтерфейсом до сервісу картографії. Для розробки та розгортання додатків використані технології платформи InterSystems IRIS, що забезпечує високий рівень продуктивності. Серверна частина додатка виконана під управлінням об'єктно-реляційній системи керування базами даних InterSystems IRIS [2].

Розроблений веб-додаток дозволить вирішати питання розрахунку маршрутів та витрат під час процесу перевезення вантажів. У зв'язку з великою кількістю чинників, що впливають на даний процес, розроблений додаток дозволить ефективно автоматизувати процес організації транспортно-логістичних перевезень.

Список літератури

1. Мельник, З. Відновлення транспортного сектору України – як зробити його "зеленим"? [Електронний ресурс] / З. Мельник. – Режим доступу: https://brdo.com.ua/analytics/vidnovlennya-transportnogo-sektoru-ukrayiny-yak-zrobyty-jogo-zelenym/. – 16.02.2023.

2. Лещенко, О. Б. Застосування технології DeepSee InterSystems для побудови багатовимірних баз даних і сховищ інформації : навч. посіб. / О. Б. Лещенко, Ю. О. Лещенко. – Харків : Нац. аерокосм. ун-т «Харків. авіац. ін-т», 2021. – 66 с.

КОМПОНЕНТНИЙ МЕТОД АНАЛІЗУ ЛОГІСТИКИ ПОСТАЧАННЯ ВІЙСЬКОВОЇ ТЕХНІКИ В ЗОНУ ВОЄННОГО КОНФЛІКТУ

Федорович О.Є., Лещенко Ю.О., Коновалова О.В., Малєєв Л.В.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Ефективне використання озброєння в зоні воєнного конфлікту пов'язане з наявністю необхідної кількості забезпечуючих компонент озброєння (боєприпаси, запчастини, ремкомплекти, допоміжна техніка, тощо). Тому актуальна тема доповіді, в якій наведені результати дослідження формування необхідних запасів забезпечуючих компонент озброєння в зоні воєнного конфлікту [1, 2].

Метою доповіді є створення, за допомогою розробленого компонентного методу, вимог до формування запасів озброєння та забезпечуючих компонент для ефективного використання зброї в зоні бойових дій.

В доповіді наведено результати розробки оригінального компонентного методу, який дозволяє сформувати кількісні вимоги до необхідних запасів військової техніки (озброєння та забезпечуючі компоненти) в зоні воєнного конфлікту.

Створена компонентна структура військової техніки, за допомогою якої оцінюється потрібність в озброєнні та її комплектуючих, що далі дає можливість сформувати вимоги до обсягів армійських складів, складів виробників та постачальників військової техніки. За допомогою багатошарової компонентної структури військової техніки та бази прецедентів формуються вимоги до виробництва озброєння та її комплектуючих в умовах потреб воєнного стану. Відокремлені види компонент військової техніки (повторного використання, адаптивні, інноваційні).

При недостатній кількості озброєння в зоні бойових дій, спочатку формуються вимоги до армійських запасів, далі до складів виробників.

Запропонований підхід дозволяє обґрунтувати потребу в кількості запасів озброєння та її забезпечуючих компонент для використання в зоні воєнного конфлікту.

Список літератури

1. Milewski, R. Decision making scenarios in military transport processes [Text] / R. Milewski, T. Smal // Archives of Transport. – 2018. – Vol. 45, iss. 1. – P. 65-81. DOI: 10.5604/01.3001.0012.0945.

2. Моделювання транспортної логістики військових вантажів з урахуванням збитків, які виникають у зоні бойових дій через запізнення у постачанні [Текст] / О. Є. Федорович, О. С. Уруський, І. Б. Чепков, М. І. Луханін, Ю. Л. Прончаков, К. О. Рибка, Ю. О. Лещенко // Радіоелектронні і комп'ютерні системи. – 2022. – № 2. – С. 63-74. DOI: 10.32620/reks.2022.2.05.

МОДЕЛІ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДОСЛІДЖЕННЯ ЛОГІСТИКИ ФОРМУВАННЯ ЗАПАСІВ ОЗБРОЄННЯ В УМОВАХ ВОЄННОГО СТАНУ

Федорович О.Є., Поліщук Є.В., Соловйов В.С., Федорович В.А.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Запаси озброєння грають основну роль для проведення ефективних бойових дій в зоні воєнного конфлікту.

Тому актуальна тема доповіді, в якій представлені результати моделювання логістики формування запасів озброєння для створення військового паритету сил в зоні воєнного конфлікту [1, 2].

Метою доповіді є побудова оптимізаційної моделі для оцінки необхідних запасів озброєння потрібних в зоні воєнного конфлікту, які забезпечують формування військового паритету сил, а також можливої асиметрії за рахунок використання сучасної зброї (перевага якості над кількістю).

В доповіді наведено результати розробки та використання оптимізаційної моделі, за допомогою якої формується вимоги до запасів озброєння в інтервальному вигляді від мінімальних до максимальних запасів. Мінімальні (страхові) запаси дозволяють не порушити характер бойових дій (наступ або оборона).

Максимальні запаси забезпечують встановлення асиметрії у військовому паритеті сил.

Проведена оптимізація логістичних витрат, які виникають при постачанні військової техніки в зону воєнного конфлікту в умовах загроз та ризиків воєнного тану.

Результати дослідження доцільно використовувати для обґрунтування необхідних обсягів озброєння та військової техніки в зоні воєнного конфлікту та формування довгих логістичних ланцюгів постачання озброєння.

Використані математичні методи: системний аналіз, цілочисельна (булева) оптимізація, багатокритеріальний метод, якісні та кісні оцінювання. Наукова новизна дослідження пов’язана зі створенням оптимізаційних моделей для аналізу формування запасів озброєння в зоні воєнного конфлікту.

Список літератури

1. Value stream analysis in military logistics: The improvement in order processing procedure [Text] / R. Acero, M. Torralba, R. Pérez-Moya, J. A. Pozo // Applied Sciences. – 2020. – Vol. 10, No. 1. – Article No. 106. DOI: 10.3390/app10010106.

2. Федорович, О. Є. Метод формування логістичних транспортних взаємодій для нового портфелю замовлень розподіленого віртуального виробництва [Text] / О. Є. Федорович, Ю. Л. Прончаков // Радіоелектронні і комп'ютерні системи. – 2020. – № 2. – С. 102-108. DOI: 10.32620/reks.2020.2.09.

МОДЕЛІ ЛОГІСТИКИ ПОСТАЧАННЯ ВИСОКОТЕХНОЛОГІЧНИХ ПІДПРИЄМСТВ В МИРНИЙ ЧАС ТА В УМОВАХ ВОЄННОГО СТАНУ

Федорович О.Є., Прончаков Ю.Л., Рибка К.О.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Сучасна логістика постачання високотехнологічних підприємств є складною з-за глобалізації виробництва та появи довгих логістичних ланцюгів. Тому актуальна тема доповіді, в якій представлені результати дослідження логістики постачання підприємств в мирний час та в умовах воєнного стану [1, 2].

Метою доповіді є створення комплексу моделей для аналізу та оптимізації логістичних ланцюгів постачання високотехнологічних підприємств як в мирний час, так і в умовах воєнного стану.

В доповіді наведені результати моделювання довгих ланцюгів постачання з урахуванням можливих загроз та виникнення вразливостей як у мирний час, так і в воєнному стані країни. Створена модель для оптимізації логістичних витрат з урахуванням вразливостей, які виникають в довгих ланцюгах постачання (старіння транспортних систем, виникнення кліматичних загроз, вузькі місця, тощо). У мирний час загрози пов'язані з деградацією транспортних систем, появою терористичних актів, аварійних ситуацій, тощо. В умовах воєнного стану, виникають нові загрози логістики постачання, які необхідно врахувати при формуванні логістичних каналів для транспортування озброєння та військової техніки. Проведена оптимізація ризиків постачання, в умовах воєнних загроз, з урахуванням часу та витрат. При евакуації (релокації) високотехнологічних підприємств до тилу, виникає ряд нових логістичних задач таких як: вибір місця розташування підприємства, формування нових логістичних каналів постачання, створення стабільної енергетичної структури, тощо. Розроблена інтерактивна імітаційна модель для дослідження динаміки логістичних процесів постачання високотехнологічних підприємств як у мирний час, так і в умах воєнного стану. Розроблено оригінальний алгоритм оптимізації, за рахунок хвиль заявок, які розповсюджуються в різнорідній транспортній мережі, для пошуку оптимальних маршрутів в умовах загроз та збудження вразливостей.

Список літератури

1. Value stream analysis in military logistics: The improvement in order processing procedure [Text] / R. Acero, M. Torralba, R. Pérez-Moya, J. A. Pozo // Applied Sciences. – 2020. – Vol. 10, No. 1. – Article No. 106. DOI: 10.3390/app10010106.

2. Моделювання транспортної логістики військових вантажів з урахуванням збитків, які виникають у зоні бойових дій через запізнення у постачанні [Текст] / О. Є. Федорович, О. С. Уруський, І. Б. Чепков, М. І. Луханін, Ю. Л. Прончаков, К. О. Рибка, Ю. О. Лещенко // Радіоелектронні і комп'ютерні системи. – 2022. – № 2. – С. 63-74. DOI: 10.32620/reks.2022.2.05.

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ЛОГІСТИКИ ПОСТАЧАННЯ ОЗБРОЄННЯ В ЗОНУ БОЙОВИХ ДІЙ

Федорович О.Є., Рибка А.В., Чмихун Є.К., Пісклова Т.С.
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Загострення бойових дій в зоні воєнного конфлікту потребує своєчасного постачання озброєння для створення військового паритету сил.

Тому актуальна тема доповіді, в якій представлені результати дослідження логістики постачання військової техніки в умовах воєнного стану країни [1, 2].

Метою доповіді є створення інтерактивної імітаційної моделі для аналізу постачання військової техніки в зону воєнного конфлікту.

В доповіді наведено результати імітаційного моделювання логістики постачання озброєння малими партіями в умовах воєнних загроз.

За допомогою розробленої імітаційної моделі досліджуються довгі логістичні ланцюги постачання озброєння в умовах виникнення загроз та ризиків воєнного стану.

Розроблено оригінальний алгоритм для дослідження логістичних ланцюгів постачання, заснований на появі клонів від заявки (мала партія озброєння) у вузлах транспортної мережі.

За результатом конкурентної боротьби клонів, в транспортній мережі формується маршрут постачання озброєння з мінімальним часом в умовах виникнення загроз та збудження можливих вразливостей. Оцінюються логістичні витрати для постачання озброєння. Своєчасне постачання озброєння створює військовий паритет сил.

Тому час постачання є основним критерієм в імітаційному інтерактивному моделюванні.

Результати дослідження доцільно використовувати для формування план-графіків та маршрутів перевезення військової техніки від постачальників до зони бойових дій в умовах воєнних загроз.

Список літератури

1. Pecina, M. Application of the new NATO logistics system [Text] / M. Pecina, J. Husak // Land Forces Academy Review. – 2018. – Vol. 23, No. 2. – P. 121-127. DOI: 10.2478/raft-2018-0014.

2. Моделювання критичних вразливостей у логістиці постачання озброєння та військової техніки в умовах воєнних загроз [Текст] / О. Є. Федорович, Є. В. Поліщук, Є. К. Чмихун, В. С. Соловйов // Авіаційно-космічна техніка і технологія. – 2022. – № 6 (184). – С. 40–49. DOI: 10.32620/aktt.2022.6.05.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ КОНТРОЛЯ ТА РЕАГУВАННЯ НА ПРИРОДНІ КАТАСТРОФИ

Євгеньєв А.М., Риков Д.М., Бураков А.Р.
Харківський національний університет радіоелектроніки, Харків, Україна

Доповідь спрямована на дослідження використання інформаційних технологій для моніторингу та реагування на стихійні лиха та їх прогнозування. Проводиться аналіз, як ці технології можуть контролювати стихійні лиха та реагувати на них.

В сучасному світі природні катастрофи стають все більш непередбачуваними та руйнівними. Над цією темою працювали відомі науковці, такі як J. Smith [1], K. Gale [2] та Бондар Ю. [3].

Метою доповіді є дослідження можливостей використання інформаційних технологій для контролю та реагування на природні катастрофи.

Одним з найважливіших інструментів в цьому процесі є супутниковий моніторинг [1]. Він дозволяє отримувати різноманітну інформацію про природні катастрофи з високої точністю та швидкістю.

Зокрема, супутники здатні визначати місцезнаходження та інтенсивність землетрусів, пожеж та повеней, що приводить до зменшення наслідків природних катастроф.

Також існують системи, які включають в себе дрони [2] та мобільні додатки, які використовуються для збору та аналізу даних про погодні, геологічні умови та інші фактори, що можуть призвести до природних катастроф. На основі отриманих даних створюються прогнози, які дозволяють вживати заходів для зменшення ризику виникнення катастроф.

Мобільні додатки використовують для забезпечення безпеки населення, а саме надання оперативної інформації про небезпеку та вказівок щодо поведінки в разі катастрофи.

Отже, використання інформаційних технологій для контролю та реагування на природні катастрофи має великий потенціал та може значно зменшити наслідки таких подій. Однак, вони не є універсальним засобом для вирішення всіх проблем.

Важливо розуміти, що дії відповідальних органів та громадськості є необхідними для досягнення успіху в боротьбі з природними катастрофами.

Список літератури

1. Smith, J. The Role of Information Technology in Disaster Response. Journal of Emergency Management. 2018. P. 195-202.

2. Gale, K. Using Drones for Disaster Management: A Review. Geomatics, Natural Hazards and Risk. 2017. P. 720-735.

3. Боднар Ю. Застосування інформаційних технологій в системі захисту населення та територій від надзвичайних ситуацій. Електроніка та зв'язок. 2015. № 2. С. 125-129.

ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО ЗАХИСТУ БУДИНКУ ІЗ СИСТЕМОЮ «РОЗУМНИЙ ДІМ»

Винник І.Р., В'юхін Д.А.,
Харківський національний університет радіоелектроніки»
Сухотеплий В.М.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба, Харків, Україна

Сучасні технології роблять наші будинки все більш безпечними та комфортними для проживання.

Завдяки системі "Розумний дім" можна ефективно контролювати стан будинку та забезпечувати його захист від різних небезпек. Ця система включає в себе різноманітні сенсори, пристрої відеоспостереження, засоби контролю доступу та інші компоненти, які дозволяють відслідковувати події, відбуваються в будинку, та вчасно реагувати на них.

У зв'язку з цим, актуальною є тема дослідження системи "Розумний дім" для забезпечення ефективного захисту будинку.

Проведений аналіз показав, що існує багато факторів, що впливають на безпеку в системі "Розумний дім" виведення з ладу комунікаційного обладнання системи, витік [1-3].

Метою доповіді є дослідження та аналіз можливостей системи "Розумний дім" для забезпечення ефективного захисту будинку.

Розглянута система "Розумний дім" як інноваційний метод забезпечення безпеки та комфорту в будинку, проведена оцінка технічних характеристик та можливостей системи "Розумний дім" для виявлення та запобігання можливих загроз безпеці житла.

Проведені дослідження впливу системи "Розумний дім" на зниження ризику крадіжок, пожеж та інших небезпечних ситуацій в будинку, розглянуті алгоритми та програмне забезпечення для оптимального управління системою "Розумний дім" з метою максимального захисту будинку.

Проведений аналіз питань впровадження системи "Розумний дім" в будинок та ефективність використання системи для забезпечення безпеки житла в різних умовах експлуатації та відповідність вимогам сучасних стандартів безпеки будинку.

Список літератури

1. Д'якова, Н.Є., Сєвєрінов О.В. Аналіз загроз безпеки у системах розумного будинку. ВА ЗС АР; НТУ" ХПІ"; НАУ, ДП" ПДПРОНДІАВІАПРОМ"; УмЖ, 2021.

2. Fernandes E., Jung J., Prakash A. Security Analysis of Emerging Smart Home Applications. *2016 IEEE Symposium on Security and Privacy*, 23–25 May 2016. P. 636–654.

3. Reddy V. S. s., Sai P. V. K., Namburu A. Smart Home Security System. *Recent Advances in Computer Based Systems, Processes and Applications*. 2020. P. 127–133. URL: https://doi.org/10.1201/9781003043980-16 (Дата звернення: 10.03.2023).

ПРИЙНЯТТЯ АНТИКРИЗОВИХ РІШЕНЬ В УМОВАХ ВИНИКНЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ РІЗНОГО ХАРАКТЕРУ

Тютюник О.О.
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
Тютюник В.В.
Національний університет цивільного захисту України, Харків, Україна

Створення в Україні ситуаційних центрів, як елементів єдиної державної системи цивільного захисту (ЄДСЦЗ), відбувається в умовах імовірнісного територіально-часового розподілу джерел виникнення небезпек. Це обумовлюється невизначеністю параметрів, які впливають на умови нормального функціонування території України. У зв'язку з цим виникає проблема прийняття оптимальних антикризових рішень в умовах невизначеності щодо забезпечення відповідного рівня безпеки життєдіяльності держави. Крім того, ситуаційний центр при функціонуванні в ЄДСЦЗ повинен забезпечити:

1) аналіз отриманої від підсистеми моніторингу інформації;

2) моделювання розвитку НС на території міста, регіону, держави;

3) розробку та ухвалення управлінських рішень щодо попередження та ліквідації НС, а також мінімізації їх наслідків [1].

В роботі [2] показано, що процедура прийняття експертами ситуаційного центру управлінських антикризових рішень ускладнюється тим, що необхідними умовами ефективності рішень є їх своєчасність, повнота й оптимальність. Тому, підвищення ефективності прийнятих рішень пов'язане з необхідністю рішення задачі багатокритеріальної оптимізації в умовах невизначеності. Це потребує розробки формальних, нормативних методів і моделей для комплексного рішення проблеми прийняття рішень в умовах багатокритеріальності й невизначеності при управлінні процесами запобігання та локалізації НС для забезпечення ефективного функціонування ЄДСЦЗ за трьома групами критеріїв, а саме: показники забезпечення відповідного рівня безпеки життєдіяльності; показники функціональної спроможності ЄДСЦЗ; показники фінансових затрат на функціонування цієї системи безпеки [2].

Список літератури

1. Рубан І.В., Тютюник В.В., Тютюник О.О. Особливості створення системи підтримки прийняття антикризових рішень в умовах невизначеності вхідної інформації при надзвичайних ситуаціях. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Київ: Національний університет оборони України імені Івана Черняховського, 2021. №1(40). С. 75–84.

2. Тютюник В.В., Ященко О.А., Рубан І.В., Тютюник О.О. Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Київ: Національний університет оборони України імені Івана Черняховського. 2022. Вип. 1(43). С. 41–52.

ПРИЙНЯТТЯ АНТИКРИЗОВИХ РІШЕНЬ В УМОВАХ ВИНИКНЕННЯ ГЕОФІЗИЧНИХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Тютюник В.В.
Національний університет цивільного захисту України, Харків, Україна
Агазаде Т.Х.
Державна Протипожежна Служба МНС Азербайджану, Баку, Азербайджан

В роботі [1] розроблено ймовірнісну математичну модель оцінки можливості виникнення землетрусів магнітудою ≥ 5 на окремій сейсмічно активній території Земної кулі в залежності від рівня сейсмічної активності Земної кулі.

У якості вхідних даних щодо визначеності параметрів розподілу Парето використані результатами спостережень Головного центру спеціального контролю Державного космічного агентства України за рівнем сейсмічної активності Земної кулі за період 2009–2021 рр.

Результати моделювання лягли в основу удосконалення функціонування ситуаційних центрів [2] щодо процедури підтримки прийняття антикризових рішень на виконання структурними підрозділами системи цивільного захисту задач за призначенням, які спрямовані на мінімізацію наслідків від геофізичних надзвичайних ситуацій. Інформаційно-технічна реалізація розробленої математичної моделі в інтересах удосконалення процедури підтримки прийняття антикризових рішень передбачає комплексне виконання в системі єдиного часу наступних п’яти функцій: 1) безперервний глобальний моніторинг рівня сейсмічної активності Земної кулі; 2) безперервний моніторинг сейсмічної активності окремої території Земної кулі; 3) оцінка, за результатами моніторингових спостережень, ймовірностей виникнення землетрусів на окремих сейсмічно активних територіях Земної кулі в залежності від рівня сейсмічної активності Земної кулі; 4) реалізація на окремій сейсмічно активній території Земної кулі, за результатами оцінки ймовірності виникнення на цій території землетрусу, режиму підвищеної готовності системи цивільного захисту; 5) реалізація на окремій сейсмічно активній території Земної кулі, за результатами безперервного моніторингу її сейсмічної активності, режиму "Геофізична надзвичайна ситуація".

Список літератури

1. Агазаде Т.Х., Тютюник В.В., Чорногор Л.Ф., Тютюник О.О. Особливості підтримання ухвалення антикризових рішень в умовах виникнення геофізичних надзвичайних ситуацій. Науковий вісник: Цивільний захист та пожежна безпека. Київ: Інститут державного управління та наукових досліджень з цивільного захисту, 2022. № 2(14). С. 65–79.

2. Тютюник В.В., Ященко О.А., Рубан І.В., Тютюник О.О. Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Київ: Національний університет оборони України імені Івана Черняховського. 2022. Вип. 1(43). С. 41–52.

УЧАСНИКИ КОНФЕРЕНЦІЇ (секції 1, 3, 4)

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Азербайджанський технічний університет, Баку, Азербайджан
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Полтава, Київ, Україна
Державна протипожежна плужба МНС Азербайджану, Баку, Азербайджан
Державний біотехнологічний університет, Харків, Україна
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Чернігів, Україна
Державний університет інфраструктури та технологій, Київ, Україна
Інститут систем управління Азербайджанської Національної академії наук, Баку, Азербайджан
Київський національний університет будівництва і архітектури, Київ, Україна
Нахічеванський державний університет, Нахічевань, Азербайджан
Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна
Національний авіаційний університет, Київ, Україна
Національний аерокосмічний університет імені М. Є. Жуковського "Харківський авіаційний інститут", Харків, Україна
Національний технічний університет "Харківський політехнічний інститут", Харків, Україна
Національний університет «Львівська політехніка», Львів, Україна
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
Національний університет оборони Азербайджанської республіки, Баку, Азербайджан
Національний університет цивільного захисту України, Харків, Україна
ТОВ "КІНЕТІКС", Львів, Україна
Український державний університет залізничного транспорту, Харків, Україна
Університет міста Жиліна, Жиліна, Словаччина
Університет технології і гуманітарних наук, Бельсько-Бяла, Польща
Харківський військовий інститут танкових військ, Харків, Україна
Харківський гуманітарний університет «Народна українська академія», Харків, Україна
Харківський національний автомобільно-дорожній університет, Харків, Україна
Харківський національний економічний університет імені Саймона Кузнеця, Харків, Україна
Харківський національний університет імені В.Н. Каразіна, Харків, Україна
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна
Харківський національний університет радіоелектроніки, Харків, Україна

ЗМІСТ

НАУКОВЕ ВИДАННЯ

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей
тринадцятої міжнародної науково-технічної конференції
(26 – 27 квітня 2023 року)
Том 1: секції 1, 3, 4

Відповідальний за випуск *В. В. Косенко*
Технічний редактор *І. А. Лєбедева*
Коректор *В. В. Богомаз*
Комп'ютерне складання та верстання *Н. Г. Кучук*

Адреса оргкомітету: вул. Кирпичова, 2, Харків, 61002, Україна
Вечірній корпус, кімната 314
тел. +38 (057) 707 61 65

Підписано до друку 18.04.2023 Формат 60 × 84/16
Ум.-вид. арк. 6,75. Тираж 100 пр. Зам. 418-23

Віддруковано з готових оригінал-макетів у цифровій друкарні Impress
61002, м. Харків, вул. Пушкінська, 56, тел. **+ 38 (057) 714-52-11**
e-mail: **irina@impress.biz.ua**